What is the Attitude of IT Professionals towards Cloud Computing Adoption Barriers?

Robert Whelan

A dissertation submitted to the University of Dublin

in partial fulfilment of the requirements for the degree of

MSc in Management of Information Systems

2017

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: 

Robert Whelan

1st September 2017

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: 

Robert Whelan

1st September 2017

Acknowledgements

I would like to thank my wife for her unwavering faith, love, and support.

I am also grateful to the participants in this study who willingly gave of their time to assist me with this research.

Finally, I would like to express my gratitude to my academic supervisor, Anthony Niland, for his guidance and advice throughout this research dissertation.

Abstract

This dissertation is an exploratory study that seeks to determine the attitude of IT professionals towards barriers to cloud computing adoption. This is an important and topical subject as many companies are beginning their journey to the cloud and the attitudes of key personnel in the IT department, those with a strong influence on the IT decision making process, will have a major impact on how successful, or not, that journey will be. This study identifies those barriers by performing a thorough examination of the extant literature on the topic of cloud computing with a particular focus on barriers to cloud computing adoption. Face-to-face semi-structured interviews were conducted with experienced IT professionals, their experience ranging from 12 to over 40 years, to elicit their attitudes towards the identified barriers. These IT professionals all play a role in the IT decision making process. The interviews were recorded and transcribed, and Grounded Theory was used to analyse the data and to inductively generate theories that are grounded in that data. These theories enabled the formulation of recommendations to practitioners, particularly cloud computing vendors. The attitudes of IT professionals towards cloud computing adoption barriers is hesitant acceptance, based on trust. This study has highlighted the importance of trust when considering the selection of cloud computing vendors and also the necessity of upskilling for all IT professionals especially those that work directly with computing infrastructure as they will be most impacted by the cloud computing journey.

Table of Contents

List of figures

List of Tables

Abbreviations

ARPANET	Advanced Research Projects Agency Network
AWS	Amazon Web Services
CEO	Chief Executive Officer
CSP	Cloud Service Provider
DoI	Diffusion of Innovation
DoJ	Department of Justice
EC2	Elastic Compute Cloud
EU	European Union
GDPR	General Data Protection Regulation
IaaS	Infrastructure-as-a-Service
IT	Information Technology
NIST	National Institute of Standards and Technology
PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
SLA	Service Level Agreement
TOE	Technology-Organization-Environment

1 Introduction

1.1 Background and Context

During the nineteenth century many companies, and wealthy households, had their own means of generating electricity; they owned their own electricity generator. By the beginning of the twentieth century it was becoming rarer and rarer for companies and households to have their own electricity generators as they were purchasing electricity directly from an electrical utility company that generated the electricity (Carr, 2008). Cloud computing is increasingly being viewed as having the potential to enable computing to transform into a utility in the same way as the transformation of electricity into a utility by allowing users of computing to consume computing resources just like they consume other utilities. Cloud computing has been called the fifth utility, with the other four utilities being electricity, water, gas, and telephony (Buyya et al, 2009).

Cloud computing is a relatively recent development in mainstream computing that has been growing rapidly with revenue from Infrastructure-as-a-Service increasing by 40% per year since 2011 (Gartner, 2016). Cloud computing has been described as a rebranding of the internet (Daylami, 2015) because cloud computing describes a model of computing where most, if not all, of the processing, the actual computing, is carried out by computers that are accessed via the internet.

Cloud computing offers many benefits to companies, primarily a reduction in the cost of operating their IT function. However, there are some concerns and potential issues with adopting cloud computing; it can be a challenging process and can lead to severe disruption of IT services if carried out without due care and planning.

This paper assesses current attitudes towards cloud computing amongst IT professionals with a specific focus on barriers to the adoption of cloud solutions. Many IT departments are concerned about potential issues that will be encountered post-adoption and also concerned about potential issues with the actual adoption itself. These potential issues are known as barriers.

1.2 Research Question

This research study is an exploratory study that seeks to determine the attitude of experienced IT professionals that are involved in the IT decision making process, to the barriers presented by cloud computing adoption. The question is:

What is the attitude of IT professionals towards cloud computing adoption barriers?

1.3 Importance of this Research

Cloud computing is a very topical subject amongst IT professionals as many companies are beginning their journey into the cloud. However, barriers to adoption may cause some companies to reconsider and not adopt cloud computing because they are concerned about these barriers. In many cases, IT professionals will have a strong influence on whether or not companies adopt cloud computing so it is very important to assess their attitudes to these barriers. This research is important to all of the stakeholders in cloud computing adoptions: the cloud computing vendors, the companies considering adopting cloud computing, and the IT professionals. This research is important for cloud computing vendors as it will enable them to become aware of, and deal with, any objections from IT professionals that could lead to companies deciding not to begin their journey to the cloud. This research is important to companies that are considering adopting cloud computing as it highlights the problems that can arise during, and after, cloud computing adoption. These problems would negatively affect companies that were not sufficiently prepared prior to their adoption. Finally, this research is important for IT professionals as it will ensure that they are aware of the barriers to adoption as well as allowing them a view on the attitude of other IT professionals towards those barriers. It will help them to solidify their own thoughts and opinions about whether or not their own company should move to the cloud.

1.4 Scope of the Study

This is an exploratory study that utilises face-to-face interviews with IT professionals to determine their attitudes towards cloud computing adoption barriers. Theories regarding their attitudes are then generated from the interview data. This study focuses on the barriers to adoption and does not delve into the benefits of cloud computing or into the various technologies that enable cloud computing.

The interviews were conducted during the month of June in 2017.

1.5 Chapter Roadmap

This study is divided into five chapters. An outline of the contents of each chapter is presented below.

• Chapter 1

This chapter serves as an introduction to the topic being researched; the background and context of the research is outlined, the question that the research seeks to answer is specified, the importance of this research along with those who will find it important is stated, the scope of the study is also specified, and a roadmap of this research paper is presented.

• Chapter 2

In this chapter, the relevant literature is reviewed. In order to properly answer the research question, the cloud computing adoption barriers will first need to be identified, this chapter identifies the barriers and describes each barrier. An overview of cloud computing is also given along with its history, and its benefits.

• Chapter 3

This chapter describes the methodology used for this research as well as the reasons why this particular methodology was utilised.

• Chapter 4

This chapter contains an in-depth analysis of the gathered data and also provides some direct quotations from the research participants. The interview process is described in detail and some theories are generated from the data.

• Chapter 5

This chapter demonstrates that the research question has been answered, discusses the limitations of the research and also provides some proposals for further research. Recommendations for the stakeholders of cloud computing are presented in this chapter.

2. Literature Review

2.1 Introduction

The topic of this literature review is cloud computing with a focus on adoption and barriers to adoption of cloud computing. Twenty-eight academic journal articles are directly referenced in this review. This review begins by defining cloud computing, its characteristics, service models and deployment models. A history of cloud computing, including the term itself, follows from this before the benefits and barriers of cloud computing are listed. The next section delves into other factors that affect adoption. Finally, the role of Cloud Service Providers is examined.

2.2 Sources

The main source for the literature referenced in this review was the library of Trinity College Dublin via its online tool, the Stella search function. The following terms were searched for initially: “cloud computing”, “cloud adoption”, and “utility computing”. Favouring newer papers, the search results were examined and relevant papers were downloaded, read, and had their references consulted. Relevant referenced papers were then searched for on Stella directly by article name. In this way, all of the seminal papers were detected and included as part of this review as they were referenced in many of the newer papers.

2.3 Definition of Cloud Computing

Cloud computing is a generic term used to describe a particular model of computing. It has historically suffered from nebulous definitions with each author providing their own interpretation of its precise meaning. For example Buyya et al (2009), Iyer and Henderson (2010), Marston et al (2011), each provide their own definition of cloud computing. However, the National Institute of Standards and Technology (NIST) in the United States of America released their sixteenth, and final, definition of cloud computing:

> “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” (Mell and Grance, 2011, p. 2).

The fact that it required sixteen revisions demonstrates the confusion, and difficulty, surrounding defining exactly what is meant by cloud computing. Since the NIST released this definition in 2011, most of the papers in this review no longer provide their own

definitions but instead reference the NIST definition. There is no paper in this review that does not begin by defining cloud computing.

Even this definition by the NIST, although it clears up the confusion in the academic world, is itself confusing for a newcomer to cloud computing. Daylami (2015, p. 39) attempts to simplify cloud computing by describing it as “a metaphor for the internet”. Taken further, this would mean that any computing done over the internet could be described as cloud computing; however, now that there is an official definition, Daylami’s description of the cloud as a metaphor for the internet is not valid as, to qualify as being cloud computing, the following characteristics must be met:

2.3.1 Characteristics of Cloud Computing

The NIST definition of cloud computing defines and lists the five essential characteristics of the cloud model: (Mell and Grance, 2011)

1. On-demand self-service: The ability for a consumer to provision additional resources, such as additional computing power or extra storage, without requiring human interaction with the service provider.
2. Broad network access: Systems can be accessed over the network from a mixture of different client types such as laptops, personal computers, tablets, phones, any device with a web browser.
3. Resource pooling: Dynamically assigned computing resources are shared by multiple consumers, in a multi-tenant model, that are location independent with the consumers often unaware of the exact location of their computing resources beyond a high-level notion of which country or general area the datacentre is based in.
4. Rapid elasticity: Resources can be increased to a seemingly unlimited degree, in some cases even automatically. It is not actually unlimited or infinite but it seems that way to the consumer. Additionally, elasticity also means that the resources can also be decreased rapidly and even automatically if required.
5. Measured service: Resource usage is metered and can be monitored and controlled. It can also be reported on in order to provide transparency for both the consumer and the provider. This is also to ensure that consumers can be billed accurately.

Taking all of the above into consideration, a succinct definition of cloud computing is given below:

Cloud Computing is automatic rapid scaling computing systems that can be shared between multiple consumers, accurately metered, and accessed over a network.

This definition is what is meant by the term “cloud computing” wherever it is used throughout this document. Although this definition is certainly longer than Daylami’s metaphor, it does

embrace all five of the essential characteristics as defined by the NIST so it is a more accurate representation of the modern, official meaning of the term.

2.3.2 Cloud Infrastructure

Cloud infrastructure is the term used to describe the hardware and software that is required to fulfil the five essential characteristics of cloud computing. This includes the actual computers, virtualisation software, and cloud management software.

2.3.3 Cloud Computing Service Models

There are three service models in cloud computing, also defined by the NIST:

1. Software-as-a-Service (SaaS): The Cloud Service Provider (CSP) enables access to applications running on underlying cloud infrastructure that is operated by the CSP. The consumer does not have the ability to manage the underlying cloud infrastructure. SaaS applications do not run directly on the infrastructure, there is an operating system layer between the SaaS applications and the infrastructure.
2. Platform-as-a-Service (PaaS): The consumer has the ability to add their own applications to the CSPs cloud infrastructure. As with SaaS, consumers of PaaS do not have the ability to manage the underlying infrastructure but they do have access to the operating systems that are running on the infrastructure.
3. Infrastructure-as-a-Service (IaaS): The consumer has the ability to provision computing resources to run their own software, including operating systems. The consumer does not have the ability to manage the underlying cloud infrastructure but can control the operating systems and storage, and can have limited control over some networking infrastructure such as firewalls.

2.3.4 Cloud Computing Deployment Models

Finally, the NIST definition of cloud computing is completed by defining the four types of deployment model:

1. Private cloud: The cloud infrastructure is utilised by a single organisation, even if it is managed by a third party.
2. Community cloud: The cloud infrastructure is exclusively utilised by a community of organisations that have shared concerns.
3. Public cloud: The cloud infrastructure can be utilised by the general public.

4. Hybrid cloud: The cloud infrastructure used is a combination of at least two of the three cloud deployments previously mentioned: Private cloud, Community cloud, and Public cloud.

2.3.5 A Model of Cloud Computing

The diagram below shows how the service models and deployment models of cloud computing interoperate.

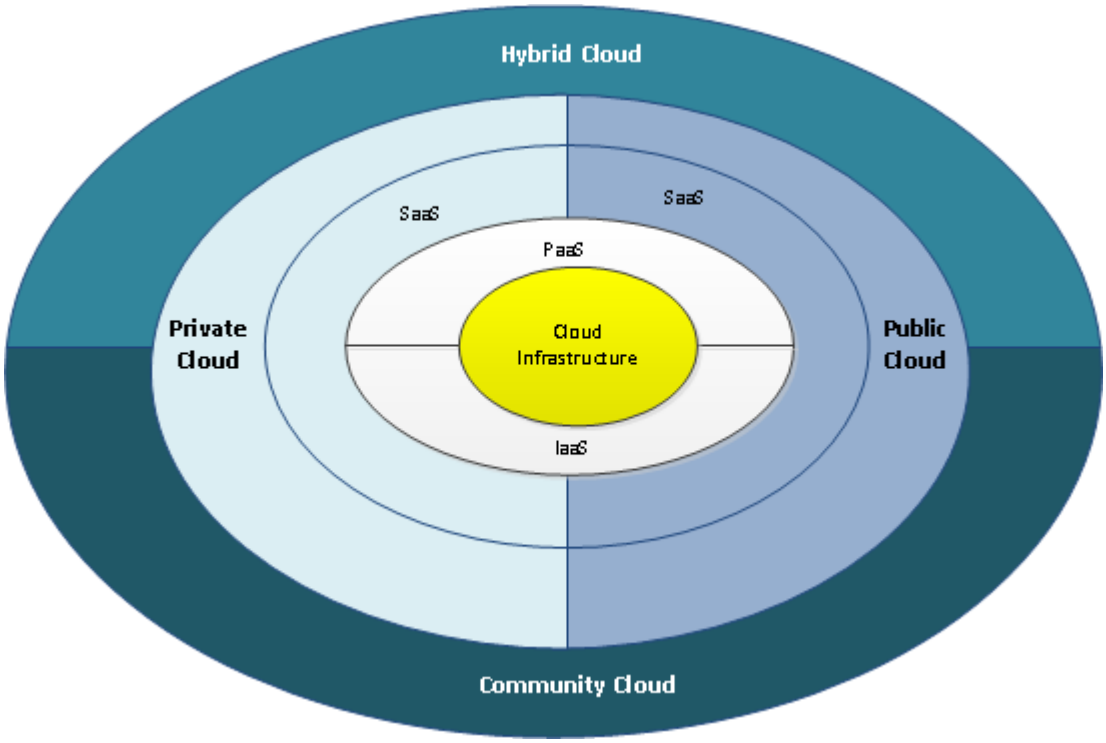

Figure 1: Cloud Computing visualised (created by the author for this paper)

The very centre of the egg diagram represents the actual hardware and software that runs the cloud computing, which is known as the cloud infrastructure. Both IaaS and PaaS interact directly with the cloud infrastructure but they are exclusive of each other so they each have their own portion of the first layer. The next layer is SaaS which requires underlying systems between it and the cloud infrastructure. The next layer shows how both public cloud and private cloud can contain IaaS, PaaS, and/or SaaS but are mutually exclusive of each other. Finally, the outer layer of the egg contains hybrid cloud solutions and community cloud solutions which can contain all of the components in the inner layers of the egg.

2.4 History of Cloud Computing

Prior to being known as cloud computing, this model of remote computing was known as utility computing. In the 1960s, researchers such as Douglas Parkhill and John McCarthy

shared their vision of the future of computing as being a utility similar to traditional utilities (Durao et al, 2014). In 1969, a press release describing the forthcoming precursor to the internet, Advanced Research Projects Agency Network, known as ARPANET, was issued. This press release closes with Leonard Kleinrock describing his vision of the future: "As of now, computer networks are still in their infancy. But as they grow up and become more sophisticated, we will probably see the spread of computer utilities which, like present electric and telephone utilities, will service individual homes and offices across the country" (Kleinrock, 2003, p. 4). This has now proven to be a prescient statement, however it was not until the 2000's that this vision could be said to have been fulfilled with the modern inception of cloud computing. Buyya et al in 2009 made the direct connection between utility computing and cloud computing by describing cloud computing as the "5th utility" with the other four being gas, water, electricity, and telephones.

The term cloud computing was originally coined by George Favaloro and Sean O'Sullivan in 1996 whilst working for Compaq. They were formulating their strategy for the internet which they described as "cloud computing"; they envisioned applications being delivered over the internet. Interestingly, O'Sullivan had a failed attempt to trademark the term in 1997 during his time with NetCentric, a company he founded (Regalado, 2011).

It was another ten years before the term became more mainstream. During a conference in 2006, the CEO of Google, Eric Schmidt said "What's interesting is that there is an emergent new model. I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing—they should be in a "cloud" somewhere" (Daylami, 2015, p. 41).

It was this same year, 2006, that Amazon Web Services (AWS) released their IaaS product, Elastic Compute Cloud (EC2). Companies then released software packages that could only be used online, such as Google's G-Suite in 2009 and Microsoft Office 365 in 2011. Microsoft, through their Azure platform, which was released in 2010, now offer 109 cloud services (Microsoft, 2017).

Certainly the vision from the 1960s of computing as a utility is now being adopted through its current incarnation of cloud computing.

2.5 Benefits of Cloud Computing

The benefits of cloud computing are well known and without controversy amongst the literature. The rise of cloud computing in recent years, and its continued growth, attests to the allure of reaping its benefits. These benefits can be divided into two main groups: financial benefits and resource management benefits (Lin and Chen, 2012).

2.5.1 Financial Benefits

Companies can immediately access both hardware and software resources without all the associated costs such as purchasing hardware, installation and configuration fees, and licensing costs. This pay-as-you-go model allows companies to view IT costs as operating expenditure rather than capital expenditure. This means that the upfront costs of computing can be eliminated thereby enabling companies to almost instantly access large amounts of computing power with relatively little outlay. This is especially beneficial to smaller companies that do not have the necessary resources to procure their own large computing systems.

2.5.2 Resource Management Benefits

Traditionally companies provisioned their hardware infrastructure for peak load. This meant that the hardware was underutilised outside of peak times. It is believed that most servers in traditional data centres have an average utilisation of between 5% and 20% (Armbrust et al, 2010). Clearly this represents a large amount of underutilisation but if companies do not size their hardware with the ability to cope with peak load, they may then lose customers due to the systems being too slow or unusable during peak times.

Elasticity refers to the property of cloud computing that allows companies to scale-up automatically as demand increases, almost instantaneously, with a seemingly infinite amount of hardware resource available. This is very beneficial for companies that have peaks and troughs in their demand, and can lead to improved response time and less wasted resources as elasticity also allows companies to scale-down automatically too, ensuring that companies only pay for the hardware that they actually need.

This level of flexibility solves the problem of sizing for peak demand as now companies only pay for the hardware that they are actually using and they can release it outside of peak demand.

2.5.3 Five Key Advantages of Cloud Computing

Lin and Chen (2012) identify five key advantages of cloud computing:

1. Lower cost of entry for smaller firms seeking to utilise large amounts of computing power. The third world is specifically mentioned as a potential beneficiary of cloud computing.
2. No upfront capital costs required; IT is an operational expense rather than a capital expense.

3. Lower barriers to innovation for start-ups as they can access large amounts of compute at a relatively low cost.
4. Due to elasticity, companies can easily scale their resources to match client demand.
5. It makes available new classes of applications; for example, companies can process huge amounts of data in a short period of time by increasing, or ramping up, their available computing power.

These five key advantages fit evenly into the areas of financial benefits and resource management benefits with the first three being financial benefits and the last two being resource management benefits but it has been useful to extrapolate them above to further illustrate the benefits.

2.5.4 Seven Capabilities of Cloud Computing

Iyer and Henderson (2010) considered the advantages of cloud computing from a business point-of-view as opposed to a technological point-of-view and identified seven capabilities of cloud computing:

1. Controlled interface
   Each application service that is added to the cloud becomes part of an organic infrastructure and can be used by other services leading to greater opportunities for collaboration and innovation.
2. Location independence
   Data and applications can be stored and accessed from anywhere without the user knowing, or needing to know, where the data is being accessed from. The user also does not need to be located near the data or applications leading to increased mobility.
3. Sourcing independence
   Companies can switch providers easily and without too much trouble. The non-cloud model of computing can lead to vendor lock-in with companies only able to switch providers at great cost.
4. Ubiquitous access
   Users can access any of the company's applications from any device using only a web browser.
5. Virtual business environments
   A suite of applications is created that specifically targets a specific business unit or function. This is especially useful with creating test environments.
6. Addressability and Traceability

The usage of the information systems can be audited and tracked enabling companies to know who accessed their data, when the data was accessed, and even where the user was at the time.

7. Rapid elasticity
   Removes the need for companies to size their hardware requirements around peak capacity, instead opting to increase their cloud usage as demand increases.

Some of these capabilities do fit neatly within the dual benefits model identified by Lin and Chen (2012), for example capability 7, Rapid elasticity, is a resource management benefit. However some of the other benefits have corresponding barriers that are not discussed by the authors, for example capability 1, Controlled interface, will lead to additional complexity despite Iyer and Henderson's (2010) assertion that cloud computing reduces complexity. The third capability, Sourcing independence, is claimed by the authors to reduce vendor lock-in but it is not mentioned that switching providers, even in the cloud, can be a very costly process.

2.5.5 Green IT

Adoption of the cloud can also enable companies to meet their targets for Green IT as moving to the cloud allows companies to reduce their IT infrastructure (Marston et al, 2011). This reduction in infrastructure means a smaller energy footprint leading to less direct energy consumption by consumers of cloud computing. However they are offloading some of this energy consumption to the cloud provider. It is in the interest of the cloud provider to keep their energy costs as low as possible so a properly managed cloud infrastructure should include powering off idle nodes (Deboosere et al, 2012) which would lead to a net decrease in energy used. It is worth noting that powering off idle nodes can affect the speed of elasticity in the cloud and it is a trade-off that cloud providers must decide for themselves.

2.5.6 End users

Gupta et al (2013) stated that convenience and ease of use are the main benefits of cloud computing cited by end users.

2.6 Barriers to Adoption

Seventeen journal articles were identified for this section of the review that discussed barriers to adoption. The seventeen articles are listed in appendix A. Each of these barriers is discussed in this section. It is a coincidence that the number of barriers is equal to the

number of articles; Armbrust et al's (2010) list of ten barriers certainly inflate the list of barriers.

The table below shows how often each barrier is mentioned in the articles with security and privacy mentioned in all seventeen articles. This shows the relative importance that the literature attributes to each of the barriers. Of the five items that were only mentioned once, four of them were mentioned by Armbrust et al (2010) and it seems that getting to the nice round number of ten barriers may have influenced the authors of the paper.

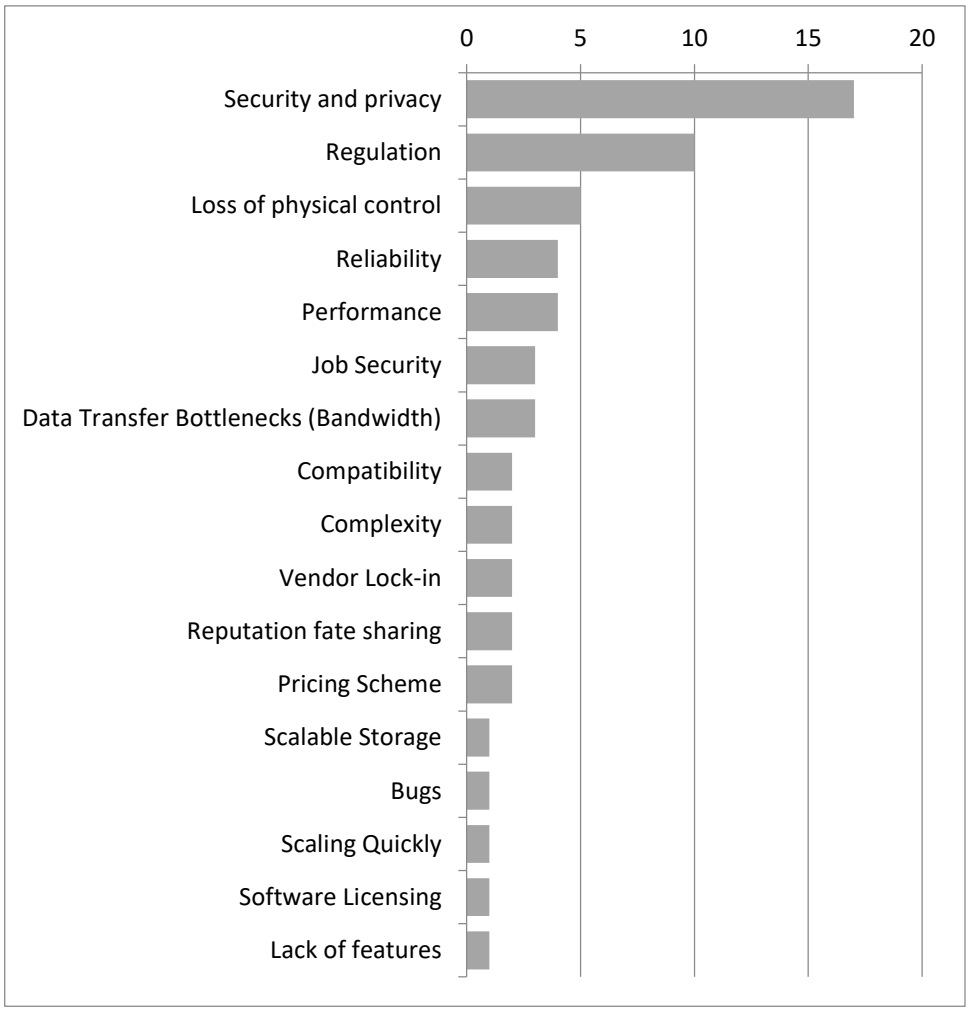

Figure 2: Ordered list of barriers

The barriers are discussed below and are presented in the order of number of mentions in the seventeen articles surveyed, with those mentioned more often being higher in the list.

2.6.1 Security and Privacy

Study after study cites security as the over-riding concern of cloud computing adoption; the fear of public disclosure of sensitive data presents an unsurmountable concern to many companies. However, most companies also admit that the controls around the security of

cloud computing are just as good as any company (Daylami, 2015). It is worth noting that it is often in the best interest of cloud service providers to not publicise vulnerabilities (Iovan and Iovan, 2016). Insecurities and vulnerabilities in the cloud platform can lead to compromises and malicious insiders can enable unauthorised access to the private systems of companies (Singh and Chatterjee, 2017). Even home users are concerned that their data could be mined and shared with other companies (Yang and Lin, 2015). In many cases it is actually more secure to be in the cloud as SaaS companies will install software patches on their systems as soon as they become available. There are two types of attacks that users of software can be exposed to: undirected and directed. Undirected attacks are typically self-propagating malware that seek out specific vulnerabilities whereas directed attacks occur when a particular target is the subject of the attack (August et al, 2014). All of the seventeen articles used in this study mentioned security as a concern, despite cloud providers having even more robust controls around security than most other companies. The literature is in firm agreement that the number one issue with cloud adoption is security. It seems that companies need to be persuaded that the security of the cloud is excellent and represents no additional risk over on-premise solutions and, in some cases, it may be even stronger.

2.6.2 Regulation

More than half of the papers surveyed, 59% (10 of 17), mentioned regulation as a major barrier to cloud adoption.

Due to its amorphous character, once data has been uploaded to the cloud, owners of the data can no longer be sure where their data is being stored. This can lead to issues with regulatory compliance (Marston et al, 2011). Data can also travel from one location to another so different laws can apply in different jurisdictions (Singh and Chatterjee, 2017). Some companies even outsource storage to other companies, who then outsource it again, in effect the data is re-re-outsourced and there is no limit to the amount of re-outsourcing that could be done (Jiang et al, 2015). EU law has determined that any disagreements between a cloud service provider and a customer will be under the jurisdiction of the country where the cloud service provider is headquartered (Haibach, 2015). Cloud Service Providers (CSPs) can, and should, allow companies to choose what country their data is stored in which will allow them to comply with laws and regulations. Jiang et al (2015) have developed an algorithm that can be used to verify that data is not being outsourced, CSPs should disseminate this algorithm to their customers so that they can be reassured that their data is stored where it is supposed to be stored.

2.6.3 Loss of Physical Control

The next most mentioned barrier is the loss of physical control. It was mentioned in almost 30% (5 of 17) of the articles.

Administrators will find the nature of their work changing; now that they no longer own the hardware, they will be relegated to opening support calls with the cloud service provider and waiting for them to fix the problem (Khajeh-Hosseini et al, 2012). It is quite possible that this would not present too much of an issue as many applications and services currently supported by administrators are actually supported by third parties who resolve issues on behalf of the administrators.

2.6.4 Reliability

Reliability is tied in fourth place with performance each mentioned in almost 25% (4 of 17) of the surveyed articles. Reliability and performance could almost be said to be two sides of the same coin.

Companies, especially large companies, are wary of entrusting mission critical applications to the cloud, despite cloud service providers offering uptime that is in excess of what is usually delivered by in-house IT staff due to the media attention that any cloud downtime attracts (Marston et al, 2011).

Reliability and performance are each mentioned in four of the papers for a total of eight mentions. Interestingly seven of the eight mentions occur in papers that are five years old or more despite these older papers being just 41% (7 out of 17) of the papers surveyed; this seems to indicate that newer papers are much less concerned with these issues likely due to technical improvements in the technologies of cloud computing.

2.6.5 Performance

Performance is tied in fourth place with reliability each mentioned in almost 25% (4 of 17) of the surveyed articles.

Network and disc input/output saturation can lead to poor or unpredictable performance thereby causing frustration amongst end users (Armbrust et al, 2010).

Performance is also discussed in the section 2.6.4 above.

2.6.6 Job security

Job security is tied for fifth place with mentions in 18% (3 of 17) of the surveyed articles.

The cloud represents a threat to IT departments; they will need to change the way they work and it may lead to some redundancies and job losses (Marston et al, 2011). IT staff can spend up to 80% of their time on maintaining systems (Ghormley, 2012) so moving those systems to the cloud could leave many IT staff idle, or their job could involve waiting for cloud service providers to look into issues, which leads to further issues of support. Users cannot contact Microsoft or Google and ask them to prioritise their issues as they could with an internal IT team (Khajeh-Hosseini, 2012). One study determined that 60% of IT staff resisted cloud computing due to fear of job loss. Of the remaining 40%, 15% did not understand cloud computing and the remaining 25% thought that it was just being used for storage (Raza, 2012).

Raza (2012) seemed to have a particular agenda with regards to job losses; according to the research in that paper, those that do not fear losing their job are too ignorant to realise that their redundancy is imminent. The author is figuratively foaming at the mouth in their desire to persuade the reader that this is the case. It is certainly true that IT departments will need to work differently but it is difficult to envision the future presented by Raza (2012) of wholesale redundancy of IT staff.

2.6.7 Data Transfer Bottlenecks

Data Transfer Bottlenecks is tied for fifth place with mentions in 18% (3 of 17) of the surveyed articles.

It is well known that data continues to grow and proliferate year-on-year. When using cloud computing, all of that data has to be transferred to the cloud leading to very high bandwidth costs as terabytes of data need to be uploaded (Armbrust et al, 2010). The cost of bandwidth has decreased in recent years and this is becoming less of a concern. Of the 3 mentions of Data Transfer Bottlenecks, 66% of them occurred at least five years ago. As with performance and reliability, data transfer bottlenecks are becoming less of a concern due to improvements in technology.

2.6.8 Compatibility

Compatibility is in joint sixth place with five other barriers, each mentioned in 12% (2 of 17) of the surveyed articles.

Companies are concerned about their existing applications working seamlessly with cloud applications. This is especially a concern for the banking and aerospace sectors as they have very robust systems and the uncertainties surrounding the cloud present a strong risk for these applications (Lin and Chen, 2012).

Some companies, especially smaller companies, do not have the in-house expertise to ensure successful integration of their existing applications to the cloud infrastructure (Oliveira et al, 2014).

It is always an issue for companies whether or not they will have compatibility issues with new software and software upgrades. It is simply not feasible to expect companies to always remain using the same software. Therefore, this may not be quite as strong a barrier as the research suggests.

2.6.9 Complexity

Complexity is in joint sixth place with five other barriers, each mentioned in 12% (2 of 17) of the surveyed articles.

The complex nature of the cloud and its many moving and interoperable parts can represent difficulties in adoption. If there is an issue it can be difficult to assign responsibility to a particular component or vendor as they will frequently assign blame to each other (Lin and Chen, 2012). Complexity in IT solutions is not unique to cloud computing but the literature does acknowledge that the cloud increases the complexity.

2.6.10 Vendor Lock-in

Vendor lock-in is in joint sixth place with five other barriers, each mentioned in 12% (2 of 17) of the surveyed articles.

Due to the many proprietary systems involved in cloud computing, there is a fear that companies will become entangled with particular vendors and will be at their mercy in terms of price increases (Marston et al, 2011). This could lead to vendor lock-in even though cloud computing is purported to reduce vendor lock-in.

This should be higher in the list as it is a strong concern for companies; high switching costs could wipe out any savings made by cloud computing.

2.6.11 Reputation Fate Sharing

Reputation Fate Sharing is in joint sixth place with five other barriers, each mentioned in 12% (2 of 17) of the surveyed articles.

Companies could be affected by the bad behaviour of other companies that happen to share the same hardware. For example, if the authorities seized some hardware, innocent bystander companies could suffer due to sharing hardware (Armbrust et al, 2010). Cloud

computing solutions often advertise a free trial period which allows hackers to set up systems, free of charge, and use them to attack other companies via denial of service attacks from the cloud infrastructure or setup up servers to send spam mail (Singh and Chatterjee, 2017). These attacks could lead to IP addresses or even entire IP ranges being blacklisted.

2.6.12 Pricing Scheme

Pricing Scheme is in joint sixth place with five other barriers, each mentioned in 12% (2 of 17) of the surveyed articles.

A cloud service provider's pricing scheme may change at any time which can lead to uncertainty (Maresova et al, 2017) and even more expense associated with migrating to a different provider.

It is an exaggeration to say that a cloud service provider could change their pricing scheme overnight as their pricing is agreed by contract, with a fixed duration. Once the contract is due for renewal, the provider could increase their price and if they have strong vendor lock-in the customer will have no choice but to pay the increased price but it would be bad for business as any customer that felt extorted would be immediately planning their migration to a different provider.

2.6.13 Scalable Storage

Scalable Storage is mentioned in just 6% (1 of 17) of the surveyed articles. It is in joint last place with four other barriers.

Storage does not offer scalability in the same way that CPU and memory do; this leads to challenges surrounding availability of data (Armbrust et al, 2010). CSPs have complex storage solutions designed to make their data as highly available as possible. This may not be as important a barrier as Armbrust et al (2010) would have us believe, although it is worth noting that this may have been more of an issue in 2010 when this barrier was identified.

2.6.14 Bugs

Bugs are mentioned in just 6% (1 of 17) of the surveyed articles. It is in joint last place with four other barriers.

Removing errors in large scale distributed systems can be very challenging and difficult to troubleshoot as the bugs may only appear at large scales which means that debugging can only be carried out on large scale systems (Armbrust et al, 2010).

All software has bugs to some degree. This is certainly not a problem that is unique to cloud computing. It seems that Armbrust et al (2010) may have been running out of ideas by the time they came up with this one.

2.6.15 Scaling Quickly

Scaling quickly is mentioned in just 6% (1 of 17) of the surveyed articles. It is in joint last place with four other barriers.

Computers that are idle use less power than busy computers and should be powered down in order to conserve energy. This can be problematical as rapid scaling needs computers to already be available and booted and scaling up will be delayed if computers need to be powered on first (Armbrust et al, 2010). This is mentioned in section 2.5.5 (Green IT) and although it is a challenge for cloud service providers it can hardly be mentioned as a barrier to adoption. If a company requires rapid scaling then they will have it built into their contract with their cloud service provider.

2.6.16 Software Licensing

Software Licensing is mentioned in just 6% (1 of 17) of the surveyed articles. It is in joint last place with four other barriers.

A lot of software has been written that restricts the computers that it can be run on. This can cause issues in a cloud environment as rapid scaling leads to machines being created and destroyed multiple times (Armbrust et al, 2010). This is the last of Armbrust et al's (2010) ten barriers to cloud computing and, once again, it does seem that Armbrust et al (2010) really wanted to get to ten barriers, no more and no less. Software licensing can hardly be seen as a major barrier to cloud computing adoption; software licensing can be quite intricate and it is certainly not a problem that is unique to cloud computing.

2.6.17 Lack of Features

Lack of Features is mentioned in just 6% (1 of 17) of the surveyed articles. It is in joint last place with four other barriers.

Some cloud applications do not have the same functionality as their locally installed counterparts (Aljabre, 2012) leading to user frustration. It is interesting that this potential

barrier was not mentioned more often in the surveyed papers as many cloud offerings do not offer the same functionality. It could be supposed that this does not represent a major barrier as companies would rarely use the full functionality of every product and those users that require advanced functionality not available in the cloud version could be given an offline fully featured version of the SaaS application.

2.7 Factors Affecting Adoption

Most academic papers around adoption used the Technology-Organization-Environment (TOE) framework or the Diffusion of Innovation (DoI) theory. The TOE framework is considered to be an extension of the DoI theory (Ray, 2016). According to the Diffusion of Innovation theory, it can take from 8 to 15 years for technology to be fully adopted. Innovations are easier for larger companies because they can support the expense but the technology is more valuable for smaller companies. Interestingly, one of the main drivers for adoption is whether or not competitors have adopted; the more companies that adopt the greater the need for more widespread adoption because of the risk non-adopters have of being at a competitive disadvantage (Utterbank, 1974). Despite this paper being very old, it is still quite relevant today as the theory is still being used to explain innovation adoptions.

There are three stages to adoption:

1. Generation of an idea: The initial stages of a new innovation involve identifying a need and a technology to satisfy that need.
2. Problem-solving or development: This stage involves designing the technical solution to the identified goals and the refinement of the solution.
3. Implementation and diffusion: The implementation stage is entered when a solution is brought to market and diffusion follows thereafter.

The implementation stage was entered in 2006 with the introduction of Amazons Elastic Compute Cloud. At the time of this writing, 11 years have passed which is certainly within the range of 8 to 15 years specified by Utterbank (1974) for full adoption.

The following factors, although they are neither benefits nor barriers, play a powerful role on whether or not a company adopts cloud computing.

2.7.1 Relative Advantage

Relative advantage refers to the capabilities of the new innovation; if they are better than the current solution then companies are more likely to adopt the innovation. In situations where there is a relative advantage of cloud computing over the current system, adoption rates increase (Lin and Chen, 2012). Therefore if there are clear and unambiguous benefits

to strategic or operational effectiveness from cloud computing, adoption rates will be positively impacted (Oliveira et al, 2014). It may seem obvious, but put simply: if the new solution is not better and/or cheaper it will not be adopted.

2.7.2 Observability

Observability refers to the visibility of successful implementations of new innovations. High observability of successful cloud computing solutions leads to increased adoption rates (Lin and Chen, 2012). This must be especially true of competing companies; highly successful, highly observable, cloud adoptions by competitors, which in turn lead to competitive advantage, must present a very strong rationale for cloud adoption.

2.7.3 Trialability

Trialability refers to whether or not companies can test an innovation before committing to an implementation. Trialability of cloud computing solutions leads to an increase in adoption (Lin and Chen, 2012). Of course, if a company can try out cloud computing at no cost or a low cost and see if it works for them, this would lead to wider adoption.

2.7.4 Technological Readiness

If there are already technologies in use in a company that can be replaced or be complemented by cloud computing solutions and there are specialised IT resources available to implement solutions, then a firm will have high technological readiness for cloud computing adoption (Oliveira et al, 2014). Utterbank (1974, p. 623) referred to these people as “technical gatekeepers”; they are the people that bring in the new technology and champion its use within a company.

2.7.5 Top Management Support

If top management recognise and support the benefits of cloud computing solutions, this will have a positive influence on cloud computing adoption as top management have the ability to direct the usage of resources and could direct those resources to cloud computing initiatives (Oliveira et al, 2014). Again, it does seem quite obvious but if management at the top level want the company to adopt cloud computing then it will certainly be adopted or there must be a very strong, very compelling, case against adoption.

2.7.6 Company Size

Larger companies have access to more resources and can take greater risks with trialling adopting innovations than smaller companies (Oliveira et al, 2014). It is interesting that the larger that a company is, the better its ability to adopt cloud computing whereas the smaller a company is the more it has to gain from adopting cloud computing.

2.7.7 Competitive Advantage

Adopting new technologies can often be the distinguishing factor between a company continuing to operate successfully and a company that fails. It can often be a strategic necessity as, if a company's competitors have all adopted a new innovation, the company must also adopt the new innovation or risk being left behind. One study found that the cost savings of cloud computing were an indirect reason for adoption as the cost savings had a direct effect on competitive advantage (Oliveira et al, 2014).

2.7.8 Regulatory Support

This refers to the impact that government regulations can have on the adoption rates of new technologies. Regulatory support will increase the rate of cloud computing adoption (Oliveira et al, 2014).

2.8 Cloud Service Providers

Once a company has decided to adopt cloud computing they must then chose a Cloud Service Provider (CSP). This section identifies the key activities of CSPs and gives an outline of the strategies available to CSPs.

2.8.1 Four Key Activities

The four key activities of CSPs that have been identified are (Califf et al, 2016):

1. They use their experience to analyse business models
2. They build custom cloud solutions to meet the business needs of their customers
3. They provide support to their customers
4. They collects fees from their customers

2.8.2 Four Key Strategies

From the perspective of the provider, it is very important to have high lock-in as a way of retaining clients; the more difficult, and costly, it is for clients to switch service, the less likely they are to do so. Four strategies for providers are identified (Wang and He, 2014):

1. Low cost and hassle free: This strategy competes on ease of use and low price. This has low lock-in and a low degree of meeting business requirements.
2. Superior quality and features: This strategy competes by having more and better features than their competitors. This strategy has high lock-in and a low degree of meeting business requirements.
3. Customisation: This strategy competes on customising the solution to meet the specific needs of a customer. This strategy has low lock-in and a high degree of meeting business requirements
4. Value Co-Creation: This strategy involves working closely with a customer and both companies developing a tailored solution just for the customer. This has high lock-in and also a high degree of meeting business requirements.

The strategy of value co-creation is recommended for late entrants to the cloud computing market as it allows providers to form partnerships with customer companies that are mutually beneficial. This approach leads to high lock-in as it involves heavily customising the cloud offering which means that it would have a very high switching cost.

Conversely, providers clearly need to be able to demonstrate to potential customers that switching service is easy and hassle-free in order to better attract customers to their service as lock-in has been identified as a reason against cloud computing.

The key challenge for providers is to actually have high lock-in while at the same time making it seem like they have low lock-in.

3. **Methodology and Fieldwork**

3.1 Introduction

This chapter describes some of the various types of relevant research methodologies considered for use in this paper. Grounded Theory was chosen for this study due to its compatibility with the goals of this research. A full explanation of all of the options that led to this decision is given in this chapter, along with a justification for the choice of Grounded Theory method.

3.2 Purpose of this research

This research seeks to assess the attitudes of IT professionals to cloud computing with a specific focus on barriers to adoption. This is an exploratory study to elicit the views, perception, interpretations, and understandings of the participants. An exploratory study allows the researcher to ask open-ended questions in order to gain insights into the topic (Saunders et al, 2016).

3.3 Research Philosophy

This section explores and describes the philosophies available to researchers. The three main philosophies are objectivism which is also known as positivism, constructionism which is also known as interpretivism, and Realism. This document uses objectivism and constructionism to describe the philosophies however the other terms, objectivism and interpretivism are also used.

The components that make up a philosophy are individually discussed before being combined in a table that outlines the choices that make up each philosophy.

Research can be broadly divided into two categories: qualitative, and quantitative. Bryman (2012, p. 35) gives a very succinct definition of the two categories that also highlights the difference between them: “Quantitative researchers employ measurement and qualitative researchers do not”. Quantitative research is usually numeric while qualitative research is usually non-numeric (Saunders et al, 2016).

3.3.1 Ontological Assumptions

Ontology is concerned with assumptions surrounding the nature of reality and has two main positions: Objectivism and Subjectivism (Saunders et al, 2016). Objectivism and Subjectivism are often described as polar opposites where taking one of the positions

automatically rules out the other one. A third position, Realism, attempts to combine elements of both main positions (Matthews and Ross, 2010).

Objectivism holds the position that social objects and categories exist independently of social actors (Bryman, 2012) and that they are unaffected by the experiences and interpretations of social actors (Saunders et al, 2016).

Subjectivism, also known as constructionism, holds the position that social objects and categories are only real in the sense that they are constructed ideas that are constantly being worked upon by social actors (Matthews and Ross, 2010).

Realism accepts that there is a reality that can be known through the senses but also that there are hidden mechanisms present that have an observable effect on reality despite these mechanisms being undetectable by the senses (Matthews and Ross, 2010).

3.3.2 Epistemological Assumptions

Epistemology refers to the assumptions of what constitutes acceptable, valid, and legitimate knowledge (Saunders et al, 2016). There are three main epistemological positions: positivism, interpretivism, and realism.

Positivism is an epistemological position, developed from the ontological position of objectivism (Matthews and Ross, 2010). It has the following features (Bryman, 2012):

- Only knowledge that is confirmed by the senses qualifies as acceptable knowledge
- The purpose of theory is to generate and test hypotheses
- Knowledge is generated by gathering facts
- Science must be conducted in a way that is objective
- Belief that scientific statements can be distinguished from normative statements as normative statements cannot be confirmed by the senses

A positivist approach typically means that quantitative data are collected and a large data set is often used.

Interpretivism is an epistemological position that can be linked to the ontological position of subjectivism (Matthews and Ross, 2010). It is an alternative to positivism and holds the viewpoint that people are different to objects and a strategy is required that allows for a subjective approach (Bryman, 2012). It has the following features (Matthews and Ross, 2010):

- People’s interpretations and understandings qualify as knowledge
- Differing perspectives can be explored

- The researcher interprets other people's interpretations and attempts to view the world from the viewpoint of those being researched
- The researcher generates theory in an inductive manner from the gathered research

An interpretivist approach means that qualitative data are collected.

Realism is an epistemological position that has two major forms: Empirical Realism and Critical Realism. Empirical Realism states that reality can be understood; for this reason it is also known as naïve realism because it is assumed by realists that there is perfect correspondence between reality and the terms used to describe it. Critical Realism recognises that there is a distinction between reality and the terms used to describe it (Bryman, 2012). Realism involves gathering quantitative and/or qualitative data (Matthews and Ross, 2010).

3.3.3 Table of Philosophies

The table below summarises the different philosophies:

	Objectivism	Constructionism	Realism
Ontology	Objectivism	Subjectivism	Realism
Epistemology	Positivism	Interpretivism	Realism
Theory	Deductive	Inductive	Abductive
Data Sources	Quantitative	Qualitative	Mixed Methods

Table 1: Overview of Philosophies

Saunders et al (2016) also mention a fourth philosophy called pragmatism. Pragmatism is led by the problem and values practical solutions. Pragmatism is similar to realism in that mixed methods are recommended.

3.3.4 Philosophy of this Research

The philosophy selected for this study was largely defined by epistemological assumptions. This study is seeking to determine the attitudes of IT professionals; therefore, people's interpretations and understandings will qualify as knowledge. Inductive research will be undertaken as the literature review has clearly demonstrated that the barriers to cloud computing are both well-known and well-represented in the literature meaning that deductive research can be answered by the literature alone. Inductive research will allow

for a deeper understanding of the attitudes of IT professional towards cloud computing barriers and allow for theory building and generation. It may even present new information that is unknown in the literature, for example, a new barrier unrepresented in the literature may become apparent. This leads to qualitative research being the most suitable data source as opinions are non-numeric.

For these reasons, the most logical choice of research philosophies for this research is the philosophy of constructionism.

3.4 Research Approach

There are two main types of research approach: deductive and inductive. With deductive theory development, the theory guides the research (Bryman, 2012). This means that a theory is hypothesized and then research is developed that will either prove, or disprove the theory. Inductive theory development is developed in the opposite direction: theory is an outcome of research (Bryman, 2012). The research is carried out and then theories are formed based upon the results of the research. There is a third type of research theory development that combines the deductive and inductive approach. This is known as an abductive approach and allows the researcher to move back and forth from theory to data (Saunders et al, 2016).

3.5 Research Strategy

Saunders et al (2016) identify eight research strategies:

Experiment	Research that measures the impact of one variable on another.
Survey	Research that involves the collection of standardised data, often via questionnaire.
Archival and documentary research	Research conducted through the use of archives and documents including textual, visual, and audio sources.
Case study	Research into a topic in its real-life setting.
Ethnography	Research into the culture of a group.
Action research	An iterative process that uses a collaborative approach to solve real organisational problems.
Grounded theory	Research that inductively develops a theory from a set of data
Narrative inquiry	Research that collects the experiences of participants' as complete stories rather than pieces of data

Table 2: Research Strategies

The first two strategies, experiment and survey, were not considered for this research as they are both concerned with quantitative research.

Archival and documentary research, ethnography, and narrative inquiry were deemed not suitable for this research.

Grounded theory was chosen over case study and action research as it provides the best integration with the chosen research philosophy given its strong emphasis on inductive research.

Grounded theory is an emergent process that consists of conducting qualitative interviews. It is emergent in that theory is developed inductively from the gathered data. The data is analysed as it is being collected in order to develop theories to analyse the data (Cooper and Schindler, 2013). This leads to the development of a theory that is grounded in the data (Saunders et al, 2016).

3.6 Research Choices

This research is using a mono-method approach which means that only one research instrument will be developed. The instrument used will be an interview schedule. There are two types of interviews that can be used to collect qualitative data: unstructured interviews, and semi-structured interviews (Bryman, 2012).

Unstructured interviews usually consist of a list of topics to be discussed, known as an interview guide. This is typically informal and the phrasing and order of the topics can vary from interview to interview (Bryman, 2012).

Semi-structured interviews consist of a series of questions, known as an interview schedule, to be asked. The interviewer can ask follow-up questions to replies that are seen as significant. The sequence of the questions can be varied from interview to interview (Bryman, 2012).

Semi-structured interviews were chosen for this research due to the flexibility offered. Although unstructured interviews offer even greater flexibility, semi-structured interviews allow for a specific list of questions to be asked, that can be varied or some questions can even be omitted entirely. The literature review revealed that there are specific cloud adoption barriers that are known so these can be asked about directly in a semi-structured interview while allowing the possibility of participants identifying barriers that were undiscovered during the literature review.

3.6.1 Development of the Instrument

The instrument used for this study was an interview schedule that was used for the semi-structured interviews. The interview schedule was developed as a direct result of the findings of the literature review. All of the identified barriers were included in the interview schedule.

3.7 Time Horizon

Saunders et al (2016) identify two time horizons that can be chosen during research: cross-sectional and longitudinal. A cross-sectional time horizon involves the research being taken at a particular time. Saunders et al (2016, p. 200) describe this as a “snapshot”. They go on to describe that a longitudinal time horizon consists of a series of snapshots that they label as a “diary” approach.

Due to time constraints, the time horizon of this research is cross-sectional, although it would be interesting to see how the attitudes of IT professionals towards cloud computing adoption barriers change over time, possibly two-to-three years into the future.

3.8 Data Collection and Analysis

This study uses the Grounded Theory Method to collect and analyse the data. Specifically, the variety of Grounded Theory Method proposed by Charmaz (2006) is used. This involves three main steps:

1. Initial Coding
2. Focussed Coding
3. Grounded Theory

Initial coding is the process of developing codes for each unit of data to categorise the data. Focussed coding involves re-coding the initial coding data into fewer, more focussed, codes. Finally, grounded theories are developed from the data.

3.9 Population Sampling

The target population for this study is IT professionals that are experienced, informed, and a part of the IT decision making process.

There are two types of sampling: probability and non-probability. Within each of these two types of sampling, there are various techniques available. For example, simple random sampling or systematic random sampling in the case of probability sampling and quota sampling or snowball sampling in the case of non-probability sampling. It is beyond the

scope of this document to give an overview of the many different types of sampling techniques available but an overview will be given for the chosen sampling technique.

Probability sampling is used when a sampling frame is available, non-probability when a sampling frame is not available. A sampling frame is a complete list of all of the cases in the target population (Saunders et al, 2016). There is no sample frame available that contains all of the IT professionals that are experienced, informed, and a part of the IT decision making process so non-probability sampling has been chosen for this research.

The selected sampling technique has been informed by the research strategy. Purposive sampling, also known as judgemental sampling, is a technique whereby the judgement of the researcher is used to select the sample based upon which cases will make the best contribution to the research. A particular form of purposive sampling, theoretical sampling, is used when grounded theory is being used as a research strategy. Theoretical sampling involves selecting participants as they are needed, chosen purposively by the requirements of the emerging theory (Saunders et al, 2016).

The sample size will be increased until data saturation is reached. Data saturation is reached when additional interviews no longer add further valuable information. Typically data saturation is reached after approximately twelve interviews (Saunders et al, 2016).

3.10 Access

Access refers to the ability of researchers to access sources that can enable them to collect data. There are two types of access: traditional access, and internet mediated access. Traditional access involves gaining physical access via face-to-face meetings, telephone conversations, correspondence by post, or travelling to data archives. Internet mediated access uses computing technologies to gain virtual access to conduct research (Saunders et al, 2016). This research is composed of face-to-face interviews so the access type used is traditional access.

Saunders et al (2016) identify three levels of access: physical access, continuing access, and cognitive access. Physical access usually involves getting the permission from a company gatekeeper to perform research. Continuing access recognises that the research is unlikely to be a one-time event and further visits may be required on a continuing basis. Cognitive access refers to the potential issue of permission being granted by a gatekeeper but the desired participants also need to agree to become participants in the research.

Researchers can either be external, or internal to the organisation or group being researched. An external researcher has no prior contact with the organisation or group, and will need to negotiate every level of access. Internal researchers are usually members of

the organisation or group that is being studied and may still have challenges with gaining all three levels of access (Saunders et al, 2016). This research will be conducted by an internal researcher.

3.11 Reliability and Validity

Reliability refers to how consistent the research findings are and whether a different researcher would achieve the same findings if they carried out the same research with the same design. Validity refers to whether or not the research method measures what it set out to measure (Bryman, 2012). Taken together, reliability and validity measure the quality of the research.

However, the tools used to measure reliability and validity are used in quantitative research and are not always applicable to qualitative research as they are based on positivist assumptions (Saunders et al, 2016). Triangulation can be used as a qualitative tool to help ensure reliability and validity. Triangulation involves using a mixed method approach (Greener, 2008). This study is using mono-method qualitative research so it will use a technique called respondent validation to ensure reliability and validity. Respondent validation involves providing each participant with an account of the interview so that they can verify that their views are accurately represented (Bryman, 2012).

3.12 Method Limitations

The primary limitation of the Grounded Theory Method is that there is a possibility that there could be nothing important or interesting discovered at the end of the research process (Saunders et al, 2016).

3.13 Justification of Selected Method

Grounded Theory Method was chosen for this research for three main reasons:

1. It allows for emergent research approach. This is relevant to this research because of the findings of the literature review; the literature contains a wealth of information about cloud computing adoption barriers but few theories regarding the attitudes of IT professionals towards these barriers were proposed.
2. It offers a holistic approach to research and provides a strong framework from strategy to data analysis.
3. The version of Grounded Theory propounded by Charmaz (2006) offers a large degree of flexibility while at the same time providing a strong framework.

3.14 Research Ethics

Ethics refers to the application of morals to the behaviour of the researcher; ethical behaviour can be characterised as being “fair, just, and acceptable” (Zikmund et al, 2009, p. 88). There are four main categories of research ethics transgressions (Bryman, 2012):

1. Harm to participants
2. Lack of informed consent
3. Invasion of privacy
4. Deception

This research will not breach any of the categories mentioned above as it will not cause harm to any of the participants, all participants are requested to read and sign an informed consent form, no participant will be identifiable from the data collected, and no participants will be deceived as part of this research. A copy of the informed consent form is included in Appendix B. This form was signed by all participants.

Ethical approval was sought for this research from the Ethics Committee of the School of Computer Science and Statistics at Trinity College Dublin. This approval was granted prior to arranging any of the interviews. The approval application form sent to the ethics committee is also included in Appendix B.

3.15 Lessons Learned

There were two main lessons learned during the writing of this dissertation; firstly, a book about thesis writing should have been read at the beginning of writing rather than in the middle, and, secondly, start the ethics approval process as soon as possible.

4. Findings and Analysis

4.1 Introduction

This chapter outlines and analyses the findings of the conducted research. As discussed in the previous chapter, Grounded Theory is used to analyse the data. The method proposed by Charmaz (2006) is used; this method heavily stresses the flexibility of the method.

A detailed description of the research methodology is provided, including a description of the interview process itself and how the data was analysed. Details regarding the participants follow, including a description of their roles and how they influence the IT decision making process.

This is followed by an in-depth reporting and analysis of the data.

4.2 Research Methodology

As outlined in the previous chapter, semi-structured interviews were used as the research instrument. The interview questions schedule that was used in each interview is reproduced in Appendix C.

These interviews were conducted in person and a total of twelve interviews were conducted. All of the interviews were conducted in a private meeting room with only the participant and researcher present. Seven of the interviews took place in Dublin and the remaining five were conducted in Cork. Each interview began by reading the Participants Information Sheet aloud to each participant and asking them to read and sign the Informed Consent Form which the researcher then signed in their presence. All participants were given a copy of both the Informed Consent Form and the Participants information sheet. The participant was then shown a list of the identified barriers and a description of each barrier was given. The participant was then informed that the recording would begin, before the recording device was placed on the table in front of the participant where it remained for the duration of the interview. The recording device used was a smartphone running an application called “Voice Recorder”.

Participants were asked a series of questions regarding their opinions on cloud computing adoption barriers and there were also some follow up questions. The follow-up questions that were asked during the interview were not planned in advance but were in response to the participants’ own responses. This gave a dynamic aspect to the interviews that caused a number of unique questions to be developed during the interviews. The interview questions schedule was used and each participant was asked the main questions, but the sub-questions were not strictly adhered to in all cases.

Upon completion of the interview, the recording device was switched off in view of the participant. The participant was then offered a debriefing on cloud computing in general, and cloud computing adoption barriers specifically. Participants were also encouraged to ask any questions pertaining to the interview and the research. This debriefing session lasted longer than the actual interview in every case. Seven of the participants commented that they found the interview to be an enjoyable experience and that it encouraged them to examine their own opinions on cloud computing adoption barriers more deeply than they ordinarily would have.

A transcript of each interview was written, and each participant was emailed the transcript of their interview and asked to confirm whether or not their opinions were accurately reflected in the attached transcript. Not all participants responded to this email, but the four that did respond, responded positively. A copy of the email sent to each participant is also reproduced in Appendix C.

The interviews were then manually coded. No computer software was used to aid the coding and analysis process. *In vivo* codes were generated during the initial coding process. *In vivo* codes are words or phrases that are used by the participants themselves (Charmaz, 2006). After completing the initial coding, focussed coding was conducted. Focussed coding revealed six broad themes that were visible as common trends throughout the interviews; each of these six focussed codes was also developed as *in vivo* codes. Each of these six focussed codes is discussed in this chapter. Finally, grounded theories were developed, that is theories that are grounded in the data.

4.3 Participants

Participants were selected for their experience and for their ability to influence the IT decision making process.

The order in which the participants are listed below is the order that they were interviewed; participants were not interviewed in any special order. The interview order was decided by convenience and the availability of the participant.

The “participant” column on the left of the table below contains a three letter code that is used to refer to each participant in the sections below when the participant is mentioned or quoted. The code will appear within parentheses in the text.

The table below outlines the role and experience of each participant.

Participant	Role	Experience	Date of Interview
SA1	Security Architect	15 years	9th June 2017
SC1	Security Consultant	12 years	12th June 2017
PMM	Performance Monitoring Manager	43 years	12th June 2017
IM1	Infrastructure Manager	20 years	13th June 2017
SA2	Systems Architect	15 years	14th June 2017
IC1	Infrastructure Consultant	32 years	14th June 2017
IC2	Infrastructure Consultant	20 years	15th June 2017
IA1	Infrastructure Architect	22 years	15th June 2017
SA3	Systems Architect	16 years	21st June 2017
SC2	Security Consultant	15 years	22nd June 2017
IC3	Infrastructure Consultant	15 years	22nd June 2017
SDM	Service Delivery Manager	18 years	22nd June 2017

Table 3: Research Participant's roles and experience

As the table above shows, the participants in this study are experienced, with their experience ranging from 12 to 43 years. The average experience is just over 20 years. All of the participants heavily influence the IT decision making process from a technical perspective and are relied upon to design and build IT solutions and would all be considered technical gatekeepers (Utterbank, 1974).

The list below gives an outline of each of the roles of the participants.

Security Architect
Security Architects are responsible for designing the overall solution from a security perspective. Typically they will be presented with requirements and it is their decision to decide which components will be included in the design. Architects do not carry out the installations themselves but focus on the solution design.
Security Consultant
Security Consultants are responsible for fulfilling the vision of the Security Architects. They will frequently be consulted by the Security Architects about various aspects of the proposed solution; the Security Architect relies heavily on the Security Consultants while designing solutions, therefore the Security Consultants play a key influencing role when the Security Architect is considering implementing solutions in the cloud.
Performance Monitoring Manager
The Performance Monitoring Manager is responsible for all performance monitoring, both in the cloud and outside of the cloud. This role is a key influencer of cloud computing

adoption as all of the consultants will consult with the Performance Monitoring Manager when attempting to assess the performance of cloud solutions during proof of concepts.
Infrastructure Manager
The Infrastructure Manager is responsible for the entire company infrastructure. This role plays a strong influencing role regarding cloud adoption as the Infrastructure Manager needs to determine whether or not proposed solutions, including cloud solutions, can be integrated into the existing infrastructure.
Systems Architect
Much like the Security Architect, a Systems Architect is responsible for designing the overall solution. Typically they will be presented with requirements and it is their decision to decide which components will be included in the design. Architects do not carry out the installations themselves but focus on the solution design.
Infrastructure Consultant
Similar to Security Consultants, Infrastructure Consultants are responsible for fulfilling the vision of the Infrastructure and System Architects. They will frequently be consulted by the Architects about various aspects of the proposed solution; the Architects rely heavily on the Infrastructure Consultants while designing solutions, therefore the Infrastructure Consultants play a key influencing role when the Architects are considering implementing solutions in the cloud. The Infrastructure Manager would also heavily rely upon them when assessing all solutions, even those that are cloud based.
Infrastructure Architect
Much like the Security Architect and the Systems Architect, an Infrastructure Architect is responsible for designing infrastructure solutions. Typically they will be presented with requirements and it is their decision to decide which components will be included in the design. Architects do not carry out the installations themselves but focus on the solution design.
Service Delivery Manager
The Service Delivery Manager plays a key role as an advocate for the users of the solutions, ensuring that the user's needs are represented accurately in all designs and fulfilled in all solutions. This is an important role regarding cloud adoption as they could block the implementation of a cloud solution if they felt that it would not meet the needs of the users.

Table 4: Role descriptions

4.4 Data Coding

95 *in vivo* codes were developed during the initial coding of the interview transcripts. After analysing the codes, common trends were identified that were present in all of the

transcripts. Six main themes have been identified that encompass all of the interview questions and all of the participant responses. Focussed codes were developed for each of these six themes and each of the focussed codes has been labelled with a one word title to describe the overarching meaning behind the code. There is some slight overlapping of codes but, in general, they are quite distinct. The six focussed codes are:

1. Data
2. Implementation
3. Fear
4. Trust
5. Upskill
6. Inevitable

Each of these codes will be discussed in detail in this section. Although this series of interviews were collecting qualitative data, all participants were asked some questions that could be answered with either yes or no, before being asked open-ended questions to clarify their reasoning. Therefore, there is small amount of data that could be described as quantitative in nature. This quantitative data is included in the relevant section to further illuminate each theme.

4.5 Data

The primary concern of all participants revolved around the security of the data; their biggest concern with security as a barrier to cloud adoption centred on the data itself as it is the data that is at risk should a security breach occur. All participants recognised that there are different types of data, sensitive data and non-sensitive data with some data being more valuable than other data. The majority of the participants have no concerns about utilising the cloud for non-sensitive data. One participant (PMM) did have concerns about categorising data as sensitive or non-sensitive and felt that all data should be treated the same because “what you might perceive today to be something that’s not a security issue” may become a security issue in future as “things like that change in time”. The idea of the value of data changing in time was not mentioned by any other participants, nor was it represented in any of the literature but cloud providers, and cloud customers, should be cognisant of this as it represents a future risk to cloud adoptions.

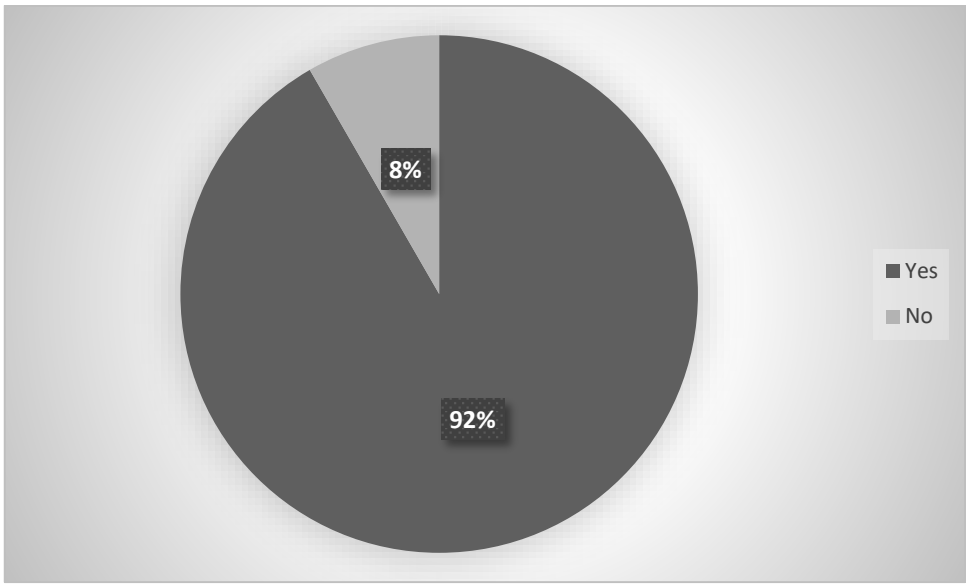

Figure 3: Would you adopt the cloud for non-sensitive uses?

All of the participants were aware of the new EU regulations that are due to be enforced in 2018, known as GDPR. These regulations offer protection for individuals and include the proviso that data owned by EU citizens should be housed within the EU (www.eugdpr.org, 2017). This means that location of data is a big concern for all participants when considering cloud adoption. The key concern is that there is no way to police the location of the data, effectively there is no way to prove that the data is located in the EU beyond the word of the provider. However, as one participant noted (SA2), “Microsoft are fully certified, the Azure, is fully certified for GDPR”, Azure being Microsoft’s cloud platform. This certification could offer false reassurance to customers of cloud computing solutions, including some participants of this study, as they think they can offload the responsibility of complying with GDPR to the cloud provider, however, under GDPR, it is the company that owns the data that is responsible for compliance with GDPR not the cloud provider themselves. If cloud providers could find a means of being able to prove to their customers that the data is located where they say it is located, effectively giving customers the ability to police the locations of the data, it would certainly negate this potential barrier. Kulkarni et al (2012) mention that it is very attractive to cloud storage brokers to de-risk their cloud storage by providing federated access to storage on the sites of partner companies. This would be invisible to their customers and could mean that the data is actually being stored in a different geographic location. Jiang et al (2015) offer a very complex algorithm that requests random pieces of files and then measures the network latency, the time taken to retrieve the data, as a means of detecting if data storage is being outsourced. It is only a matter of time before a commercial version of this algorithm is made available.

One participant (IA1) had concerns about data-in-transit, that is, data that is being migrated to a cloud provider. If there is a lot of data being migrated, cloud providers can ask for the data to be shipped to them on hard-drives which led this participant to be very concerned

about the security of the data while it was being moved to the cloud as they felt the data was not secure while being “transferred around on the back of a bike, or in a taxi”. This can only be remedied by increasing bandwidth substantially. This should be a concern for all customers of cloud computing as it could take weeks for extremely large amounts of data to be copied over existing bandwidth connections; this could mean that some of the data would be stale by the time the upload was completed.

Residual data was highlighted as a concern by one participant (PMM) who illustrated his concern by describing a disaster recovery scenario whereby a company needs to restore their data from backup. This participant was concerned about what would happen to the tapes and other equipment that was used to restore the data, that the data could remain on the tapes for many years before being accessed by a different company in the future as all of the customers of a cloud provider would be using the same disaster recovery equipment and “you could have an amalgamation or a cross-contamination of your data”. This is a very real risk and was not highlighted in the literature. Cloud providers should ensure that all of their disaster recovery processes cater for this risk of residual data. It is also something that customers of cloud computing should ensure that their selected cloud provider is aware of and has processes to deal with this risk.

Another item of concern regarding data was mentioned by several participants and that was that their ability to access their data over the internet, because it is in a cloud solution, means that other people could also potentially access their data, leading some participants to believe that the cloud will always have this as a security flaw as, if their data remains on-site, it cannot be accessed over the internet. Cloud providers will find this concern very difficult to mitigate; their only option is to ensure that their security is kept up to date.

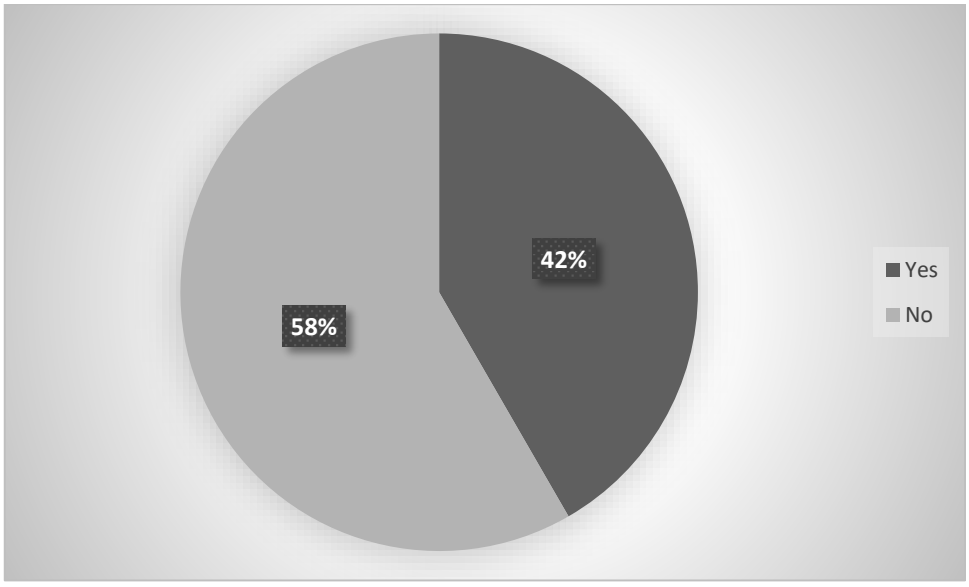

Figure 4: Would you adopt the cloud for sensitive uses?

In the above examples non-sensitive uses was deemed to be data that had less value; that did not contain financial data, medical data, or data that could identify individuals, whereas sensitive uses concerned data that did have those characteristics.

One participant (IC3) mentioned that jurisdiction of the data would be a concern, that if a company had migrated their data to the cloud, to an American company, Microsoft for example, that even though the data is physically located in Ireland, what would happen if the American Government wanted access to the data? A case was taken in 2013, by the US Department of Justice (DoJ) against Microsoft. The DoJ wanted to gain access to files that were held on a server in Dublin and Microsoft contested this claiming that because the servers were located outside of the US, the DoJ had no jurisdiction over the data. The court found in favour of Microsoft and said that "US warrant authority only extends to stored communications content (like emails) that are physically located in the United States". This was appealed and the original judgement was upheld (Daskal, 2017). It seems that this participant's concern is unfounded.

4.6 Implementation

This section details the concerns that participants' had concerning the barriers to the actual implementation of a cloud computing solution. Participants discuss their thoughts on cloud computing from a technical perspective; performance, reliability, and loss of physical control are the main topics discussed.

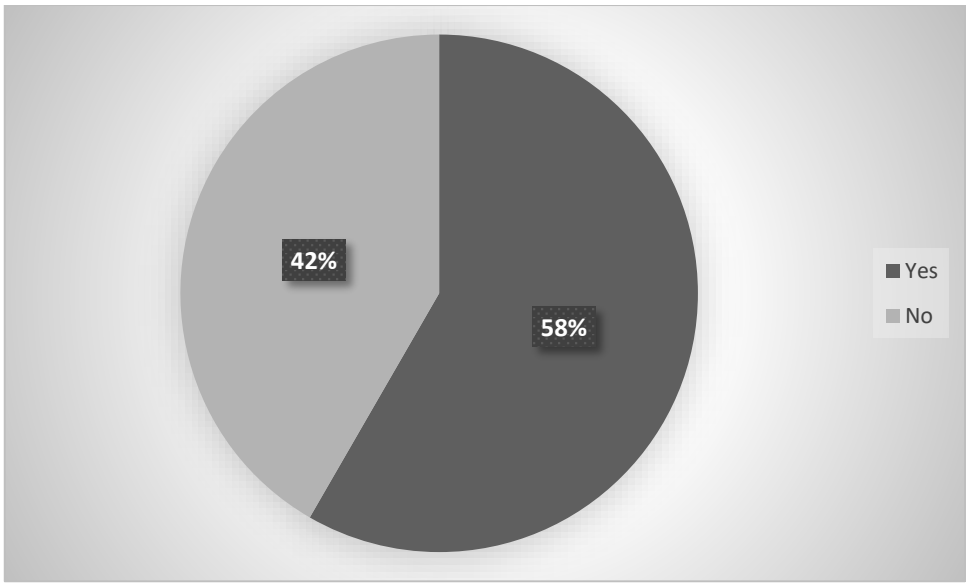

Figure 5: Are you concerned with performance?

When asked about performance, some participants said that they would be concerned and the rest said that they would not be concerned. However, whether the participant was concerned or not, they all felt that the cloud was capable of delivering performance, in some

cases even better performance than an in-house solution. Several participants highlighted the fact that a cloud solution can deliver excellent performance but it depends on the actual requirements regarding performance of the application as some applications are more sensitive to poor performance than others. One participant (SA1) summed it up: “that’s where proof-of-concepts come in”, stressing the need to fully test every aspect of the solution thoroughly prior to moving it into production, with the option to adopt a hybrid approach to a scenario where a fully cloud enabled solution was not good enough to satisfy requirements. The idea that cloud requirements should be clearly understood before embarking on a cloud journey is heavily stressed by Goutas et al (2016) and a proof-of-concept approach to cloud adoption would certainly expose any limitations or gaps in that understanding. Performance should be negotiated up-front with the cloud provider and Service Level Agreements (SLAs) should be put in place to protect the negotiated performance, with the cloud provider being subject to penalties should the SLAs not be met.

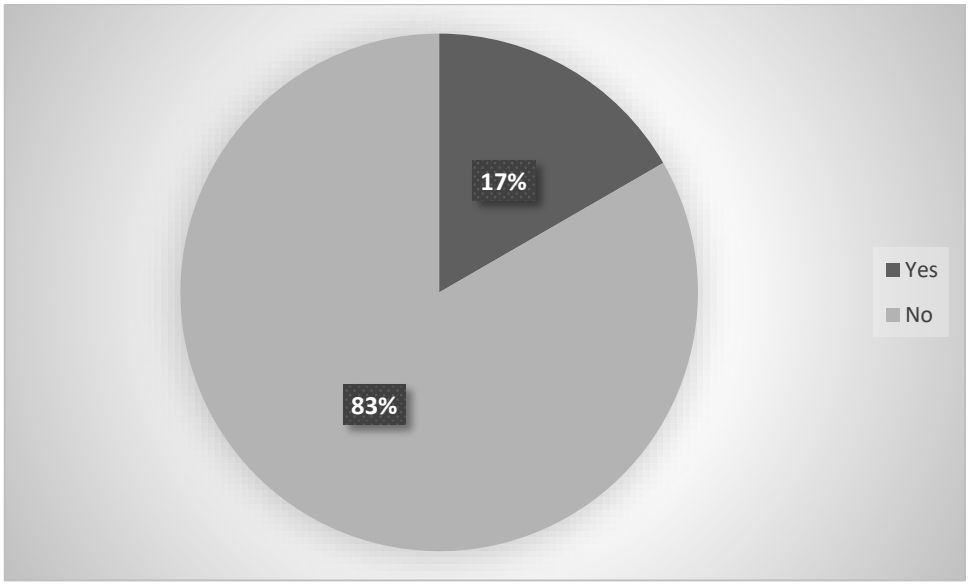

Figure 6: Are you concerned with reliability?

Almost all participants felt that the cloud was reliable, that cloud providers invested enough into their cloud infrastructure that reliability would not be an issue with some even stating that they felt that a cloud solution would be even more reliable than an in-house solution due to the greater investment in infrastructure that a cloud provider would be able to provide. One participant (IC1) noted that the reliability of the tools used to manage the infrastructure would be a concern as cloud providers “have a habit of changing dashboards overnight” and that the cloud management interface is subject to being changed at the whim of the provider. However, this participant was not concerned with the reliability of cloud computing as a solution. This is an important point and providers should be aware that when users become comfortable with using their software, radical changes can cause confusion even amongst experienced IT users. Any changes to the interface should be communicated to users in advance of the change being carried out.

Several participants mentioned regular audits of the cloud providers infrastructure should be carried out to ensure compliance from a security perspective as well as a performance perspective, and that these concerns could be mitigated against by getting an independent company to perform the audits and award an accredited standard to cloud providers that complied with known standards so that customers of cloud computing would know to a fine degree exactly what standard of security was being provided. This would be useful to providers as a means of being able to prove to their customers that they are being guaranteed a minimum level of security. Audits of this nature could also help with proving the location of data as mentioned in the previous section.

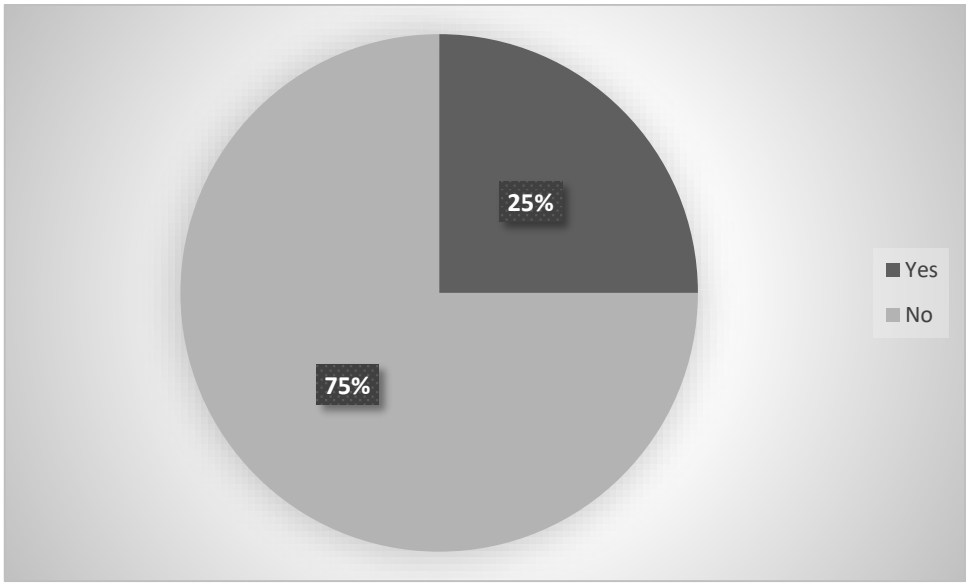

Figure 7: Are you concerned with loss of physical control?

The majority of participants are unconcerned about loss of physical control when operating in the cloud, one participant (SA2) noted that whether the hardware is “100 yards from me or 500 miles away from me, it makes no difference”. Of those that said they are concerned, one participant (IC1) mentioned that there could be a delay between a serious issue occurring and the cloud customer being notified of that issue, whereas if an issue occurred in an in-house data centre there would be no delay. Another participant (IA1) felt that losing physical control of the infrastructure would introduce unnecessary delays to the implementation of changes because the “red tape” could limit “your capability to change as the business changes”. One other participant (SC2) felt that the loss of physical control “would be quite daunting”. This indicates that cloud providers should consider methods to reduce this concern, such as introducing options for allowing customers to request expedited changes, but it is certainly telling that the vast majority of participants are totally unconcerned about losing physical control and those that are concerned are mostly those that work directly on the infrastructure.

Some participants cited cost as being a major factor in implementing cloud computing, however, one participant (IA1) warned that sometimes it can be more expensive than expected, going on to give the specific example of a development system that is expected to only be in operation from 9am – 5pm, thereby budgeting a certain amount of money for this system with the expectation that the system will be powered down after 5pm. The same participant mentions that the developers then expect access to the system to always be available to them and the cloud customer ends up paying for the systems to be operated 24/7 as the cloud customer themselves could end up with penalties being applied from their outsourced development company "if your system isn't available to them when they want it". This does indicate that customers of cloud providers should carefully define their requirements before moving a service to the cloud and consider that those requirements could grow beyond their expectations.

4.7 Fear

All participants, in some way or another, expressed their fear of cloud solutions, although fear is an *in-vivo* code, not all participants used the word fear, however, in many ways, it was clear that they had fears regarding cloud computing. These fears could be divided into three main sub-sections:

1. Fears that cloud computing is not a secure solution
2. Fears that cloud computing is not a viable solution
3. Fears about bandwidth

Each of these fears will be discussed in their own sub-section below.

4.7.1 Security Fears

Participants felt that there are additional security risks when using cloud computing, that by being in the cloud, it is inherently less secure. All participants mentioned security concerns, but the three listed below are the main reasons:

1. A 3rd party, the cloud provider, now has access to the data.
2. The data is now available directly over the internet presenting greater opportunities for attackers.
3. Moving to a large provider means that they are now a part of a bigger target, that, for attackers, (IM1) "their prize is bigger".

One participant (SC2) described his fears by saying that "once you lose sight of your servers, you begin to worry straight away", going on to say that "the biggest organisations

have been prone to security attacks", "you can't be 100% guaranteed". Another participant (SDM) mentioned that "there's probably a perceived additional risk", "at least if the systems are on-premise, they're directly within your control", it is notable that this participant did not express any concern about loss of physical control.

There are also fears around lack of visibility and lack of control specifically regarding security; vendors may keep silent about attempted breaches, or even actual breaches. However, GPDR mandates that all breaches need to be reported so that specific fear may be groundless but it can prove impossible to police whether all attacks have been reported, companies can be very secretive about being subject to attacks due to potential reputational damage. It is easy to see that it is in a cloud provider's best interest to try to minimise or keep secret any breaches as that type of reputational damage could harm them irrevocably, even to such a degree as to cause their business to fail entirely if the breach was severe enough. Iovan & Iovan (2016) acknowledge that it is against the interests of cloud providers to volunteer information regarding vulnerabilities and they suggest that companies should constantly monitor SLAs according to pre-defined metrics to help detect service interruptions.

Several participants urged caution and that a risk assessment should be undertaken, with one participant (SA3) saying "a proper risk assessment and detail the risk, and then it'll be for the business to accept whether it's acceptable or not". This is excellent advice and should be followed by all potential cloud customers prior to embracing the cloud.

4.7.2 Viability Fears

Many of the participants felt, because cloud computing is still quite a new solution, that it had not yet been proven over the long term to be a viable solution, that they had not yet personally had enough experience with adopting cloud computing to be fully confidant in it as a solution. Cloud providers should be engaging directly with IT professionals to ensure that this lack of confidence is overcome.

Some of the participants that did have prior experience with the cloud also have concerns about those experiences.

Those who do have experience of the cloud highlighted the lack of visibility as being a strong concern, that (IM1) "you don't get enough information back from them on what they're doing on a daily basis" and that this makes managing a service difficult. Another participant (IC1) also highlighted the loss of control as being a fear, that it would be more difficult to manage a cloud solution since it is "on an infrastructure not owned by the company". This lack of visibility directly relates to fear of loss of control, cloud providers should ensure that they provide full visibility to cloud customers, that every aspect of the system can be examined.

If customers feel that certain parts of the infrastructure are not visible to them it can be difficult for them to have full confidence in the solution especially if there is a failure that is attributed to a part of the system that the customer has no control or visibility over.

One participant (IM1) did make a connection between the increased complexity of cloud computing solutions and how that would influence vendor lock-in, while another (IA1) said “they make it very easy to get into the cloud, to get out of the cloud is almost impossible”. Another (SA3) felt that companies would be prey to cloud vendors changing their offerings to the detriment of their customers, who would be captive due to vendor lock-in. This is a very real fear and should be handled carefully by cloud vendors; the feeling that after a cloud migration the customer is now a captive of the cloud provider would certainly be enough to curtail a potential cloud adoption project. Wang & He (2014) mention that the amount of customisation of the cloud solution has a direct impact on vendor lock-in; the more heavily customised the solution is, the more difficult it is to switch providers.

The fear of a company going into receivership was raised by one participant (IA1), “your data is there but you don’t have access to it because they’ve shut down”. This can be a massive challenge for smaller, less well known, cloud providers as companies like Microsoft and Amazon are so large and well known that it is very difficult to imagine them failing.

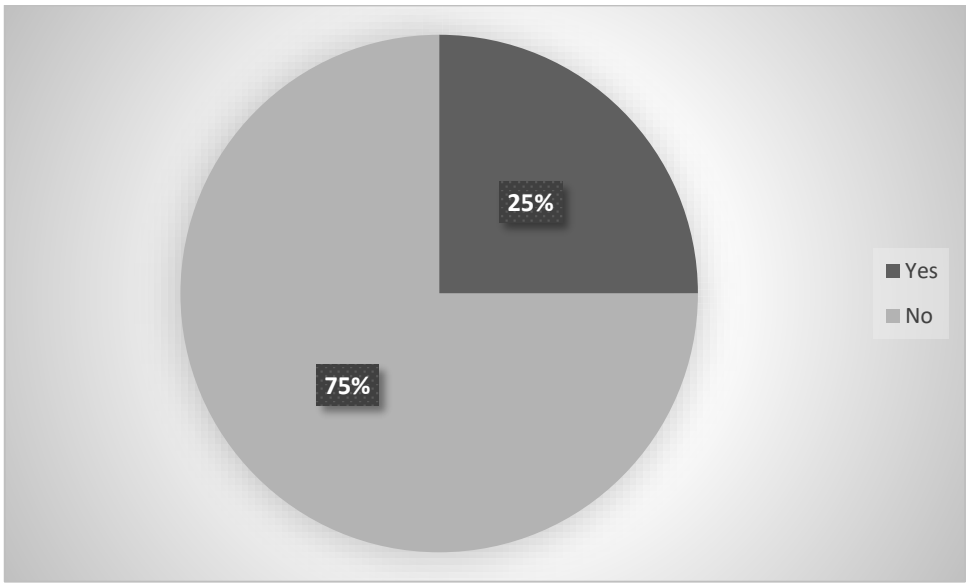

Figure 8: Would you adopt the cloud for mission critical applications?

4.7.3 Bandwidth Fears

Almost all participants mentioned bandwidth as being a fear when adopting cloud security, as highlighted by Carcary et al (2014). There was no fear regarding the bandwidth that the provider had to the internet, but rather the fear is that the bandwidth between the customer and the cloud provider would not be good enough, with one participant describing it as a (IM1) “black hole” where “you can’t detect where the problem is”. This can only be

addressed by increasing bandwidth but even with increased bandwidth, issues on the line itself could cause problems for users, especially affecting performance. Support issues were raised as a concern by participants with and without direct cloud experience, that it would be an unknown, and therefore, a risk. There was certainly a fear hinted at by one participant (IM1) that the cloud providers would absolve themselves of responsibility when issues were occurring, without offering any real proof that the fault was not on their cloud platform.

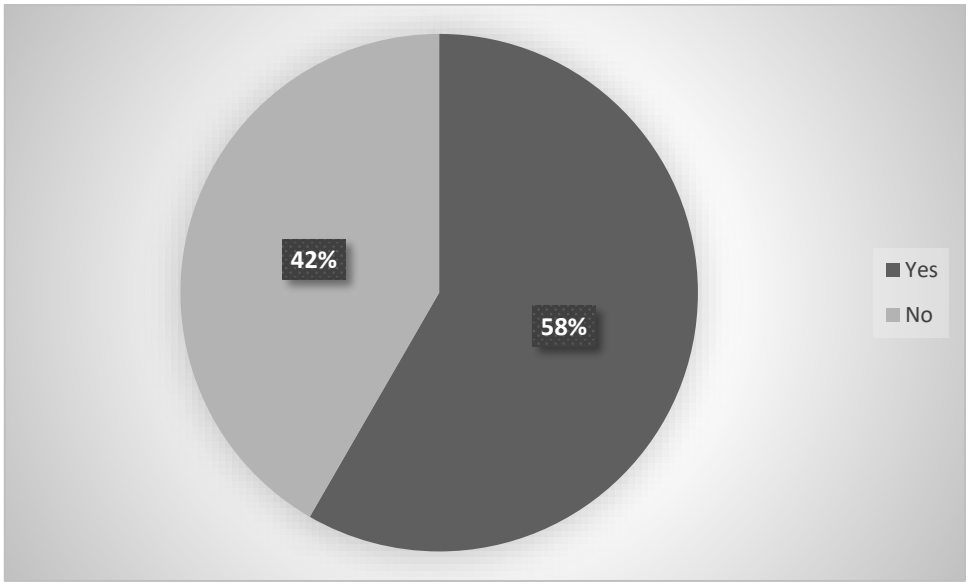

Figure 9: Are you concerned about bandwidth?

4.8 Trust

A counterpoint to fear is trust; trust of cloud computing as a solution and trust of the individual cloud providers themselves. Trust was a very strong theme throughout the interviews (SC1) “trust, trust is a big thing”.

4.8.1 Trust in Cloud Computing

As discussed in section 4.7.2, cloud computing as a mainstream solution is still quite new and some participants felt that it was not quite proven (SA2) “people need to establish trust in the solution”. One participant felt that trust could be compromised very easily by providing poor support; (IM1) “my users are seeing that their application is slow” but “cloud suppliers are saying no, everything is fine on my side” which leads to less trust of the cloud as a viable solution. Some participants felt that they had not established enough trust in the cloud themselves yet due to not having enough exposure, with one participant saying that (SA2) “once you’ve a bit of experience in it, and moved your applications to it” that a migration of mission critical applications should be considered. The same participant felt that the IT

industry as a whole has knowledge that could be classified as “very immature at the moment” that “not many companies have done it”. This does indicate a gap in the market for cloud enablers. Cloud enablers are companies that can assist other companies with their adoption of the cloud and help them to manage it into the future.

These concerns aside, almost all participants trust the cloud as a solution and many of them can see the benefits, with many saying that they believe the cloud to be more reliable, more resilient, more secure, better resourced, with greater ongoing investment.

One participant (SA3) compared it with virtualisation; at first the industry was wary of virtualisation and considered it as a viable solution for test and development environments, but then “you get more trust in it and people would start to put production workloads on it”. It is easy to see the parallels between the adoption of virtualisation and the adoption of cloud computing. Cloud computing would not be possible or be seen as a viable option without the massive success of virtualisation.

4.8.2 Trust in Cloud Vendors

The second major pillar of cloud computing trust is trust in the cloud provider, all participants emphasised the need to trust the cloud provider because the actual hardware, the cloud infrastructure, is now abstracted from the customer, and the customer has no visibility of the underlying hardware. The customers of cloud providers need to believe the cloud providers with regards to underlying hardware, security configurations, and location of the data. There is no way for customers to easily police the cloud providers in these areas so trust is the only option for customers of cloud providers. They also need to trust that the cloud provider has competent staff. One participant (SA2) felt that customers of cloud providers are in good company: “there’s enough companies in the cloud at the moment” so “if they’re acceptable to these changes, why shouldn’t me, as a company, be acceptable to those changes as well” indicating that other companies trusting cloud providers is a good reason to trust them. Lin & Chen (2012) called this observability and mention it as an influencing factor on whether or not the cloud would be adopted.

Several participants mentioned that this trust could be policed in some ways by means of Key Performance Indicators (KPIs) and SLAs with some participants citing the lack of information from cloud providers as being potential barriers to embracing trust. Manuel (2015) posits that trust could be measured by the use of SLAs. Most participants gave the impression that the bigger a cloud provider is, the easier it is to trust them. This illustrates just how important trust is for cloud providers, they are trading on that trust and should that trust be compromised it could well be disastrous for the cloud provider.

(SA3) “Now you’re moving to a model where it’s complete vendor trust”.

4.9 Upskill

Participants were divided when asked about whether or not job security was a concern, but whether they expressed concern or not, all agreed that the increased adoption of cloud computing would cause their role to change, that (SA1) “cloud is just the start of a new journey in the line of our work”. Some participants feel that there are (IC2) “ample opportunities” in cloud computing; (SA2) “there’s always going to be a role for IT, the role will diversify”. Several participants mentioned that the cloud still needs to be managed by IT staff. As a profession, IT has changed massively over the years and is continuously evolving, new software and software upgrades are being developed all the time and IT professionals need to quickly become proficient in their use. It may be easy for IT professionals to view cloud computing as just another upgrade to their systems that they need to manage, which would explain the lack of fear that is evident in the participants’ response to this question.

Most participants mentioned that upskilling would be necessary for IT staff to remain employed in a future where most companies have migrated to the cloud; upskilling was emphasised by those expressing concern about job security and those that were unconcerned. It is certainly interesting that all participants realise the need for upskilling, perhaps because they have been upskilling for their entire careers. Ghormley (2012) certainly agrees with this approach and urges IT professionals to embrace cloud computing in order to secure their future.

Although a future of mass unemployment was not envisioned by any of the participants, one participant (IA1) mentioned that “people in IT departments are always hearing about downsizing” and that there would be less work overall for IT people to do leading to less IT jobs overall. This concern was not shared by any of the other participants.

One participant (IC3) expressed his lack of concern: “I don’t think anyone’s job is secure, no matter what they do”.

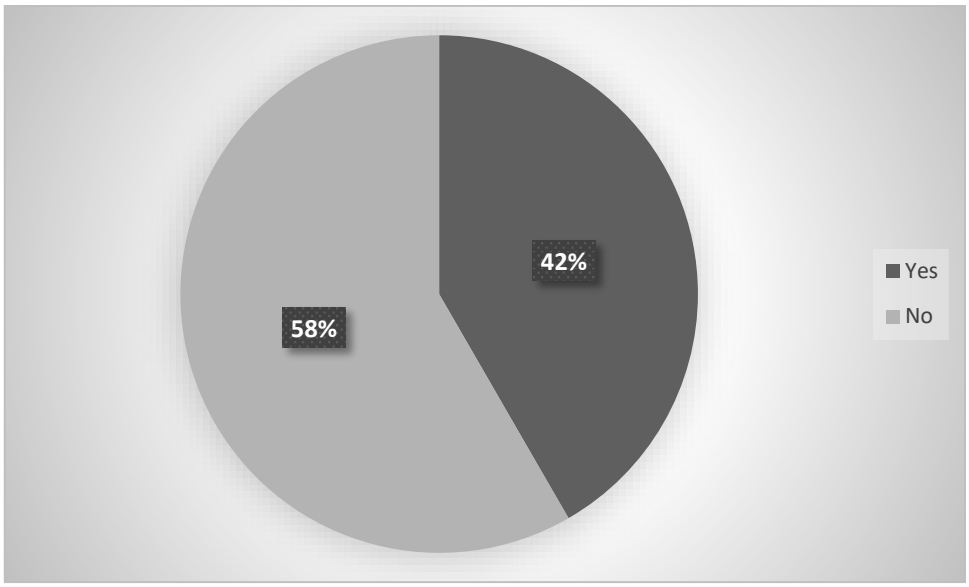

Figure 10: Are you concerned about job security?

4.10 Inevitable

A strong underlying theme throughout all of the interviews was about the inevitability of mass adoptions of cloud computing (SA2) “give it 5 years, we won’t even be considering if you should go to the cloud or not, you’ll just be putting your application in the cloud”. This 5 year period until cloud adoption has been fully adopted falls almost exactly within the range of 8 to 15 years advanced by Utterbank (1974) in his diffusion of technology paper, which has continued to prove prescient. (IC2) “I believe everyone, sooner or later, everyone will be in the cloud”. Another participant (SC2) used the word “inevitable” three times during the interview, in reply to three different questions, to express the belief of the coming mass adoption of cloud computing. This is most likely because all of the participants in this study are very experienced and have all directly experienced the evolution of IT brought about by virtualisation; approximately half of the participants would also have experienced the massive evolution brought about by the internet.

4.11 Barriers

This section lists each of the barriers identified in the literature and outlines the participants’ attitudes to each barrier. A description of each barrier is provided as an *aide memoire*.

Barrier	Attitude
Security and Privacy This barrier refers to the safety and security of the data stored in the cloud	Participants did express concerns about security and privacy, as expected, but none of them felt that this was a barrier to cloud computing adoption as they felt that the security in the cloud would be at least as good, if not

	better, than what they would have in-house, however they did express concern so it is still something that cloud vendors need to continue to consider as a major barrier
Regulation The ability of government bodies to influence cloud computing via the implementation of laws	Most participants are aware of the new GDPR regulations but they feel that this responsibility would be offloaded to the cloud provider in the event of cloud adoption. However one participant (IM1) expressed strong concerns about this barrier
Loss of Physical Control Cloud computing customers no longer have access to the actual hardware used by their systems	Most participants are entirely unconcerned about this barrier; most of the participants do not interact physically with any hardware so perhaps it is not surprising that they are unconcerned
Reliability The ability of cloud computing systems to be available at all times	All participants felt that the cloud providers are able to ensure reliability
Performance Concerns whether or not applications will be responsive enough when operated by users	Participants were divided about performance as a barrier. This highlights the fact that performance is an important consideration
Job Security In a world that has almost entirely migrated to cloud computing, will there still be a requirement for IT professionals?	Although participants were divided about whether this is a concern or not, all agreed that upskilling would alleviate this concern. Therefore, job security does not represent a strong barrier to adoption
Data Transfer Bottlenecks (Bandwidth) Is the data throughput to the cloud enough to ensure good performance?	Most participants are concerned about bandwidth causing issues. This remains an important barrier
Compatibility	No participants expressed concern about compatibility

Whether or not applications will continue to interoperate when migrated to the cloud	
Complexity Moving services to the cloud makes applications more complicated to manage and support	Complexity was mentioned by two participants only; one participant (IM1) felt that the increased complexity would cause issues whereas the other participant (SA3) felt that cloud computing makes IT less complex. The vast majority of participants are unconcerned about complexity as a barrier
Vendor Lock-in The difficulty of switching to a different cloud provider	Most of the participants did not mention vendor lock-in at all, with only two participants (IM1, IA1) highlighting it as a concern
Reputation Fate Sharing The action of another company that happens to share cloud infrastructure could negatively harm innocent companies	Prior to the interview, not even one of the participants had heard of this barrier; all participants were unconcerned
Pricing Scheme Cloud vendors could change their prices or penalize customers for unplanned usages	Only one participant had any concerns about the pricing scheme and the concern related to cloud customers underestimating their own predicted usage of the cloud rather than any issue with the cloud vendors pricing scheme
Scalable Storage Can adequate storage be provided fast enough when needed?	No participant expressed concern about this barrier
Bugs The potential for new problems to appear that are caused by migrating to the cloud	No participant expressed concern about this barrier
Scaling Quickly Will cloud infrastructure be available quickly enough when demanded?	No participant expressed concern about this barrier

Software Licensing Will cloud computing add additional complexity to software licensing?	No participant expressed concern about this barrier
Lack of Features Some applications in the cloud do not offer the same level of functionality as their offline version	No participant expressed concern about this barrier

Table 5: Participant attitudes towards each barrier

The attitudes to cloud adoption barriers expressed by the participants' shows that the most important barriers that are mentioned in the literature are:

- Security and Privacy
- Performance
- Bandwidth

Although not specifically mentioned as barriers in the literature, a fourth and fifth barrier should be added to the list of most important barriers. As discovered in this research, both fear and trust represent important barriers in the minds of the participants' of this study.

Of less concern, but still mentioned as a concern by a minority of the participants, are the barriers listed below:

- Loss of Physical Control
- Regulation
- Complexity
- Vendor Lock-in
- Pricing Scheme
- Job Security

The rest of the barriers mentioned in the literature did not cause any concern for the participants of this study.

Participants were asked what barrier they felt would cause the most concern when adopting cloud computing. The chart below shows the barrier that was mentioned as most important by each participant:

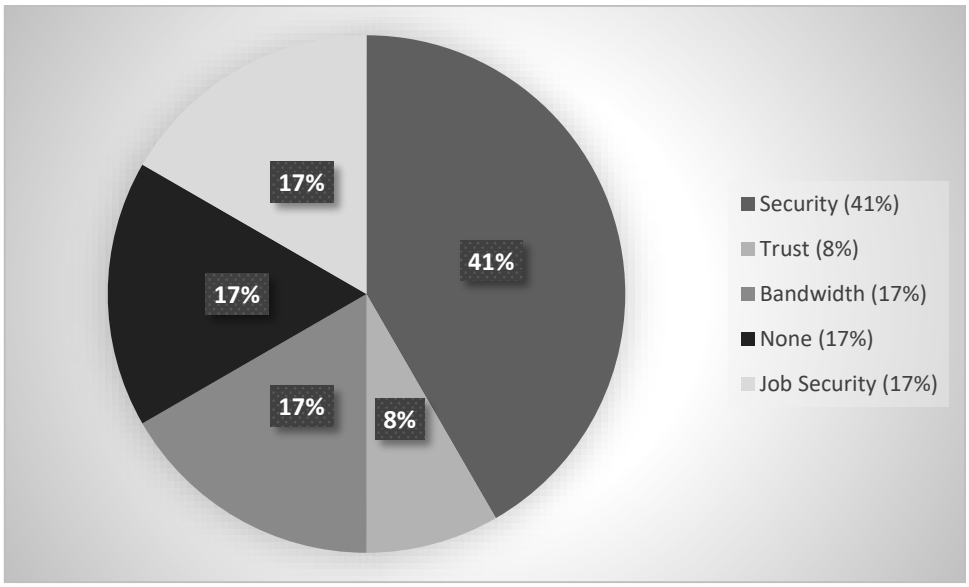

Figure 11: Which barrier is the most important?

Security was declared as the most significant issue by 41% of participants. Bandwidth is also mentioned by two participants and a further two of the participants were not concerned with any of the barriers and feel that the cloud is ready for full scale adoption. One participant mentioned trust as the most important barrier. Interestingly, two participants cited job security as the most important barrier for adoption despite both of them previously mentioning that upskilling would alleviate any such fears. Perhaps they feel that upskilling may not be enough, although they do not predict the mass unemployment feared by Raza et al (2012).

4.12 Quantitative Data

Throughout this chapter there have been pie charts included in the text to illustrate the general thoughts of the participants' in relation to some of the yes or no questions that were asked during the interview. The table below has a column for each participant and a row for each question asked. Years of experience is also included. Highlighted squares indicates that the participant answered negatively to the question from a cloud adoption perspective. For example, the question, "Are you concerned with performance?", listed as "Performance?" in the table, would be highlighted if the participant answered "Yes", because for this question, answering "Yes" indicates that performance is seen as a barrier to that participant.

The table has been ordered to show those participants with the most concerns on the left and those with the least concerns on the right.

Question	PMM	IA1	IC1	IM1	SA3	SA1	SC2	SA2	SDM	SC1	IC2	IC3
Experience	43	22	32	20	16	15	15	15	18	12	20	15
Non-Sensitive?												
Sensitive?												
Performance?												
Reliability?												
Control?												
Critical?												
Bandwidth?												
Job Security?												

Table 6: Quantitative data

There are two broad observations that can be made from the table above:

1. In general, those with greater experience have more reservations about adopting the cloud. This could be because those with greater experience are more realistic about the challenges involved while those with less experience are more idealistic about the potential benefits.
2. The participants whose role is in infrastructure are split between those that fully embrace cloud adoption, and those that have the most number of reservations, with no infrastructure participants in the middle ground. Interestingly, it is those with greater experience in infrastructure that have the most reservations which could also indicative a realistic versus idealistic view of cloud adoption. It is also worth mentioning that, in terms of job security, infrastructure will be the role that is most subject to evolving due to cloud computing.

4.13 Grounded Theory

The in-depth analysis that has been conducted in this chapter gives rise to the theories in this section. These theories are grounded in the data.

- The mass adoption of cloud computing will have been achieved within the next 5 years.
- Trust of the cloud provider is the key ingredient in cloud adoption; if this trust is abused, compromised, or harmed in any way, it could lead to the failure of the cloud provider.
- Fear of cloud computing is currently holding back some companies from adopting cloud computing but that fear will diminish over time as more and more companies adopt the cloud.

- IT professionals, especially those that work directly with infrastructure, will see their role evolve and should upskill to remain employed into the future.

4.14 Conclusion

This chapter has described the research in-depth; how the research was conducted, who was participating in the research, and what was contained within the research. The research was also examined in great detail before the conclusions to the research were presented.

5 Conclusions and Future Work

5.1 Introduction

This exploratory study set out to assess the attitudes of IT professionals towards cloud computing adoption barriers. The review of the currently available literature identified the adoption barriers and the research was designed in such a way as to elicit the attitudes of IT professionals towards the identified barriers.

This chapter presents the conclusions from the research, demonstrates that the research question has been answered, discuss the generalisability of the findings, outlines the limitations of the research, and presents some ideas for possible future research in this area.

5.2 Research Claims

This research began by identifying the most important barriers to cloud computing adoption; this was achieved by studying the literature surrounding this subject.

The existing literature shows that security is the most important barrier to cloud computing adoption; the findings of this research do not contradict the literature in this regard but actually reinforce the literature. Security continues to be the most important barrier. Regulation as a barrier was emphasised quite strongly by the literature but only one participant showed any concern about regulation, with most participants believing that the cloud vendor will assume responsibility for this barrier. The literature regards loss of physical control and reliability as being the next most important barriers but this was also not reflected by the participants in this study. However, the next three barriers, performance, job security, and bandwidth, were considered important by the participants, with job security and bandwidth being specifically mentioned as most important by two participants each. Although performance was not mentioned by any participants as being the most important barrier, it was mentioned during the interviews quite frequently as being a cause of concern. The next barrier mentioned in the literature, compatibility, was entirely unmentioned by the participants of this study. Complexity and vendor lock-in were mentioned as concerns by two participants only. The remaining barriers, reputation fate sharing, pricing scheme, scalable storage, bugs, scaling quickly, software licensing, and lack of features, were virtually unmentioned by the participants. These were identified by the literature as being the least important barriers since they were only mentioned in one or two articles each so it is unsurprising that participants displayed no concern about them.

The attitudes of the participants are broadly in line with what could be expected from an examination of the literature with the notable exception of the relative importance of some of the adoption barriers. The literature placed a greater emphasis on three of the barriers, regulation, loss of physical control, and reliability, highlighting all of them as being just below security in terms of importance, than was shown by the participants. In the case of regulation, it is because the participants feel that the cloud vendor will assume responsibility for compliance with regulations and they may be correct. However, the cloud vendor is not actually liable for breaches of regulations; this responsibility ultimately resides with the owners of the data, the cloud computing customers. Loss of physical control was not regarded as being an important barrier as the success of virtualisation has already abstracted many IT professionals from the hardware. Reliability is not a concern for the participants as they trust the vendors to ensure that adequate reliability is in place.

In addition to assessing the attitudes of IT professionals to the identified barriers, this study has also exposed the key role that trust plays in cloud computing adoption, trust in cloud computing as a viable solution, and trust in the cloud vendors themselves. This trust can overcome the concerns around security, and can also overcome concerns regarding the other identified barriers to adoption if the trust is great enough.

Fear has also been identified as a major component in the attitudes of IT professionals towards cloud computing; this fear is hampering cloud computing adoption but the fear is decreasing as trust grows with more and more cloud computing adoptions expected until cloud computing has reached full adoption in 5 years from the time of this study.

IT professionals, especially those working directly with infrastructure, are going to see their role evolve over the next 5 years and it is vital that they upskill to keep their skills relevant.

5.3 Importance of this Research

This research set out to examine the attitude of IT professionals towards adoption barriers whereas other studies of this type sought to identify the barriers themselves. In this regard, this research is important as it examines how IT professionals feel about the identified adoption barriers, and how they believe cloud computing adoption will be impacted by each of the adoption barriers. It advances the current knowledge in this area by highlighting the importance of trust, as well as ranking the relative importance of each of the adoption barriers. This shows all stakeholders of cloud computing which barriers they should focus on, and the recommendations for practitioners, outlined below, offer actionable advice for all of the stakeholders.

5.4 Demonstration that the Research Question has been answered

This study set out to examine attitudes to cloud computing adoption barriers by exploring the following question:

What is the attitude of IT professionals towards cloud computing adoption barriers?

The answer to this question is that IT professionals feel a hesitant acceptance towards cloud computing adoption barriers; an acceptance that is mixed with fear but balanced by trust. Their feeling of the inevitability of mass cloud computing adoption acts to enforce this acceptance as acceptance is the only response available in the face of this inevitability.

5.3.1 Recommendations for Practitioners

In answering this question, recommendations can be made to the various stakeholders that are interested in cloud computing adoption barriers. These stakeholders are cloud computing vendors, companies that are considering, or beginning, their cloud computing journey, and the IT professionals themselves. All 17 of the identified barriers to cloud computing adoption are covered by the recommendations in this section.

5.3.2 Recommendations for Cloud Computing Vendors

It is clear from the results of this study that all cloud vendors need to do everything they can to ensure that they are trusted by IT professionals and they must never endanger this trust once it has been established. There are two distinct areas where trust is important: trust of cloud computing as a solution, and trust of the cloud vendors themselves. Trust of cloud computing as a solution has been growing as people are becoming more familiar with it due to its growth, and also due to improvements in the technologies surrounding cloud computing. Once this trust has been established, it will remain in place and become unshakeable. This trust can overcome concerns about security and privacy, loss of physical control, reliability, performance, data transfer bottlenecks, compatibility, complexity, scalable storage, bugs, scaling quickly, and lack of features. These 11 barriers can be overcome by trust, but only if the cloud provider is not choosing to save money by investing poorly in their cloud infrastructure, which leads to the second area of trust: trust in the cloud vendor. This trust will not be unshakeable and if a cloud vendor causes their trust to become tarnished in the eyes of IT professionals, it will be very difficult, potentially even impossible, for them to regain that trust. Cloud vendors can maintain, and build, their trust by following the recommendations below:

- Ensure that SLA violations are addressed rapidly and underlying causes eliminated

- Undertake regular audits of their infrastructure by independent 3rd parties and publicly disseminate the results
- Keep their infrastructure current by investing heavily in the underlying hardware and in security technologies
- Provide as much visibility as possible to their customers
- Be as open and clear as possible regarding costs and licensing

A cloud vendor that follows the recommendations above can overcome the 11 barriers that rely on trust of cloud computing as a solution as well as the additional barriers of regulation, pricing scheme, and software licensing. Reputation fate sharing is a more difficult barrier for cloud providers to overcome due to the random nature of its occurrence; if a vendor wanted to overcome this barrier, they would need to offer customers infrastructure that is operating in a sandbox style environment. This means that they would not be sharing infrastructure with any other companies, which would negate many of the cost savings associated with operating on shared infrastructure. However companies that are concerned about this barrier would pay a premium to overcome, and thoroughly negate, this barrier. None of the participants in this study showed any concern for reputation fate sharing as a barrier so it does not seem to be a major concern when considering adoption.

Vendor lock-in presents an interesting conundrum for cloud computing vendors; on the one hand, it is in their best interests to encourage vendor lock-in by any means possible, on the other hand, in order to attract customers, they need to show that it is relatively easy to migrate away from their cloud solution. The more that the customer customises their solution, the more difficult it will be for them to migrate away to a competitor. The solution to this conundrum for cloud vendors is to ensure that their customers trust that they can migrate away from the solution by providing them with the means to do so should they want to, but also to offer plenty of customisations to the customers so that they do not want to migrate away as they would then lose all of their vendor specific customisations.

5.3.3 Recommendations for Potential Cloud Customers

Companies that are considering moving to the cloud need to pick a cloud vendor. This will be their most important decision regarding cloud computing adoption. When considering this decision, companies should be asking the following questions:

- Why is this cloud vendor trustworthy?
- Is the SLA reasonable and fair, with appropriate penalties for violations?
- Does this cloud vendor undertake regular audits by a 3rd party, or is willing to undertake audits?

- Does this cloud vendor provide a clear and straight-forward means of migrating away from their infrastructure?

Once a company has migrated to the cloud, vendor lock-in will be their greatest concern. The only way to overcome it would be to utilise as little optimisations as possible. By keeping the solution as generic as they can, they can lessen their risk of vendor lock-in.

5.3.4 Recommendations for IT Professionals

The only recommendation for IT professionals is to ensure that they upskill and learn about cloud computing solutions. This recommendation is especially important for IT professionals that are working directly with the infrastructure; once a company has migrated to the cloud, all of their infrastructure will be in the cloud.

5.5 Generalisability of the Findings

This exploratory study focussed on 12 participants only so it is not realistic to claim generalisability across all IT professionals. However, the theories presented in this study are grounded in the data so they could be tested on a larger number of participants, perhaps in a quantitative study. The findings are interesting as they take an in-depth look at cloud computing adoption barriers and provide a unique perspective on this topic as well as some deep insights into the challenges facing cloud computing vendors, potential cloud customers, and IT professionals themselves, when considering their journey into the cloud.

5.6 Limitations of this Study

There are three primary limitations of this study:

1. The sample size of 12 is not enough to claim generalisability
   The sample size of 12 is enough to reach theoretical saturation for a qualitative study but it cannot be said that the finding will necessarily apply universally.
2. This study represented the opinions of the participants' at a single point in time
   Cloud computing is continuously evolving as are people's views about it; a follow-up interview of the same participants in the future may lead to entirely different conclusions. Unfortunately there was not enough time to complete a longitudinal study of these participants.
3. This study focussed only on IT professionals in Ireland
   IT professionals from different countries could have different viewpoints and those differing viewpoints could lead to different conclusions

Although not a limitation of the research portion of this study, it is worth mentioning that the fact that the relative importance of the adoption barriers attributed to the literature was based purely on the number of papers that mention each barrier.

5.7 Areas for Future Research

This study has uncovered several areas that would be worthwhile to conduct further research on. These would be the grounded theories presented in Chapter 4.

The first theory is that the mass adoption of cloud computing will have been completed within five years. Research into whether this is the case would present interesting findings if conducted in a year or two, to see if the adoption of cloud computing is still growing and is it likely to reach full market penetration within the remaining three to four years.

A study centred on the importance of trust and fear in cloud adoption would be very interesting to see if these broad themes are truly universal when considering the cloud.

A study focussed on IT professionals and whether or not they have upskilled to become knowledgeable about cloud and cloud technologies would also be very interesting. Did those that upskilled see an improvement in their careers? Did those that were unable to upskill see a decline in their career?

It would also be interesting to take a closer examination of the reasons for the disparity between the literature and the findings of this study regarding the relative importance of some of the barriers. Why were the participants unconcerned about some of the barriers that the literature placed greater importance on?

Finally, if this study was repeated with the same participants in a few years from now, it would be very interesting to see how the participants views and opinions may have changed over time, especially with the continued prevalence and expected future growth of cloud computing.

5.8 Conclusion

This is a key period for the stakeholders of cloud computing as it is over the next few years that the strongest players in the world of cloud computing will be able to cement their positions as market leaders. This is mainly due to the difficulty and high costs of switching providers; once a company has migrated to the cloud they will be extremely reluctant to do it all over again by migrating to a different provider. For this reason, vendor lock-in may prove to be the most important barrier of all.

However, there are still many uncertainties regarding the future of cloud computing and, although it would be interesting to wait and see how things develop, in the words of one participant (PMM), “you have to proceed with what you know”.

References

Aljabre, A. (2012) Cloud Computing for Increased Business Value. International Journal of Business and Social Science, 3, 234–239.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. (2010) A View of Cloud Computing. Communications of the ACM, 53, 50–58.

August, T., Niculescu, M.F., Shin, H. (2014) Cloud Implications on Software Network Structure and Security Risks. Information Systems Research, 25, 489–510.

Bryman, A. (2012) Social Research Methods. Oxford, Oxford University Press.

Buyya, R., Shin Yeo, C., Venugopal, S., Broberg, J., Brandic, I. (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616.

Califf, C.B., Sarker, Suprateek, Sarker, Saonee, Skilton, M. (2016) The Role and Value of a Cloud Service Partner. MIS Quarterly Executive, 15, 231–242.

Carcary, M., Doherty, E., Conway, G. (2014) The Adoption of Cloud Computing by Irish SMEs – an Exploratory Study. Electronic Journal Information Systems Evaluation, 17, 3–14.

Carr, N. (2008) The Big Switch Rewiring the World, From Edison to Google. New York, W. W. Norton & Company.

Charmaz, K. (2006) Constructing Grounded Theory. London, Sage Publications Limited.

Cooper, D., Schindler, P. (2014) Business Research Methods. New York, McGraw-Hill Companies Inc.

Daskal, J. (2017) Congress Needs to Fix Our Outdated Email Privacy Law. Slate [Internet] Available at: http://www.slate.com/articles/technology/future_tense/2017/01/the_confusing_court_case_over_microsoft_data_on_servers_in_ireland.html [Accessed 7th August, 2017]

Daylami, N. (2015) The Origin and Construct of Cloud Computing. International Journal of the Academic Business World, 9, 39–45.

Deboosere, L., Vankeirsbilck, B., Simoens, P., De Turck, F., Dhoedt, B., Demeester, P. (2012) Cloud-Based Desktop Services for Thin Clients. IEEE Internet Computing 60–67.

Durao, F., Carvalho, J.F.S., Fonseka, A., Garcia, V.C. (2014) A systematic review on cloud computing. Journal of Supercomputing, 68, 1321–1346.

EU Legislators (2017) GDPR Key Changes [Internet] Available from: http://www.eugdpr.org/the-regulation.html [Accessed 7th July 2017]

Forni, A., van der Meulen, R. (2016) Gartner Says By 2020, a Corporate “No-Cloud” Policy Will Be as Rare as a “No-Internet” Policy Is Today. Gartner, Inc. [Internet], June 2016, Available from: http://www.gartner.com/newsroom/id/3354117 [Accessed 6th June, 2017]

Ghormley, Y. (2012) Cloud Computer Management from the Small Business Perspective. International Journal of Management & Information Systems, 16, 349–356.

Goutas, L., Sutanto, J., Aldarbesti, H. (2016) The Building Blocks of a Cloud Strategy. Communications of the ACM, 59, 90–97.

Greener, S. (2008) Business Research Methods. Frederiksberg, Ventus Publishing ApS.

Gupta, P., Seetharaman, A., Raj, J.R. (2013) The usage and adoption of cloud computing by small and medium businesses. International Journal of Information Management, 33, 861–874.

Haibach, G. (2015) Cloud computing and European Union private international law. Journal of Private International Law, 11, 252–266.

Iovan, S., Iovan, A.A., 2016. Cloud Computing Security. Fiability & Durability Supplement, 1, 206–212.

Iyer, B., Henderson, J.C. (2010) Preparing for the Future: Understanding the Seven Capabilities of Cloud Computing. MIS Quarterly Executive, 9, 117–131.

Jiang, T., Chen, X., Li, J., Wong, D.S., Ma, J., Liu, J.K. (2015) Towards secure and reliable cloud storage against data re-outsourcing. Future Generation Computer Systems, 52, 86–94.

Khajeh-Hosseini, A., Greenwood, D., Smith, J.W., Sommerville, I. (2012) The Cloud Adoption Toolkit: supporting cloud adoption decisions in the enterprise. Software - Practice and Experience, 42, 447–465.

Kleinrock, L. (2003) An Internet vision: the invisible global infrastructure. Ad Hoc Networks, 1, 3–11.

Kulkarni, R.G., Waghmare, R.P., Waykule, V., Bankar, H., Koli, K. (2012) Cloud Storage Architecture. Presented at the 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), pp. 76–81.

Lin, A., Chen, N.-C. (2012) Cloud computing as an innovation: Perception, attitude, and adoption. International Journal of Information Management, 32, 533–540.

Manuel, P. (2015) A trust model of cloud computing based on Quality of Service. Annals of Operations Research, 233, 281–292.

Maresova, P., Sobeslav, V., Krejcar, O. (2017) Cost–benefit analysis – evaluation model of cloud computing deployment for use in companies. Applied Economics, 49, 521–533.

Marston, S., Zhi Li, Bandyopadhyay, S., Zhang, J., Ghalsasi, A. (2011) Cloud computing — The business perspective. Decision Support Systems, 51, 176–189.

Matthews, B., Ross, L. (2010) Research Methods. Essex, Pearson Education Limited.

Mell, P., Grance, T. (2011) The NIST Definition of Cloud Computing. NIST Special Publication 800–145.

Microsoft, (2017) Azure Directory of Services [Internet] Available from: https://azure.microsoft.com/en-us/services/ [Accessed 12th February 2017]

Oliveira, T., Thomas, M., Espadanal, M. (2014) Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. Information & Management, 51, 497–510.

Ray, D. (2016) Cloud Adoption Decisions: Benefitting from an Integrated Perspective. The Electronic Journal Information Systems Evaluation, 19, 3–21.

Raza, M.H., Adenola, A.F., Nafarieh, A., Robertson, W. (2015) The Slow Adoption of Cloud Computing and IT Workforce. ScienceDirect, 52, 1114–1119.

Regalado, A. (2011) Who Coined “Cloud Computing”? MIT Technology Review [Internet], October 2011, Available from: https://www.technologyreview.com/s/425970/who-coined-cloud-computing/ [Accessed 11th February 2016]

Saunders, M., Lewis, P., Thornhill, A. (2016) Research Methods for Business Students. Essex, Pearson Education Limited.

Singh, A., Chatterjee, K. (2017) Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88–115.

Utterbank, J.M. (1974) Innovation in Industry and the Diffusion of Technology. Science, 183, 620–626.

Wang, F.K., He, W. (2014) Service strategies of small cloud service providers: A case study of a small cloud service provider and its clients in Taiwan. International Journal of Information Management, 34, 406–415.

Yang, H., Lin, S. (2015) User continuance intention to use cloud storage service. Computers in Human Behaviour, 52, 219–232.

Zikmund, W., Babin, B., Carr, J., Griffin, M. (2009) Business Research Methods. Cincinnati, South-Western College Publishing.

Bibliography

Assuncao, M.D., Calheiros, R.N., Bianchi, S., Netto, M.A.., Buyya, R. (2015) Big Data computing and clouds: Trends and future directions. Journal of Parallel and Distributed Computing, 79, 3–15.

Beltrán, M. (2016) BECloud: A new approach to analyse elasticity enablers of cloud services. Future Generation Computer Systems, 64, 39–49.

Bento, A., Bento, R. (2011) Cloud Computing: A new phase in Information Technology Management. Journal of Information Technology Management, XXII, 39–46.

Chang, V., Kuo, Y.-H., Ramachandran, M. (2016) Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24–41.

Chang, V., Wills, G. (2016) A model to compare cloud and non-cloud storage of Big Data. Future Generation Computer Systems, 57, 56–76.

Fanning, K., Cannon, D.M. (2015) DaaS: A Cost-Savings Strategy. The Journal of Corporate Accounting & Finance 15–20.

Goiri, I., Guitart, J., Torres, J. (2012) Economic model of a Cloud provider operating in a federated Cloud. Information Systems Frontiers, 14, 827–843.

Goode, S. (2015) A Note on Service Switching: Evidence From Cloud Storage Services. Services Marketing Quarterly, 36, 153–172.

Hsu, P., Ray, S., Li-Hsieh, Y. (2014) Examining cloud computing adoption intention, pricing mechanism, and deployment model. International Journal of Information Management, 34, 474–488.

Huang, Z., Chen, J., Lin, Y., You, P., Peng, Y. (2015) Minimizing data redundancy for high reliable cloud storage systems. Computer Networks, 81, 164–177.

Iyer, B., Henderson, J.C. (2012) Business Value from Clouds: Learning from Users. MIS Quarterly Executive, 11, 51–60.

Menard, P., Gatlin, R., Warkentin, M. (2014) Threat Protection and Convenience: Antecedents of Cloud-Based Data Backup. The Journal of Computer Information Systems, 55, 83–91.

Misra, S.C., Mondal, A. (2011) Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment. Mathematical and Computer Modelling, 53, 504–521.

Mithas, S., Tafti, A., Mitchell, W. (2013) How a firms competitive environment and digital strategic posture influence digital business strategy. MIS Quarterly, 37, 511–536.

Neumann, P.G. (2014) Risks and Myths of Cloud Computing and Cloud Storage. Communications of the ACM, 57, 25–27.

Rimal, B.P., Jukan, A., Katsaros, D., Goeleven, Y. (2011) Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. Journal of Grid Computing, 9, 3–26.

Supriya, M., Sangeeta, K., Patra, G. (2016) Trustworthy Cloud Service Provider Selection using Multi Criteria Decision Making Methods. Engineering Letters, 1, 24.

Tang, C., Liu, J. (2015) Selecting a trusted cloud service provider for your SaaS program. Computers & Security, 50, 60–73.

Wang, B., Qi, Z., Ma, R., Guan, H., Vasilakos, A.V. (2015) A survey on data centre networking for cloud computing. Computer Networks, 91, 528–547.

Appendix A: Seventeen papers surveyed in section 2.6

Authors	Year	Title
Armbrust et al	2010	A View of Cloud Computing
Marston et al	2011	Cloud computing — The business perspective
Rimal et al	2011	Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach
Aljabre	2012	Cloud Computing for Increased Business Value
Khajeh-Hosseini et al	2012	The Cloud Adoption Toolkit: supporting cloud adoption decisions in the enterprise
Ghormley	2012	Cloud Computer Management From The Small Business Perspective
Lin and Chen	2012	Cloud computing as an innovation: Perception, attitude, and adoption
Carcary et al	2014	The Adoption of Cloud Computing by Irish SMEs – an Exploratory Study
Oliveira et al	2014	Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors
Neumann	2014	Risks and Myths of Cloud Computing and Cloud Storage
Raza et al	2015	The Slow Adoption of Cloud Computing and IT Workforce
Jiang et al	2015	Towards secure and reliable cloud storage against data re-outsourcing
Yang and Lin	2015	User continuance intention to use cloud storage service
Daylami	2015	The Origin and Construct of Cloud Computing
Iovan and Iovan	2016	Cloud Computing Security
Maresova et al	2017	Cost–benefit analysis – evaluation model of cloud computing deployment for use in companies
Singh and Chatterjee	2017	Cloud security issues and challenges: A survey

Appendix B

B.1 Participants Information Sheet

The below information sheet was issued to all participants prior to the commencement of the interview.

Participants Information Sheet

Cloud Computing: Attitudes to Adoption Barriers amongst IT Professionals

LEAD RESEARCHER: Robert Whelan

BACKGROUND OF RESEARCH: This interview is designed to assess current attitudes towards cloud computing amongst IT professionals with a specific focus on barriers to the adoption of cloud solutions.

You have been selected as a participant in this research due to your experience as an IT professional and your ability to influence the IT decision making process.

Experience of Cloud Computing is not necessary to be a participant in this research and if you have any questions about Cloud Computing, or require clarifications in order to answer any of the questions, the researcher can answer your questions and give you any background information that is needed.

PROCEDURES OF THIS STUDY: This interview is entirely voluntary and the interviewee can withdraw their consent at any time and for any reason without penalty. Interviewees can choose to not answer any of the questions asked.

This interview will have a duration of between 30 minutes to 60 minutes. There is a minimum of 9 questions and a maximum of 20 questions that can be asked. Some of the questions require a yes/no answer and some questions are open-ended and require more in-depth answers. This interview will be recorded by the interviewer.

There are no risks to the interviewee.

The interviewee can make a request to be debriefed after the interview has concluded. This may benefit the interviewee as it will enable them to clarify their understanding of cloud computing and barriers to adoption.

In the extremely unlikely case of illicit activity being reported the interviewer will contact the relevant authorities.

DATA STORAGE: The interview recordings collected during this study, and all data pertaining to this study, will be stored on the researchers own personal computer which is kept in the researchers home and only the researcher has the credentials to access this device. The recordings will be destroyed six months after the completion of the study.

PUBLICATION: The results of this interview will be included in a dissertation that will be submitted on the 1st of September 2017 to Trinity College Dublin as a partial requirement in order to be awarded an MSc in Management of Information Systems. All participants in this study have the right to see the end result of the research.

Individual results may be aggregated anonymously and research reported on aggregate results, however some direct quotations, quoted anonymously, from participants may also be included.

CONFLICTS OF INTEREST: Interviewees have been selected for interview due to their prior working relationship with the lead researcher, who will be conducting the interview. The results of the interview will not be used for any commercial purpose and this research is not being conducted on behalf of any company. Any information provided during this interview is confidential and no interviewee will be identifiable from the published study results.

B.2 Informed Consent Form

The informed consent form was signed by every participant prior to initiating the interview.

INFORMED CONSENT FORM

TRINITY COLLEGE DUBLIN

BACKGROUND OF RESEARCH: This interview is designed to assess current attitudes towards cloud computing amongst IT professionals with a specific focus on barriers to the adoption of cloud solutions.

PROCEDURES OF THIS STUDY: This interview is entirely voluntary and the interviewee can withdraw their consent at any time and for any reason without penalty. Interviewees can choose to not answer any of the questions asked.

This interview will have a duration of between 30 minutes to 60 minutes. There is a minimum of 9 questions and a maximum of 20 questions that can be asked. Some of the questions require a yes/no answer and some questions are open-ended and require more in-depth answers. This interview will be recorded by the interviewer.

CONFLICTS OF INTEREST: Interviewees have been selected for interview due to their prior working relationship with the lead researcher, who will be conducting the interview. The results of the interview will not be used for any commercial purpose and this research is not being conducted on behalf of any company. Any information provided during this interview is confidential and no interviewee will be identifiable from the published study results.

DECLARATION:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.

- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.
- I understand that my interview will be recorded and that I may be quoted in the resulting study but I will remain anonymous.

PARTICIPANT'S NAME:

PARTICIPANT'S SIGNATURE: _____

DATE: _____

- Statement of investigator's responsibility: I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHER'S CONTACT DETAILS: rwhelan1@tcd.ie

0868048991

INVESTIGATOR'S SIGNATURE: _____

Date

B.3 Research Ethics Approval Application Form

This form was used to apply for ethical approval

School of Computer & Statistics
Research Ethics Application

Part A

Project Title: CLOUD COMPUTING: ATTITUDES TO ADOPTION BARRIERS

Name of Lead Researcher (student in case of project work): ROBERT WHELAN

Name of Supervisor: ANTHONY NOLAND

TCD E-mail: RWHELAN1@TCD.IE Contact Tel No.: 0868048991

Course Name and Code (if applicable): MANAGEMENT OF INFORMATION SYSTEMS

Estimated start date of survey/research: MAY 1ST 2017

I confirm that I will (where relevant):

- Familiarize myself with the Data Protection Act and the College Good Research Practice guidelines ;
- Tell participants that any recordings, e.g. audio/video/photographs, will not be identifiable unless prior written permission has been given. I will obtain permission for specific reuse (in papers, talks, etc.)
- Provide participants with an information sheet (or web-page for web-based experiments) that describes the main procedures (a copy of the information sheet must be included with this application)
- Obtain informed consent for participation (a copy of the informed consent form must be included with this application)
- Should the research be observational, ask participants for their consent to be observed
- Tell participants that their participation is voluntary
- Tell participants that they may withdraw at any time and for any reason without penalty
- Give participants the option of omitting questions they do not wish to answer if a questionnaire is used
- Tell participants that their data will be treated with full confidentiality and that, if published, it will not be identified as theirs
- On request, debrief participants at the end of their participation (i.e. give them a brief explanation of the study)
- Verify that participants are 18 years or older and competent to supply consent.
- If the study involves participants viewing video displays then I will verify that they understand that if they or anyone in their family has a history of epilepsy then the participant is proceeding at their own risk
- Declare any potential conflict of interest to participants.
- Inform participants that in the extremely unlikely event that illicit activity is reported to me during the study I will be obliged to report it to appropriate authorities.
- Act in accordance with the information provided (i.e. if I tell participants I will not do something, then I will not do it).

Signed: ..... Date: 15/03/17

Lead Researcher/student in case of project work

Part B

Please answer the following questions.		*Yes/No*
Has this research application or any application of a similar nature connected to this research project been refused ethical approval by another review committee of the College (or at the institutions of any collaborators)?		No
Will your project involve photographing participants or electronic audio or video recordings?		YES
Will your project deliberately involve misleading participants in any way?		No
Does this study contain commercially sensitive material?		No
Is there a risk of participants experiencing either physical or psychological distress or discomfort? If yes, give details on a separate sheet and state what you will tell them to do if they should experience any such problems (e.g. who they can contact for help).		No
Does your study involve any of the following?	Children (under 18 years of age)	No
	People with intellectual or communication difficulties	No
	Patients	No

School of Computer Science and Sta tics
Research Ethical Application Form

Details of the Research Project Proposal must be submitted as a separate document to include the following information:

1. Title of project
2. Purpose of project including academic rationale
3. Brief description of methods and measurements to be used
4. Participants - recruitment methods, number, age, gender, exclusion/inclusion criteria, including statistical justification for numbers of participants
5. Debriefing arrangements
6. A clear concise statement of the ethical considerations raised by the project and how you intend to deal with them
7. Cite any relevant legislation relevant to the project with the method of compliance e.g. Data Protection Act etc.

Part C

I confirm that the materials I have submitted provided a complete and accurate account of the research I propose to conduct in this context, including my assessment of the ethical ramifications.

Signed: Robert M ..... Date: 15/3/17 .....
Lead Researcher/student in case of project work

There is an obligation on the lead researcher to bring to the attention of the SCSS Research Ethics Committee any issues with ethical implications not clearly covered above.

Part D

If external or other TCD Ethics Committee approval has been received, please complete below.

External/TCD ethical approval has been received and no further ethical approval is required from the School's Research Ethical Committee. I have attached a copy of the external ethical approval for the School's Research Unit.

Signed: ..... Date: .....
Lead Researcher/student in case of project work

Part E

If the research is proposed by an undergraduate or postgraduate student, please have the below section completed.

I confirm, as an academic supervisor of this proposed research that the documents at hand are complete (i.e. each item on the submission checklist is accounted for) and are in a form that is suitable for review by the SCSS Research Ethics Committ

Signed Anthony Niland ..... Date: 23rd March 2017 .....
Supervisor

Completed application forms together with supporting documentation should be submitted electronically to the online ethics system - https://webhost.tcd.ie/research_ethics/ When your application has been reviewed and approved by the Ethics committee, hardcopies with original signatures should be submitted to the School of Computer Science & Statistics, Room 104, Lloyd Building, Trinity College, Dublin 2.

Ethics Application Guidelines 2016

Appendix C

C.1 Interview Schedule

Question 9 below was deemed to be a little cumbersome to answer during the interview and instead became “which barrier do you feel is the most important?”

1. How long have you been working in IT?
2. Is cloud security a concern?
    a. What are your concerns?
    b. Would it stop you from adopting?
        i. Why not?
    c. Is there any security measure that would persuade you to adopt cloud?
    d. Would you adopt the cloud for non-sensitive uses?
3. Is regulation an issue?
    a. Why?
    b. Would it stop you from adopting?
4. Are you concerned with loss of physical control?
    a. Why?
    b. Would it stop you from adopting?
5. Are you concerned about reliability, performance, or bandwidth?
    a. Why?
    b. Would it stop you from adopting?
6. Is job security a concern?
    a. Why?
7. Would you adopt the cloud for mission critical applications?
    a. Why not?
8. Rank the most important five barriers in order of importance:
    a. Security and privacy
    b. Regulation
    c. Loss of physical control
    d. Reliability
    e. Performance
    f. Job security
    g. Data transfer bottlenecks (bandwidth)
    h. Compatibility
    i. Complexity
    j. Vendor lock-in
    k. Reputation fate sharing
    l. Pricing scheme

m. Scalable storage
n. Bugs
o. Scaling quickly
p. Software licensing
q. Lack of features

9. Any final thoughts or comments?

C.2 Interview Schedule Flowchart

The figure below visualises the interview schedule as a flowchart.

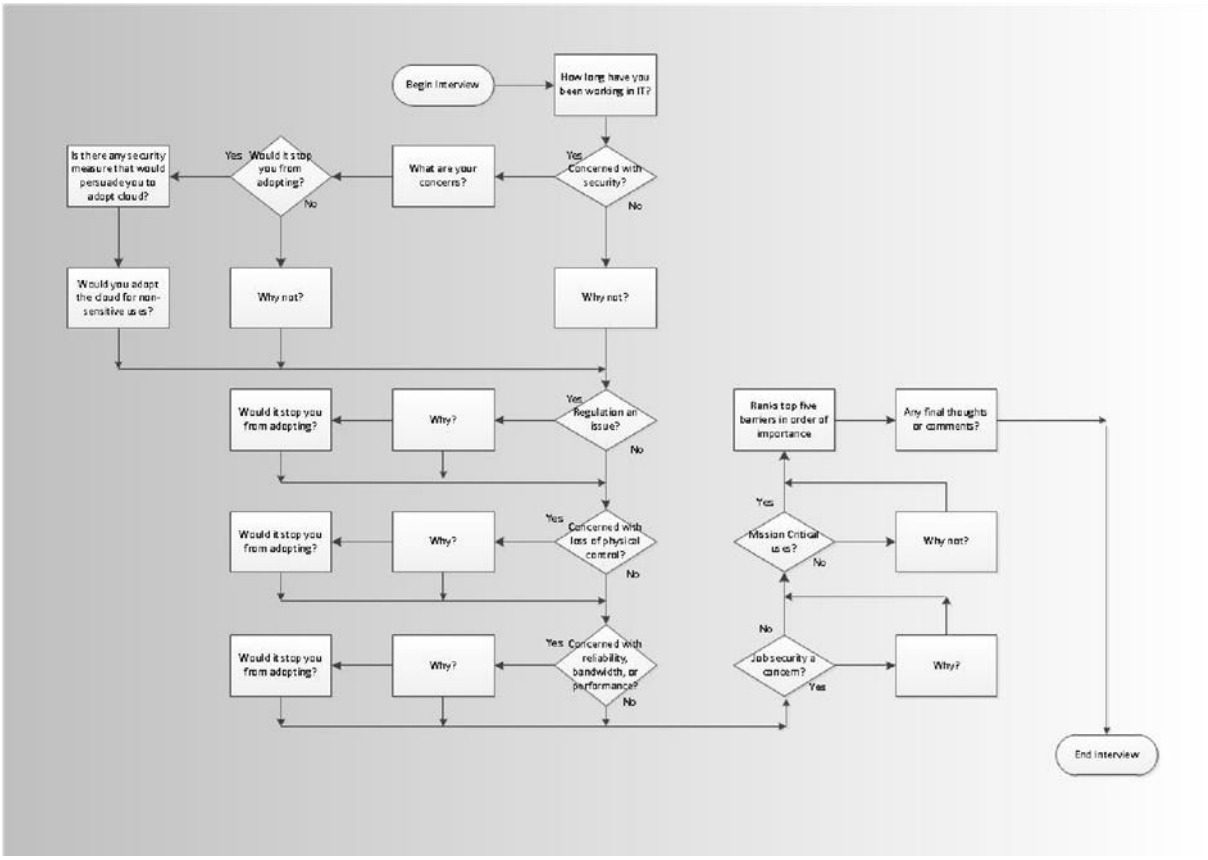

Figure 12: Interview schedule flowchart

C.3 Follow-up email

The email below was sent to all participants, along with a copy of the transcript of their interview. Not all participants responded but those that did all responded affirmatively. Four participants responded to this mail.

Hi *Participant*,

Thanks again for your time. The interview was of great benefit to me in my research work.

I've attached a transcript of this interview to this email. Would you look over it and confirm that this represents your opinions accurately?

Thanks very much.

Regards,

Robert