



OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Interoperability in Intercloud

Paul Joyce

This dissertation is submitted in fulfilment of the requirements for the degree of Master of Science (Cloud Computing Research)

Research Supervisor: Prof. Thomas Acton

Head of School: Prof. Alma McCarthy

Submitted to: College of Business, Public Policy, & Law,
J.E. Cairnes School of Business &
Economics, University of Galway

Date: June 2023

Table of Contents

LIST OF TABLES.....	iv
LIST OF FIGURES.....	iv
ABSTRACT.....	v
ACKNOWLEDGEMENTS.....	vi
1 Introduction	1
1.1 Background	1
1.2 Motivation for study	3
1.3 Research Question	3
1.4 Research Method.....	4
1.5 Summary of chapters.....	4
2 Literature Review	6
2.1 Introduction	6
2.2 Cloud Computing	7
2.3 History and Core technologies.....	9
2.3.1 Virtualisation.....	10
2.3.2 Multi-tenancy.....	10
2.3.3 Web services	10
2.4 Advantages of Cloud Computing	11
2.5 Cloud Computing Challenges	11
2.5.1 Technical Issues.....	12
2.5.2 Security	12
2.5.3 Cost	13
2.6 Cloud deployment models.....	14
2.6.1 Hybrid Cloud.....	14
Benefits of hybrid model.....	15
Challenges with hybrid model	15
2.6.2 Multi-Cloud	17
Benefits of Multi-Cloud model.....	19
Challenges with Multi-Cloud model.....	20
2.6.3 Intercloud.....	21
Benefits of Intercloud model	22

Challenges with Intercloud model	24
2.7 Cloud interoperability	26
2.8 Conclusion.....	29
3 Research Methodology and Objectives	30
3.1 Introduction	30
3.1.1 Overview	30
3.1.2 Research objective and Research Questions	30
3.2 Business and management research	30
3.2.1 Differing Approaches to business and management research.....	30
3.2.2 Research Philosophy	31
3.2.3 Research approaches	32
3.2.4 Choosing a research approach.....	33
3.3 Research strategies.....	34
3.3.1 Experiments	34
3.3.2 Case study	35
3.3.3 Grounded theory.....	35
3.3.4 Ethnography.....	35
3.3.5 Action Research	36
3.4 Appropriate Research strategies	37
3.4.1 Survey.....	37
3.5 Research Approach	38
3.5.1 Research Design	38
3.5.2 Research Method.....	38
3.6 Limitations.....	40
3.7 Conclusion.....	40
4 Research Findings	41
4.1 Introduction	41
4.2 Participant Overview.....	41
4.3 Company A.....	42
4.4 Company B	43
4.5 What are the interoperability barriers in Intercloud? (RQ1)	44
4.5.1 Themes identified – both old and new	44
4.5.2 Ocurring Themes.....	45

4.6	How can these barriers be overcome? (RQ2).....	46
4.6.1	Portability.....	46
4.6.2	Economy.....	50
4.6.3	Provisioning.....	53
4.6.4	Service Level Agreement.....	55
4.6.5	Security	57
4.6.6	Network	59
4.6.7	Monitoring	61
4.6.8	Cloud Standards	61
4.6.9	Autonomics	63
4.6.10	Customer demands	64
4.6.11	Risk management.....	64
4.6.12	Cloud Providers	65
4.6.13	People skills.....	66
4.7	Conclusion.....	66
5	Discussion and Conclusions	68
5.1	Introduction	68
5.1.1	What are the Interoperability barriers in Intercloud (RQ1)?	68
5.1.2	How can these barriers be overcome? (RQ2).....	69
5.2	Portability.....	71
5.3	Economy.....	72
5.4	Provisioning.....	74
5.5	Network	75
5.6	Service Level Agreements	76
5.7	Security	77
5.8	Monitoring	79
5.9	Cloud Standards (new).....	79
5.10	Autonomics	81
5.11	Customer demands (new).....	82
5.12	Risk Management (new)	82
5.13	Cloud Providers (new).....	83
5.14	People Skills (new)	84
5.15	Further research	85

5.16	Contributions	85
5.16.1	Methodological	85
5.16.2	Theoretical	86
5.16.3	Practical.....	88
5.17	Limitations.....	88
5.18	Conclusion.....	89
Appendix A: The Interview Guide.....		91
REFERENCES.....		94

LIST OF TABLES

Table 1: Top 10 reasons for using multiple Clouds (Petcu, 2014).....	18
Table 2: Benefits of Multi-Cloud	19
Table 3: Interview Overview	42
Table 4: Interview Themes occurrences	45

LIST OF FIGURES

Figure 1: Literature review approach funnel	6
Figure 2: Cloud Service stack source (Toosi, Calheiros et al. 2014).....	8
Figure 3: Hybrid Cloud (Toosi, Calheiros et al. 2014).....	14
Figure 4: Multi-Cloud (Toosi, Calheiros et al. 2014)	18
Figure 5: The Intercloud vision (Bernstein, Vij and Diamond, 2011)	22
Figure 6: Taxonomy of Intercloud challenges (Toosi, Calheiros et al. 2014)	25
Figure 7: Cloud interoperability motivations (Toosi, Calheiros et al. 2014)	27
Figure 8: The research process 'onion' (Saunders 2003)	31
Figure 9: Interview Themes - Green depicts new themes since 2014 (Toosi et al., 2014)	44
Figure 10: Top challenge for an organisation's cloud strategy (Forrester, 2022).....	66
Figure 11: Intercloud Challenges and Solutions.....	70
Figure 12: Taxonomy of Intercloud challenges 2023 – Grey depicts not mentioned in interviews - Green depicts new barriers based on this research since 2014 (Toosi, Calheiros et al. 2014) .	87

ABSTRACT

Intercloud is a cloud deployment model that interconnects multiple public cloud services together in a 'cloud of clouds'. Intercloud provisioning has the potential to be the next stage in cloud evolution, involving interconnected public clouds based on multiple underlying technologies. However, cloud service providers have still not adequately considered the inherent interoperability barriers for its realisation. This research revisits a 2014 study on cloud barriers and, almost a decade on, re-employs its framework to identify and detail intercloud interoperability barriers to provision, and posits approaches to overcome them. As a contribution to research, the study extends the framework, identifying the relative importance of interoperability barriers in 2023, paving the way for future research. For cloud service providers, the study identifies interoperability issues previously not considered, provides a relative importance of these issues, and approaches for mitigation.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Prof. Tom Acton, for all your help, advice, and guidance in completing this research. I couldn't have wished for a better supervisor. I really enjoyed our Friday meetups and the coffee!

I would like to thank my wife Sonya for listening to me talking about the merits of Intercloud while out for evening walks. Despite it not being her field of expertise, she still managed to provide valuable insights.

I would like to thank my work colleagues at CSG. John Tierney, Paul Finnegan and Andrew McCormack for their help and support with my studies over the last 2 years.

I'd like to dedicate this work to my late friend Bob P. and will try to live by his mantra "you have to keep working on yourself P".

1 Introduction

1.1 Background

Cloud computing is the delivery of different services provided on a “utility” basis via the Internet. These services include resources and applications like servers, data storage, networking, databases, and software hosted in large geographically dispersed data centers. The resources are hosted and managed by a service provider, who maintains the underlying infrastructure and ensures its availability and security. The Cloud computing data centres use virtualization technologies such as hypervisor-based virtual machines. Users can leverage these resources as per their requirements, scaling them up or down as needed, and paying only for the resources they consume. The services provisioned are automated and a user can be “up and running” on a new service in a matter of minutes. Within cloud computing there are service layers such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) that can be used in a single public cloud provider.

The hybrid cloud model is a commonly used deployment strategy, in which private clouds are extended through the services of a particular public cloud provider, without the need to build out new capacity and only “bursting out” to public cloud during peak usage times. Due to increasing competition among cloud providers, businesses are looking for cost-efficient providers to host their applications. The hybrid cloud model provides organisations with the flexibility to leverage the advantages of both private and public clouds, enabling them to meet specific business needs, optimise resource utilisation, enhance security, and maintain control over critical systems and data.

In some cases, certain parts of an enterprise application stack reside in one cloud while others might reside in a different cloud provider. Hence the emergence of a multi-cloud deployment model. In a multi-cloud, cloud interoperability has been restricted to use cases where a service running on one public cloud explicitly references a service on another public cloud, no implicit interoperability exists. Additionally, the provisioning, portability, monitoring, network, Service level Agreements (SLA) and billing services used by cloud service providers are heterogeneous and by design not interoperable. The multi-cloud model also introduces complexities in terms

of management, integration, and security. Multi-cloud also requires expertise in managing multiple cloud platforms, ensuring interoperability, and implementing appropriate security measures across different environments. To effectively implement a multi-cloud model, organisations typically need to utilise cloud management and orchestration tools that provide centralised control and visibility over various cloud resources. These additional tools are needed to help streamline operations, automate workflows, and optimise resource allocation across multiple clouds, however these tools can be complex to implement and require additional domain expertise. Although cloud standards bodies are trying to address some aspects of the interoperable challenges, a lot of gaps still exist. This is a concern for organisations that require flexibility and agility in their business. During the COVID-19 pandemic, there was an unprecedented surge in demand for cloud resources as organisations relied heavily on remote work, online learning, and digital services. Specific regions or cloud services experienced temporary resource constraints or performance issues during peak usage periods. Some online services faced disruptions or outages due to the surge in traffic and increased demand. Additionally, certain industries with unique requirements faced challenges in accessing sufficient cloud resources. It has become apparent to cloud users that no single provider can have the flexibility and capacity to meet all of cloud consumers' requirements. This has elevated the idea of sharing resources among cloud service providers. The basic idea behind an Intercloud deployment model is that services in multiple clouds can be interchanged in a seamless and explicit way. This study introduces and analyses the relevant aspects motivating cloud interoperability. The motivations for an Interconnected-cloud (Intercloud) include scalability, optimal performance, and pricing, avoiding vendor lock-In, high availability and disaster recovery, geographic distribution, and low-latency access, meeting regulations and saving energy. This research uses a framework of Intercloud challenges identified by Toosi, Calheiros and Buyya (2014) as the lens to identify common themes existing today and also to identify new themes that are now evident almost a decade later. Have these interoperability challenges been resolved by technological advances since 2014 or are cloud providers more siloed than ever? The reader will obtain an understanding of the interoperability challenges existing in the Intercloud model today and the research suggests some approaches to overcome the barriers to deploying applications in an Intercloud.

1.2 Motivation for study

Inter-connecting different clouds can provide dividends to both cloud users and cloud providers. Benefits from the cloud users's perspective include (Martino, 2015) (Grozev and Buyya, 2014):

- Vendor lock-in avoidance. If interoperability is enabled in inter-connected clouds, the cloud users can easily migrate elsewhere for better Quality ofService (QoS) and cost which would overcome the angst of being locked-in to one service provider.
- Wider geographic distribution. Different cloud providers from multiple locations around the globe can draw legislation-compliant services of cloud users and help reduce latency by having services physically located closer to their customers.

Benefits from the cloud provider perspective include the following:

- Enhanced scalability. The marketing rhetoric of limitless cloud resources claimed by cloud providers does have a limit. With the increasing demand on cloud computing resources, this limit would be increased by sharing resources.
- Cost and energy efficiency. The idle capacity of one cloud provider can be utilised by other interconnected clouds to cut down on capital and operational costs, allowing providers to deliver better Service-Level Agreements (SLAs) and QoS to their customers.

This research highlights the challenges for Intercloud realisation and identifies open issues and new challenges. The research then turns to how we can resolve these interoperability challenges.

1.3 Research Question

The purpose of this research is to study the interoperability challenges to an Intercloud and how these barriers can be resolved. From a provisioning perspective, the central research questions (RQs) are:

- RQ1: What are the interoperability barriers in Intercloud?
- RQ2: How can these barriers be overcome?

1.4 Research Method

This research is achieved by employing a qualitative exploratory research methodology involving semi-structured interviews. Purposeful sampling was used by the researcher to obtain participants who were especially knowledgeable in Cloud Computing. Analyses were then conducted on the resultant data from the interview recordings to determine whether the research questions could be answered.

1.5 Summary of chapters

Chapter 2: Literature review

This chapter presents the literature on the cloud computing journey from the one cloud to the hybrid, multi, inter and distributed cloud deployment models. It presents the attributes of quality and success of the different deployment models. History and core technologies in the context of cloud computing are discussed. Cloud interoperability motivations are also discussed.

Chapter 3: Research Methodology and Objectives

This chapter presents the methodology followed in this study. It discusses various viewpoints of business methods research and presents the most suitable standpoint for this research. The possible approaches to business research methods are presented and a semi-structured interview is put forward as the most prudent approach in the context of this research. The processes of setting up the interviews are presented, as are the reasoning for choosing the participants, and method of acquainting the participants with the research questions. Limitations resulting from these decisions are also presented.

Chapter 4: Research Findings

This chapter presents the findings from the research. The findings are detailed under the two research question headings. The researcher used the Toosi framework (Figure 6) as the lens to identify common themes in the research and identify new themes and sub-headings. It also provides an interview participant and company they work for overviews.

Chapter 5: Discussion and Conclusions

This chapter presents a summary of findings per RQs. It then summarizes the findings per theme heading (Table 4: Interview Themes occurrences) for each of the RQs and compares them to the literature review. It also provides an updated Toosi framework (Figure 12) for today. This chapter also defines research limitations and recommends topics for future research.

2 Literature Review

2.1 Introduction

This chapter presents a review of the literature discussing the cloud computing journey from the monolithic (or cloud Island ‘all in one’ cloud approach), to the hybrid, multi, inter cloud deployment models. Figure 1 shows the approach to reviewing the literature from Cloud, Hybrid, Multi and Inter. The review also explored the adoption and greater interoperability challenges along the way. The research examined the potential issues with moving towards a greater cloud federation or inter-connected cloud (Intercloud). To understand the factors that hinder the adoption of cloud interoperability it is important to understand the background technologies and architecture involved in the cloud service model. A literature review of the challenges in adopting a multi cloud approach for using cloud services was carried out to firstly identify the different options and then explore the challenges encountered with each cloud configuration. To enhance the understanding of the current literature, the research identified the published articles on cloud, hybrid, multi and inter cloud, its adoption, and challenges. The researcher used the university library online resources to databases such as Scopus and also Google Scholar. The further down the funnel (Figure 1) the less published material found.

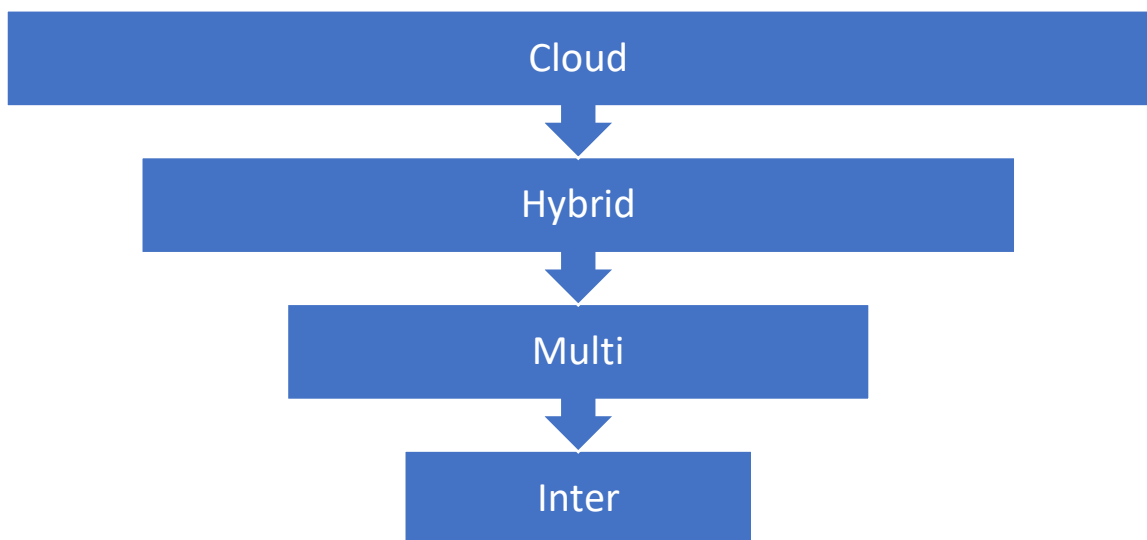


Figure 1: Literature review approach funnel

2.2 Cloud Computing

Xu (2012) indicated the main point to cloud computing is to provide on-demand computing services with high reliability, scalability and availability in a distributed environment. Xu also suggested Cloud computing is changing the way industries and enterprises do their businesses in that dynamically scalable and virtualized resources are provided as a on demand service over the Internet. Marston, Li et al (2011) concurs with this when suggesting “The evolution of cloud computing over the past few years is potentially one of the major advances in the history of computing. However, if cloud computing is to achieve its potential, there needs to be a clear understanding of the various issues involved, both from the perspectives of the providers and the consumers of the technology” (Ibid). There are a multitude of definitions for Cloud Computing. Some definitions are either too long or miss some of the important characteristics. One of the more concise and complete definitions encountered, encapsulating the key characteristics is this “In coming up with our definition, we tried to encapsulate the key benefits of cloud computing from a business perspective as well as its unique features from a technological perspective. Our formal definition of cloud computing is as follows: “It is an information technology service model where computing services (both hardware and software) are delivered on-demand to customers over a network in a self-service fashion, independent of device and location. The resources required to provide the requisite quality-of service levels are shared, dynamically scalable, rapidly provisioned, virtualized and released with minimal service provider interaction. Users pay for the service as an operating expense without incurring any significant initial capital expenditure, with the cloud services employing a metering system that divides the computing resource in appropriate blocks.” (Marston, Li, Bandyopadhyay, Zhang and Ghalsasi, 2011). Cloud computing is often described as a stack, with a broad range of computing services built on top of one another under the name *cloud*. End users can quickly acquire (Pay As You Go – PAYG) and use parts of bulk compute resources. “IaaS, SaaS, and PaaS are known as SPI (software, platform, infrastructure) models of cloud computing. These are stacked with servers that offer three types of cloud services” (Sultan, 2011). Figure 2 shows in simple terms the stack and the various service delivery models in layers sitting on “the stack”.

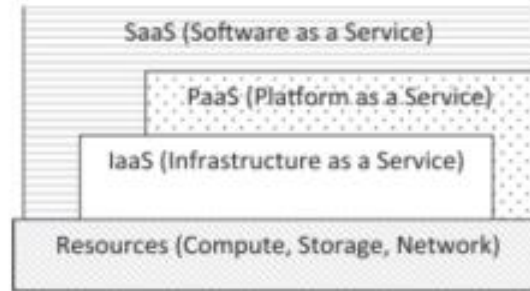


Figure 2: Cloud Service stack source (Toosi, Calheiros et al. 2014)

The researcher looked at these service delivery models in more detail. At the top of “the stack” is Software-as-a-Service or SaaS “SaaS offers a multi-tenant platform whereby common resources and a single instance of both the object code of an application and the underlying database are used to support multiple customers simultaneously. To this end, SaaS is also referred to as the Application Service Provider (ASP) model. Examples of the key providers are the Salesforce Customer Relationships Management (CRM) system. A major consideration in SaaS is effective integration with other applications. At the application level, the important aspects of scalability, performance, multitenancy, configurability, and fault-tolerance are primary considerations.” (Xu, 2012). Another commonly used SaaS example is Microsoft’s office 365 suite including the Outlook email service.

In the middle of “the stack” is Platform-as-a-Service or PaaS “PaaS as the name implies, provides developers with a platform including all the systems and environments comprising the life cycle of development, testing, deployment and hosting of sophisticated web applications as a service delivered by a cloud-based platform. Commonly found PaaS include Google App Engine, PaaS may offer a number of readily available services, which means that PaaS can support multiple applications on the same platform” (Ibid).

Towards the bottom of the stack and just above the hardware resources is the Infrastructure-as-a-Service or IaaS. “IaaS is sometimes called Hardware as a Service (HaaS). IaaS promotes a usage-based payment scheme, meaning that customers pay as they use. This service is extremely useful for enterprise users as it eliminates the need for investing in building and managing their own IT systems. Another important advantage is the ability of having access to, or using, the latest technology as it emerges. On-demand, self-sustaining or self-healing, multi-

tenant, customer segregation are the key requirements of IaaS. Rackspace is one of the pioneer IaaS providers. The Cloud model may also be defined as “cloud providers maintains multiple data centres which are dispersed in various parts of the world and those data centres are well interconnected”. “Cloud computing refers to both the applications delivered as services over the internet and the hardware and systems software in the data centers that provide those services” (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica and Zaharia, 2010).

Industry and enterprises are increasingly dependent on cloud services to meet their business requirements. In 2022, more than \$1.3 trillion in enterprise IT spending is at stake from the shift to cloud, growing to almost \$1.8 trillion in 2025 (Gartner, 2022). With the COVID 19 pandemic and the move to using remote computing services, this trajectory is set to continue in 2023 and beyond. When a cloud is available to the public in a pay-as-you-go manner, it is called public cloud, and when a cloud belongs to a business or an organization and not made available to the public, it is called private cloud. The focus of this research is on public cloud however as discussed in the hybrid cloud section, private cloud has a big role to play in meeting business infrastructure requirements.

2.3 History and Core technologies

As in most research fields it is important to understand the background and composition of the research topic. Cloud Computing is no different. An exploration on how this technology worked in the past helps us to understand how it came to work the way it is now. The research looked at how cloud computing was conceptualised, developed and evolved. Cloud computing builds on over 50 years of research in virtualisation, distributed computing, utility computing, networking, web, and software services. It implies a service-oriented architecture, reduced infrastructure technology knowledge overhead for the end-user, greater flexibility, reduced total cost of ownership, on-demand services with a multi-tenancy architecture that can increase revenues for the Cloud Service Providers while providing greater computing access and flexibility to the end user. To enhance the understanding of how Cloud Computing evolved over these decades the research required taking a more in depth look at some of these characteristics.

2.3.1 Virtualisation

“Virtualisation refers to abstraction of logical resources from their underlying physical characteristics in order to improve agility, enhance flexibility and reduce cost” (Golden, 2013). Virtualisation technology hides the physical characteristics of a computing platform from the end users. Virtualisation presents an abstract, emulated computing platform. This emulated computing platform behaves like “an independent system, but unlike a physical system, can be configured on demand, and maintained and replicated easily” (Marston et al., 2011). The computing infrastructure is much better utilised, leading to lower upfront and operational costs (one side benefit of virtualisation is the savings in real estate space for the data centres). While the concept of virtualisation has been in existence since the 1960s, it is only in the recent past that compute and networking resources have caught up to deliver the level of performance now required in an emulated system.

2.3.2 Multi-tenancy

A related characteristic is that of multitenancy, whereby a single instance of an application software can (unknown to them) serve multiple end users. This allows more efficient utilisation of system resources (resource pooling) in terms of memory and compute processor overhead. This cuts out on a lot of duplication.

2.3.3 Web services

The World Wide Web Consortium (W3C) is the main international standards organisation for the World Wide Web. Founded in 1994 the consortium works in the development of standards for the WWW. The W3C define a Web Service as “a software system designed to support interoperable machine-to-machine interaction over a network”. The most common protocol used for clients and servers communicating is over HTTP. As a request-response protocol, HTTP gives users a way to interact with web resources by transmitting messages between clients and servers. HTTP clients generally use Transmission Control Protocol (TCP) connections to

communicate with servers. “Web services help standardize the interfaces between applications, making it easier for a software client (e.g. a web browser) to access server applications over a network” (Marston et al., 2011).

The combination of the development of these core technologies with advances in networking and high speed internet availability made the possibility of virtual on demand cloud computing the reality it is today.

2.4 Advantages of Cloud Computing

Historically, IT systems were designed to run on custom-built IT infrastructure. Applications that run on these systems required their own set of custom configurations of compute, memory and storage. Enterprises needed highly skilled in-house infrastructure experts to configure and maintain their IT systems. Capacity planning for the future was difficult and unpredictable. Cloud computing allows users to access computing services and resources on demand without having to buy their own infrastructures (or physical data centre building) and to pay only for what they use (Kogias, Xevgenis and Patrikakis, 2016). If enterprises undersized their infrastructure requirements they risked hitting capacity shortfalls and possible delays in procurement and configuring. If over estimated they were paying for unused capacity and the overheads associated with this. Cloud computing can take away some of these capacity planning burdens. It can also help to standardise and increase automation across IT systems, allowing the possibility to innovate faster.

2.5 Cloud Computing Challenges

While the benefits of cloud computing around flexibility and availability are well documented several challenges remain. Some of the key inhibitors to cloud are listed.

2.5.1 Technical Issues

The expectation is that cloud services and data stored in the cloud are available all the time. “Despite the salient features of cloud computing, cloud services may be interrupted due to various issues” (Wu, Wang, Lu, Qi, Shan and Luo, 2020). One issue is internet availability, which as everyone has experienced, also has outages. Technical glitches do occur for every cloud service provider (CSP). There have been numerous examples of a particular Cloud Providers cloud data centre being offline or even a full regions with multiple data centres experiencing an outage.

2.5.2 Security

Cloud computing creates a large number of security issues and challenges. Storing sensitive information and data on the cloud could make the organisation more vulnerable to external cyber attacks over the internet. Companies also need to realise that their data (which may be highly sensitive) is in essence being handled by the 3rd party Cloud Provider. Companies need to make the right decision in choosing a reliable Cloud Service Provider (CSP) to handle their data. Bohli, Gruschka, Jensen, Iacono and Marnau (2013) suggests that “even though in the majority of cases it may be legitimate to assume a cloud provider to be honest and handling the customers’ affairs in a respectful and responsible manner, there still remains a risk of malicious employees of the cloud provider, successful attacks and compromise by third parties, or of actions ordered by a subpoena”. Companies also need to ensure that their CSP complies with local or regional regulatory requirements such as GDPR in the euro zone. Ünver (2019) suggests that “given the actual and potential problems as to the cloud interoperability, a cloud-focused attention needs to be upheld by EU policy makers”. Cloud interoperability and sharing of data across cloud data centres and borders could make this even more difficult to meet regulatory requirements.

2.5.3 Cost

Migrating from current infrastructure to a cloud computing one is a risky and expensive matter. The main question when considering cloud computing migration is the investment's effectiveness and return on investment (Xinhui, Ying, Tiancheng, Jie and Fengchun, 2009). Initially using cloud services may appear to businesses to be cost effective in comparison to running their own data centre in a physical building. However, companies need to look carefully at various pricing plans to ensure they are getting the best value for the services they consume. Also they may need to have strict policies in place around shutting down and/or terminating cloud services when not being used. Unchecked cloud useage can quickly spiral out of control and can lead to high unexpected usage bills. The size of a company's cloud budget also impacts their ability to receive larger discounts as they scale.

Most cloud customers are unaware of proprietary standards which inhibit interoperability and portability of applications when taking services from Cloud Providers. Vendor lock in to a certain CSP can prove costly. "In economics, vendor lock in is a situation where a customer becomes dependent on a vendor for its products or services and cannot move to another vendor without considerable cost and technical effort. It is also perceived as one of the current drawbacks of cloud computing" (Armbrust et al. 2010). With respect to cloud computing, vendor lock in is the direct result of noncompatible underlying technologies and the implicit lack of interoperability. Some of the the big CSP's are not making life easier for customers to switch to another provider if they wanted to. Having customers pay only for what they use, while combining different services as needed, is a major advantage of cloud computing. At certain CSPs "service dependency" within their cloud is seen as a competitive advantage. The larger cloud providers also have a habit of making it cheap and easy to transfer data onto their clouds but pricey to move them out again. Some potential strategies to avoid vendor lock in are to try to select a CSP that support standardised formats and protocols regarding APIs in particular and an awareness of commonalities and dependencies among cloud-based solutions.

2.6 Cloud deployment models

The researcher wishes to differentiate the various cloud deployment models and attempt to categorise them. Hybrid-cloud can be defined as being Private (on-prem) cloud plus one public cloud provider. Multi-cloud can be defined as having no federation between public clouds – a company uses different public cloud for different services – e.g. CP A for Application 1 and CP B for application 2. Multi-cloud has no interoperability. The term Multi-cloud can denote the usage of multiple and independent Clouds by a client or a service. Intercloud on the other hand is a federation of 2 or more public clouds e.g. running an application across 2 public clouds that are interoperable. The difference being by the degree of collaborations between the Clouds involved and by the way by which the user interacts with the Clouds.

2.6.1 Hybrid Cloud

“In hybrid cloud architecture, an organization that owns its private cloud moves part of its operations to external or public Cloud Providers. This extension of a private cloud to combine local resources with resources from remote CPs is called hybrid cloud” (Toosi et al., 2014).

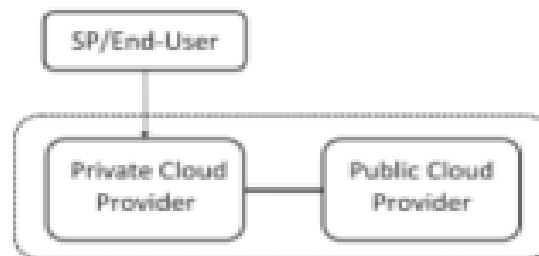


Figure 3: Hybrid Cloud (Toosi, Calheiros et al. 2014)

The advantage of such a hybrid cloud deployment from a cloud user’s perspective is that an organization only pays for extra compute resources only when they are needed (Martino, 2015). IDC data shows an overwhelming 97% of enterprises have adopted hybrid cloud (Turner, 2021). “Cloud bursting” is the simplest and most common hybrid scenario, in which an

application that is executing in a private cloud bursts into a public cloud when the demand for computing capacity spikes.

Benefits of hybrid model

Hybrid cloud is the preferred model allowing enterprises to maintain a degree of control while maximizing cost savings and performance by taking advantage of the fast provisioning capabilities of public cloud (Radhika and Sudha Sadasivam, 2021). One of the most examined federation scenarios is the hybrid cloud model, also called “cloud bursting”, which combines the existing on-premise cloud infrastructure (e.g., a private cloud managed by a cloud manager, such as VMware) with external resources from one or more public clouds (e.g. Amazon EC2 and Azure VMs). This model allows for the possibility to transform the local datacenter’s in to a highly scalable hosting environment. The hybrid cloud model is a widely used solution to satisfy the compute demands of many organisations. These organisations usually have their own on-premises private cloud infrastructures to support the internal compute infrastructure requirements. Their infrastructures are often oversized to meet any peak demand periods, and avoid performance issues. Adopting a hybrid cloud solution enables the reduction of the on-premises infrastructure size, so that it can be sized for an average load, and it can then be boosted with external resources from a public cloud provider to satisfy peak demands. Another motivation is the ability to run sensitive applications without leaking their data into the public segment of the hybrid cloud (Azumah, Sørensen, Montella and Kosta, 2021). Some open cloud platforms, such as OpenNebula, offer a single management point for both local private and remote public cloud resources, enabling users to decide whether their resources are deployed in local infrastructure, or in the public cloud.

Challenges with hybrid model

“Cloud federation is the practice of interconnecting two or more private or public cloud infrastructures” Köstler, Gebauer and Reiser (2021). The term cloud federation implies the creation of a group of aggregated providers that are mutually collaborating to share their resources in order to improve each other’s services (Kurze, 2011). Cloud federation enables

cloud providers to cooperate and allocate their resources to create a large virtual pool of resources at multiple network points. This model improves the competitiveness of IT companies, datacenters and cloud providers, since it offers the possibility of increasing its computing and storage capacity, on an on-demand basis at a reduced cost, and also brings other important benefits, such as vendor lock-in avoidance, higher availability, service portability and geographical accessibility. In general, an overall improvement on the Quality of Experience (QoE) for end-users. “Despite these benefits, CSPs are hesitant to contribute to cross-cloud federation, mainly due to the lack of confidence and trust among CSPs” (Ahmed, Raza and Hussain, 2019).

One of the main challenges for a Federated Cloud is to define the mechanism used for the allocation of resources between the sites composing it. Such a mechanism needs to be fair and ensures mutual benefits for all the parties involved (Gomes, Vo and Kowalczyk, 2012). Many different federation scenarios are possible, such as cloud brokering, cloud peering, or hybrid cloud architectures, among others, which exhibit different level of coupling and interoperation among the cloud resources. Although hybrid cloud is a very widely used deployment model, current hybrid platforms reveal a major limitation which is - the lack of federated network provisioning services to allow the seamless and efficient interconnection of resources distributed among different clouds. “In a typical hybrid cloud scenario, resources from different clouds are seen as separated resources, located at independent remote networks with their own addressing schemes and attributes” (Moreno-Vozmediano, Montero, Huedo and Llorente, 2017). In this configuration the end-user is responsible for implementing their own network interconnectivity (e.g. VPN tunnels, overlays, secure channels, etc.) to enable connectivity between geographically dispersed cloud resources. Many public cloud providers offer the possibility of creating site-to-site Virtual Private Network (VPN) tunnels (e.g. Amazon VPN Services, Google Compute Engine VPN, or VPN Azure Service), which provide secure Layer 3 (L3) connectivity between the private local cloud network and the remote network deployed in the public cloud. However, these VPN services exhibit several drawbacks. First, each cloud provider exposes its own interfaces, configurations methods, and software and/or hardware requirements to instantiate and configure the VPN tunnels between the local infrastructure and the remote cloud provider, so the manual configuration of these VPN connections for different providers would require very experienced users with advanced administrative skills. Second, these VPN based solutions do not scale properly when the number of clouds involved

increases in the multi hybrid configuration, due to the configuration complexity, since the user has to manually configure many different VPN tunnels between the different cloud instances. VPN services offered by public clouds only provide L3 connectivity, so each network has its own addressing scheme, and the VPN ends act as gateways that encapsulate and route the L3 traffic between the remote networks. In the last few years, the implementation and deployment of Layer 2 (L2) virtual overlay networks for hybrid scenarios is now supported by the partnering of some cloud providers and cloud management platform (e.g. VMware cloud on AWS and Azure VMware) L2 overlay networks present many advantages, first they are independent of the network protocol, so they allow to capture not only IPv4 traffic, but also IPv6 traffic, and non-IP traffic; second they support broadcast and multicast traffic, so they are suitable for deploying applications based on broadcast or multicast; third they natively support mobility and migration, since hosts in different sites share a common overlay addressing scheme, so these hosts can be moved from say a private cloud to a public cloud with minimal reconfiguration requirements (Moreno-Vozmediano et al., 2017). However the the lack of a comprehensive federated network provisioning services to allow the seamless and efficient interconnection of resources distributed among an Intercloud still remain.

2.6.2 Multi-Cloud

Multi-cloud refers to the distribution of cloud assets and applications across several different Cloud Service Providers. “Using resources and services from multiple Clouds is a natural evolution from consuming the ones from in-silo Clouds” (Petcu, 2013). Multi-cloud refers to leveraging more than one of those multiple cloud solutions providers for your enterprise operations. Using resources and services from multiple Clouds is a natural evolution from consuming from a single Cloud Service Provider. The usage of services and resources from multiple clouds is driven by the needs of their consumers expressed in simple requirements, like service quality and cost.

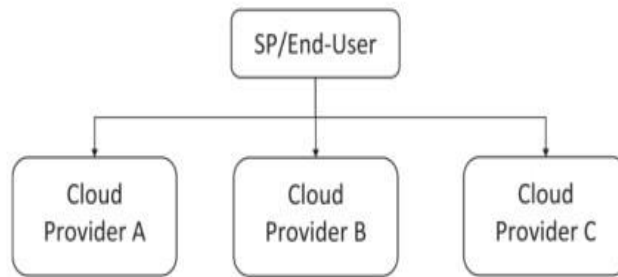


Figure 4: Multi-Cloud (Toosi, Calheiros et al. 2014)

At Microsoft, Azure cloud costs are often rolled into the “enterprise agreements” which include other services such as Office 365, all-encompassing subscriptions that big companies typically sign up to. Many companies that would have traditionally used Amazon cloud services are realising by leveraging and expanding on their existing agreements they can receive large discounts for Microsoft Azure services. GCP (Google cloud) being the smallest of the top three, “strongly believes” in the “multi-cloud”, says Amit Zavery, a senior executive. In other words, it aims to enable customers to choose the best and cheapest cloud services from different providers - thus making it easier for them to pick Google (The-Economist, 2021). Another increasingly popular configuration is “Hybrid multi-cloud” which is a combination of multiple public clouds, along with an on-premises environment. 92% of enterprises do business with two or more cloud service providers (Turner, 2021). Table 1 shows the reasons for using ‘multiple clouds’ – types of use are Serial (multi-cloud) and simultaneous (Intercloud).

Type of use	Reason
Serial usage	Optimize costs or improve quality of services
	React to changes of the offers by the providers
	Follow the constraints, like new locations or laws
	Avoid the dependence on only one external provider
	Ensure backup-ups to deal with disasters or scheduled inactivity
Simultaneous usage	Deal with the peaks in service and resource requests using external ones, on demand basis.
	Replicate applications/services consuming services from different Clouds to ensure their high availability
	Act as intermediary
	Enhance own Cloud resource and service offers, based on agreements with other providers
	Consume different services for their particularities not provided elsewhere.

Table 1: Top 10 reasons for using multiple Clouds (Petcu, 2014)

Benefits of Multi-Cloud model

There are many different reasons why the services and resources from multiple Clouds are needed.

Petcu (2013) describes these reasons and these are added to Table 2:

Benefit#	Benefits of Multi-Cloud	Beneficiary
1	deal with the peaks in service/resource requests using other cloud providers, on demand basis	Cloud Provider
2	optimise costs or improve quality of services	Cloud Consumer
3	react to changes of the offers/services/price by the providers	Cloud Consumer
4	Adhere to data sovereignty laws, more locations	Cloud Consumer
5	replicate the applications or services consuming resources/services to different Cloud providers in more than one location to ensure their high availability	Cloud Consumer
6	avoid the dependence on only one cloud provider (lock-in)	Cloud Consumer
7	ensure backup-ups to deal with disasters or scheduled inactivity	Cloud Provider
8	act as intermediary	Cloud Provider
9	enhance own Cloud resource and service offers, based on agreements with other providers	Cloud Provider
10	consume different services for their particularities not provided elsewhere	Cloud Consumer

Table 2: Benefits of Multi-Cloud

Even if cloud interoperability is not supported in multi-cloud by cloud providers, cloud consumers can still benefit from client-centric interoperability facilitated by user-side libraries or third-party brokers. Multi-cloud application stack deployment using an API layer provides the possibility to run applications on several clouds. (Toosi et al., 2014). From a Cloud Providers perspective, they are interested in benefits 1,7,8 and 9 from table 2. While Cloud consumers are interested in benefit 2,3,4,5,6 and 10.

Challenges with Multi-Cloud model

In a multi-cloud, the available public clouds are independent, and their resources are managed by the individual providers, so the interconnection between providers is not voluntary. This means that inter-communications need to be set up and configured. Cloud diverseness results from having different PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) service offerings provided by Cloud Providers. Consequently, SaaS services cannot easily port between different clouds due to the need for code customisations. SaaS, PaaS, and IaaS services interface via exchanging messages. A message indicates the action to be performed by the service receiving the message. As Cloud service providers use different protocols and definitions to manage this messaging, a communication incompatibility issue can arise due to incompatibilities (Elgedawy, 2015).

Ensuring data consistency across multi-clouds is also a major challenge. Cloud users usually choose cloud storage at design time, then create their applications based on this storage. This approach limits the agility of business services, as it tightly couples them to the chosen data consistency storage approach. Ensuring data security is also considered a major challenge in a multi-cloud environment. For example, when dealing with SaaS applications, the major security concern is often about the data protection and location, the security policies of the cloud providers. A multi-cloud environment is dynamic and complex, the traditional security solutions are no longer effective in dealing with the multi-cloud security issues. Protecting the private and critical information from loss or theft, facing control and privacy issues, guaranteeing data integrity and confidentiality are some of the challenges involved while dealing with Multi-cloud. (Lahmar and Mezni, 2018).

Interoperability is another challenge in a multi-cloud when an application needs several cloud platforms and have to communicate and cooperate. Similar service offerings across clouds have different granularities and varying complexities, which make the cooperation between heterogeneous cloud environments more and more difficult. "Cloud interoperability requires cloud providers to adopt and implement standard interfaces, protocols, formats, and architectural components that facilitate collaboration" (Toosi et al., 2014). The required standards and common protocols across clouds are currently lacking. The literature revealed that the challenges with a multi-cloud are also the challenges with an Intercloud. These

common challenges are discussed in more detail under 2.6.3. The literature also revealed that many of these common challenges revolve around the lack of Cloud Interoperability. Cloud interoperability is discussed in more detail in section 2.7.

2.6.3 Intercloud

The term Intercloud has been described as a “cloud of clouds”, essentially, an Intercloud allows for the dynamic coordination and distribution of load among a set of cloud data centres. (Grozev and Buyya, 2014). Intercloud means that integration must take place between two services, with each service on a different cloud infrastructure. Intercloud is important for use cases where a company is seeking to integrate data and analytics workflow across different services/clouds. Buyya, Ranjan and Calheiros (2010) describes an Intercloud as a federated Cloud computing environment that facilitates just-in-time, dynamic, and scalable provisioning of application services, consistently achieving Quality of Service targets under variable workload, resource and network conditions. Intercloud is an advanced form of multi-cloud. If multi-cloud consists of using two or more cloud solutions, Intercloud takes that usage a step further. Intercloud means a company uses more than one cloud solution to actively manage data in the same application. In practice, this would look like a hybrid environment with its resulting complex architecture requirements, but between two or more public clouds. An example would be running a Microsoft PowerBI dashboard in Azure for Salesforce based in AWS. Intercloud is when a company uses more than one cloud to work together with the same data. The Intercloud Technology Forum (GICTF) was established in Japan in July 2009 to study subjects for Intercloud Computing schemes and to promote standardization for corresponding technologies. The aim of the GICTF is to provide “– on a global scale – higher-reliability and higher-quality Cloud services in case of service failures of Cloud systems caused by natural disasters”. (Aoyama and Sakai, 2011).

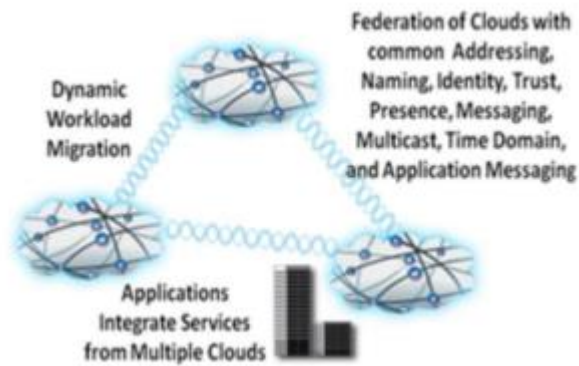


Figure 5: The Intercloud vision (Bernstein, Vij and Diamond, 2011)

Benefits of Intercloud model

A Cloud computing model, where a client utilises a single cloud data centre, introduces several challenges. A cloud service unavailability can leave end customers relying on a potential single point of failure and without access to essential and paid for resources. Reliance on a single cloud data centre makes it more difficult to implement SLA's, adequate performance and usability to clients distributed globally. The goal of an Intercloud is to reach a “higher level of sustainability by autonomously shifting resources among the participating Cloud systems when unexpected load levels occur or disasters strike” (Aoyama and Sakai, 2011). The benefits of an Intercloud for consumers are numerous and can be summarised as:

- Diverse geographical locations for cloud data centres. Leading cloud providers have established data centres globally. However not every cloud provider has established cloud data centres in every country. Some customers may have legislative requirements as to where their data can be stored. A data centre within a region of countries may not be enough, it may be that to meet legislative demands data has to be stored within the boundaries of a specific country. By utilising Intercloud consumers can access a more widely distributed network of resources, providing performant and legislation-compliant services to consumers. An Intercloud provides an opportunity for the cloud provider to identify another provider able to meet the regulations due to the geographical location of its data center (Toosi et al., 2014). In this way data backed up to a remote site can still meet data regulations for that region.

- Better application fault tolerance. In the past, there have been several cases of major regional cloud service outages. Most critical cloud applications are designed to be highly available and to use multiple cloud data centres for fault tolerance. Using resources from different cloud providers mitigates the risk of a cloud provider outage and supports high availability (Martino, 2015). It also provides an alternative should a provider be unavailable due to a natural disaster, or shutdown for a regulatory or legal reason.

- Avoid vendor lock-in. By using an Intercloud and being able to freely migrate workload among cloud providers, a consumer can avoid vendor lock-in. They lessen the impact and exposure if a cloud provider decides to increase service pricing, giving them the potential to quickly migrate to another provider. Most of the Multi/Inter cloud research efforts found in the literature were focused on helping eliminating the barrier of vendor lock-in (Petcu, 2013).

Overall, the main benefits of an Intercloud to cloud consumers is that they can diversify their cloud infrastructure portfolio in terms of both providers and location. This can help make their businesses operations more adaptable to cloud provider's policy and availability changes and more easily expandable in new legislative regions. Cloud service providers may also benefit from engaging in an Intercloud. The foundational idea of Cloud computing is that a cloud service should be available, elastic and scalable to meet the customer's requirements (Marston et al., 2011). A cloud provider should ensure enough resources to meet demand at all times. They make promises of infinite capacity but the reality is they have limited capacity. Workload spikes can come unexpectedly, and thus, cloud providers need to overprovision resources to meet them. During the COVID pandemic capacity constraints were seen with Cloud Providers in some regions due to high demand for providing cloud remote services. Another issue is the huge amount of data centre power consumption . Keeping an excess of resources in a ready to use state at all times for coping with unexpected load spikes leads to increased power consumption and cost of operation. Power management has become an increasingly prominent concern in cloud data centers (Gao, Guan, Qi, Song, Huan and Liu, 2014). Power shortages in certain countries where cooler climate is appropriate for data centres is an ongoing concern. The rollout of new Data centres to meet capacity demands can often be delayed due to planning/power consumption restrictions in certain countries.

Cloud providers' benefits can be summarised as follows:

- Expand on demand. Being able to offload to other clouds, a provider can scale in terms of resources like cloud-hosted applications do within a cloud. A cloud should maintain in a ready to use state enough resources to meet its expected load and a buffer for typical load spike. If the workload increases beyond these limits, resources from other clouds can be leveraged. This can maintain the illusion of "infinite capacity" (Martino, 2015).

- Better service level agreement (SLA) to customers. When Cloud Providers are aware that their customers workload can easily switch providers they are more likely to try to limit outages, increase capacity and provide a better all round Quality of Service to customers.

Achieving these benefits for both cloud providers and consumer should be done without compromising business applications requirements. Appropriate application brokering (consisting of provisioning and scheduling) should meet the requirements in terms of performance, responsiveness and legal considerations. The literature surveyed presented various Cloud Brokering techniques showing their strengths and weaknesses/limitations (Chauhan, Pilli, Joshi, Singh and Govil, 2019). The taxonomy for brokering in an Intercloud includes pricing, quality of services and optimisation.

Challenges with Intercloud model

The literature highlighted the challenges associated with Intercloud are similar to multi-cloud. These challenges are summed up in Figure 6. When reading the literature from 2014 the researcher considered if these challenges have been resolved or are still relevant today?

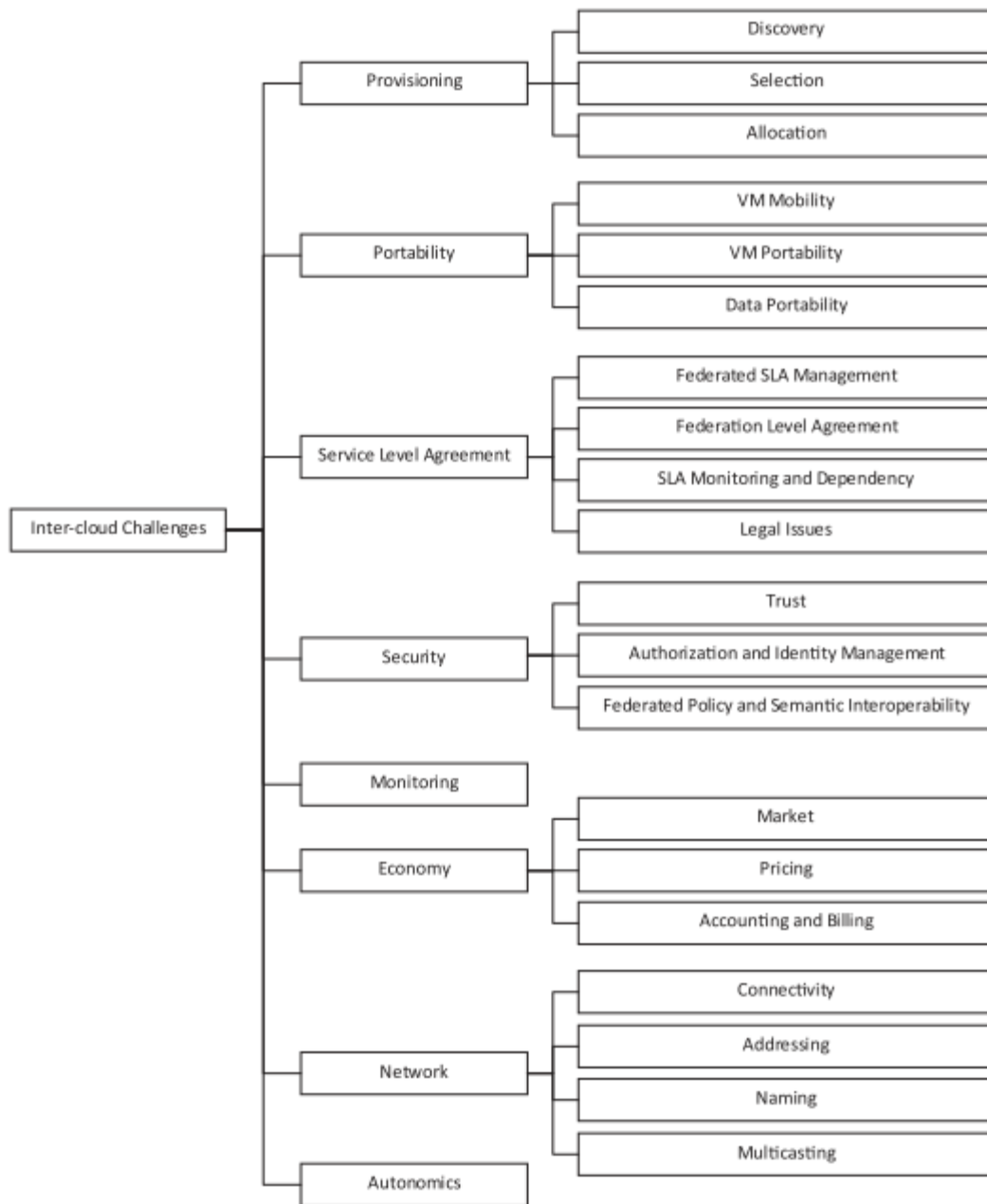


Figure 6: Taxonomy of Intercloud challenges (Toosi, Calheiros et al. 2014)

To resolve the issues in Figure 6 formal agreements between large Cloud providers would need to exist, however these are difficult to achieve, especially due to the need to control the resources and services that the external provider is expected to obtain for its benefit. The smaller Cloud providers may see a business opportunity to enter into such agreements to enhance their offering and to avoid the cases when potential users are not served due to the lack of sufficient resources. The literature highlighted a number of projects involved in

Intercloud initiatives (Martino, 2015). In an Intercloud more than one cloud works together with the same data. A big consideration to look out for in Intercloud environments are data egress charges, which are the fees a cloud user may see accumulate quickly as they move data out of one cloud and into another. Best practice data flow design can mitigate against these charges. Lack of agreement and standards on these data charges hinder interoperability.

The challenges highlighted in Figure 6 are a direct consequence of the lack of interoperability between clouds (Kaur, Sharma and Kahlon, 2017). When researching multi-cloud and Intercloud the main theme highlighted in the literature was the need for interoperability between clouds; it is the crux of the research.

2.7 Cloud interoperability

“To satisfy the demand for collective and collaborative cloud use, academia and industry want to interconnect heterogeneous clouds to form a federated system. This approach is promising but also faces significant challenges” (Kogias et al., 2016). The demand for interoperable cloud services has grown as cloud users see the limitations of using a single cloud provider. Cloud users may want to cherry pick the services they use from various Cloud providers. Reasons could include service availability in particular region, quality of service or cost. In the early days of Cloud, most businesses branching out from their own data centre started with just a single cloud provider. Back then public cloud choice was limited and the perception that keeping all application workloads in one cloud made for easier maintenance and less expensive than training and certifying their IT staff for multiple public clouds. However, things have moved on and today there are several big public cloud players in the market, all offering compute, storage, and networking capabilities combined with a plethora of services. Cloud users now realise that different clouds suit different applications based on the service offering of the cloud provider. There are also key business reasons for a shift in thinking towards distributing their application workloads. Businesses are not comfortable trusting their key applications to a single public cloud provider. They have concerns around reliability and security risks in having all their eggs in one basket. Vendor lock in is also a key concern (Martino, 2015), businesses do not like to become dependent on a vendor for products, unable to use another vendor without

substantial switching costs. “The benefits of interconnected cloud environments for both cloud providers and their clients are numerous and there are essential motivations for cloud interoperability, which will eventually lead to the Intercloud” (Toosi et al., 2014).

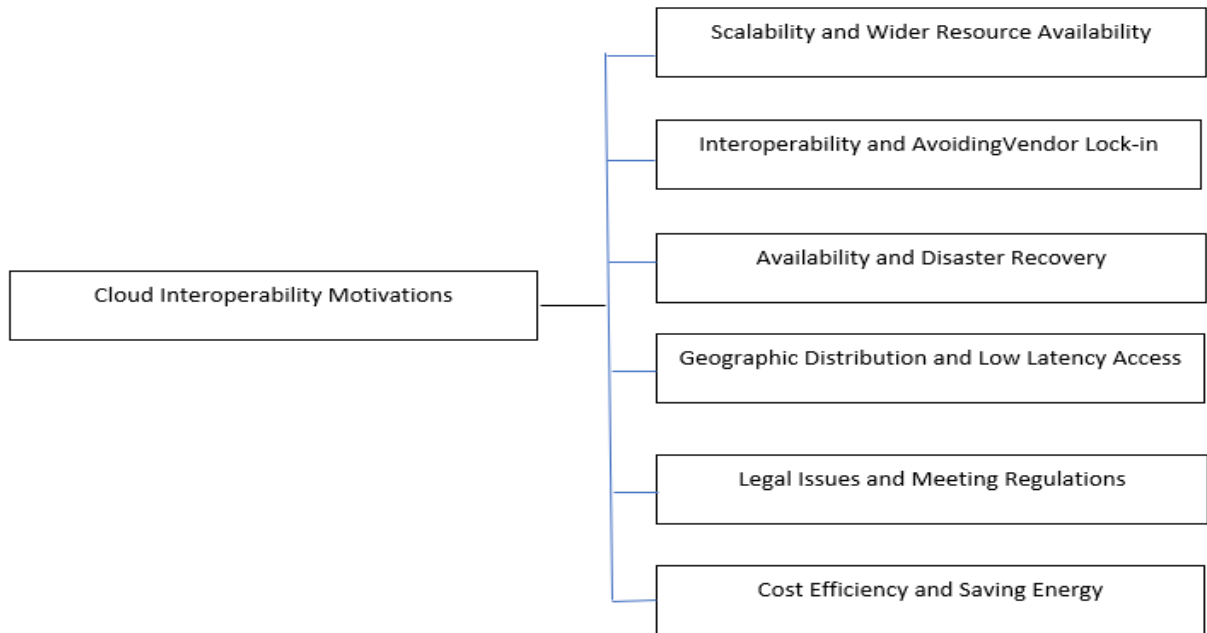


Figure 7: Cloud interoperability motivations (Toosi, Calheiros et al. 2014)

Cloud environments include a multitude of independent, heterogeneous, private, and public clouds. Posited by Celesti, Galletta, Fazio and Villari (2019), the evolution of cloud computing can be hypothesized in three subsequent phases: monolithic, vertical, and horizontal federation. In the monolithic stage, cloud providers are based on their own proprietary architectures that create islands of cloud. Cloud services are delivered by different providers in this stage. During the COVID pandemic capacity constraints were seen with CPs in some regions due to high demand for providing cloud remote services. There may have been plenty of capacity on another Cloud Provider in the same region but lack of interoperability is a limitation for the end user. In the vertical supply chain stage, some cloud providers leverage services from other providers. For example, a SaaS provider deploys services of an IaaS provider to serve its own customers. In horizontal federation, different cloud providers federate themselves to gain the benefits of a federation. For example, a fully utilised IaaS provider may use resources in an underutilised provider to accommodate more VM requests.

Interoperability can happen between clouds at different levels of the cloud stack layers. Interconnection between a PaaS and IaaS provider would be a vertical federation. If interconnection between clouds happens at the same layer (e.g., IaaS to IaaS), we call this horizontal federation. The adoption of the latter faces many more hurdles.

Villegas et al. (2012) considers that a federated cloud structure can be viewed as a vertical stack comparable to the layered cloud service model. At each layer, a service request can be served either through local resources using delegation or by a partner cloud provider through federation. If cloud interoperability requires cloud providers to adopt and implement standard interfaces, protocols, formats, and architectural components that facilitate cooperation, this is provider-centric interoperability. Cloud federations are multiple clouds organisations utilised to help to address problems that arise in monolithic clouds. For example, the European Grid Infrastructure (EGI) maintains a cloud federation¹⁴ to help researchers from several countries to solve problems that require large amounts of processing that cannot be handled by monolithic clouds (Assis and Bittencourt, 2016). Although these federations exist, a lack of formalisation can be observed. The lack of formalisation of cloud federations brings difficulties especially if no formal cooperation contract is agreed which is needed as a mechanism for the maintenance of the system integrity. Furthermore, as in most distributed computing, security is also a challenging issue due to a lack of a defined “periphery” (Bernstein et al., 2011). Advances have been made in interoperability but seamless interoperability may still be an aspiration. Cloud promises infinite capacity, but due to lack of interoperability this has been a challenge. Cloud interoperability could help meet peak capacity requirements.

2.8 Conclusion

The literature review showed a general absence in Intercloud literature between 2015 and 2021. Most of the literature found on Intercloud was from 2010 to 2015. This chapter presents an outline of research to date on cloud, hybrid, multi and intercloud. It also presents an initial view of some of the interoperability challenges for intercloud. A widely used framework for discussing challenges with Intercloud is the “Taxonomy of Intercloud challenges” (Figure 6) identified by Toosi et al. (2014). The researcher used the Toosi framework as the lens to identify common themes in the research and identify new themes and sub-headings to update and augment the framework a decade on. As the Interoperability barriers in Intercloud became apparent, it also became evident these barriers are still not resolved. The researcher was presented with an opportunity to research into identifying the most salient barriers today.

3 Research Methodology and Objectives

3.1 Introduction

3.1.1 Overview

This chapter outlines the research methods available, and the choice of method used for the research. It outlines the classification of approaches to research methods available for business and management research. The suitability of methods is discussed from which the research approach is presented. The research approach discusses in detail the implementation of the research method and the implicit limitations derived.

3.1.2 Research objective and Research Questions

The objective of this research is to identify and understand the interoperability barriers facing software service providers with adopting an Intercloud to host their software and how these barriers may be overcome.

Following the literature review, the following two Research Questions (RQs) emerged:

- RQ1: What are the interoperability barriers in Intercloud?
- RQ2: How can these barriers be overcome?

To build a foundation on how to address these questions for the purposes of the study it is important to understand and provide a background into appropriate tools and techniques. These will be discussed in the following sections.

3.2 Business and management research

3.2.1 Differing Approaches to business and management research

As Saunders (2003) states there are differing approaches to research and many important layers of the research 'onion' (Figure 8) to peel away before getting to the data collection

methods to use. As we move through the chapter each of these approaches and important layers will be discussed.

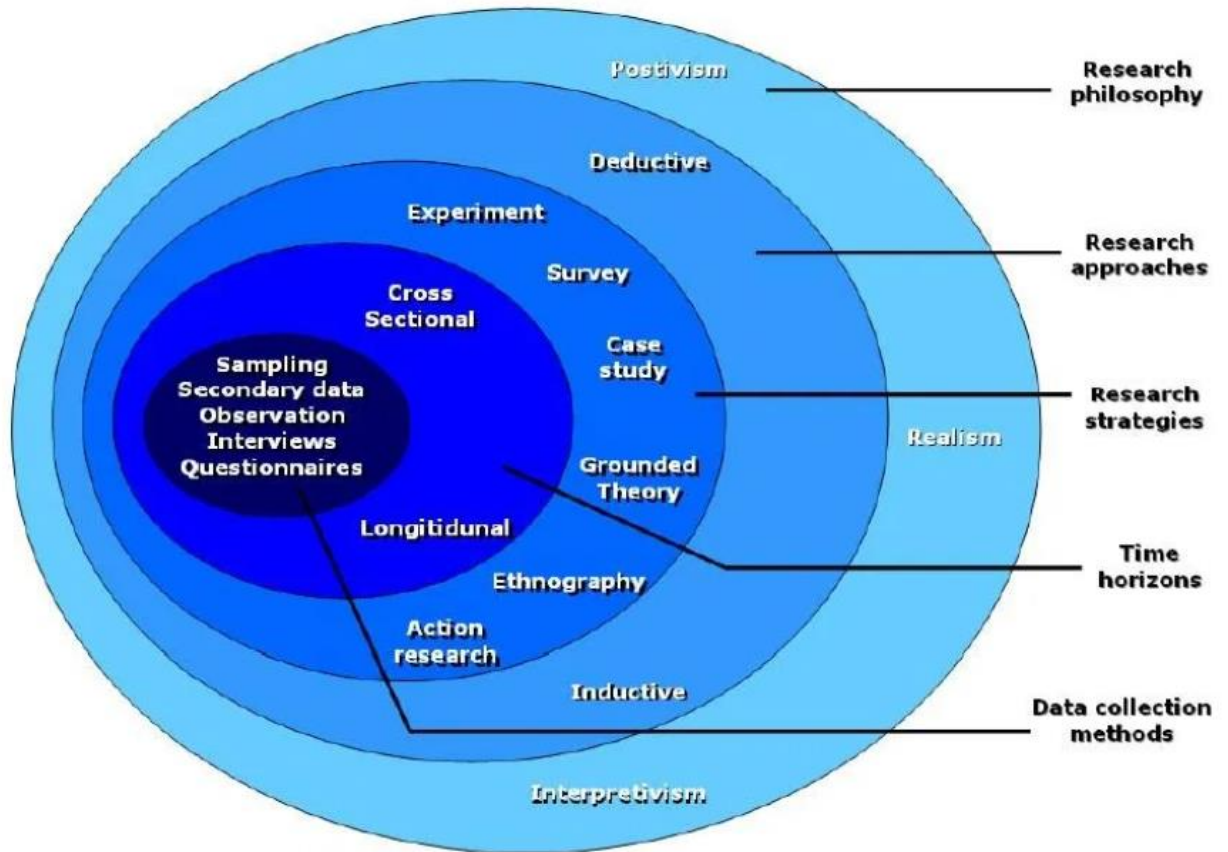


Figure 8: The research process 'onion' (Saunders 2003)

The appropriate approach for a particular study is also reliant on a research philosophy.

3.2.2 Research Philosophy

Creswell (2018) suggests that “individuals preparing a research proposal or plan make explicit the larger philosophical idea they espouse”. The first of Saunders (2003) onion layers (Figure 8) prompts the researcher to think about the research philosophy to adopt. A research philosophy is a belief about the way in which data about a research topic should be gathered, analysed and used. Epistemology is about the nature and creation of knowledge and addresses the question of what it is possible to know and what counts as knowledge (Braun, 2013). The

way we think about the development of knowledge affects the way we go about doing research. Saunders (2003) declares three views of research philosophy dominate the literature: positivism, interpretivism and realism. They are distinct, if not mutually exclusive perspectives about the way knowledge is advanced and deemed as being acceptable. These views have an important part to play in business and management research.

3.2.3 Research approaches

Positivism is commonly associated with experiments and quantitative research. Positivism is a belief that we should not go beyond the boundaries of what can be observed, it is research similar to those produced by physical scientists. Interpretive approaches on the other hand dismiss positivism as being overly deterministic and in the context of business and management, argue that the world of business is far too complex to be suitable for hypothesizing by definitive laws in a similar way to the physical sciences.

Realism means that certain claims can be made about the research that are true, independently of what anyone thinks. In the study of business and management this can indicate that there are large-scale social forces and processes that affect people without their necessarily being aware of the existence of such influences on their interpretations and behaviours. Business and management research is often a blend of positivism and interpretivism, and perhaps reflecting the stance of realism (Saunders, 2003).

According to Creswell (2018) a quantitative research methodology involves the process of collecting, analysing, interpreting and writing the results of a study. Saunders (2003) suggests that virtually all research will involve some numerical data or contain data that could usefully be quantified to help answer the research question(s) and to meet objectives. "Quantitative data refers to all such data and can be a product of all research strategies". It can range from simple counts such as the frequency of occurrences to more complex data such as test scores or prices" (Ibid). On the other hand, a qualitative research is understood to be a subjective process. The researcher brings their own histories, values, assumptions, perspectives, and mannerisms into the research. The subject we find interesting also reflects who we are, in other words, our subjectivity (Braun, 2013). Chenail (2016) stresses a cautionary note regarding

researcher bias in qualitative research especially if the researcher is embarking on a project in a field where they feel at “home”. He states that “Instrumentation rigor and bias management are major challenges for qualitative researchers employing interviewing as a data generation method in their studies”. He also states “the researcher must assess potential researcher biases especially if the investigator has a strong affinity for the participants being studied or is a member of the population itself” (Ibid). The researcher must take on a stance of neutrality and don the mantle of an independent researcher or at least acknowledge their bias. Braun (2013) echo this sentiment and make clear the active role of the researcher in qualitative research. She states that the researcher should not adopt a naïve view, where they merely “give voice” to their participants. Instead, they draw attention to the fact that it is the researcher who identifies the themes and patterns and selects and reports areas of interest to the reader.

3.2.4 Choosing a research approach

The second layer of Saunders (2003) onion (Figure 8) is concerned with choosing the appropriate research approach for the study. A deductive research approach is concerned with “developing a hypothesis (or hypotheses) based on existing theory, and then designing a research strategy to test the hypothesis” (Wilson, 2014). A deductive approach is concerned with deducting conclusions from a hypothesis, a logical approach where there is progress from general ideas to specific conclusions. Quantitative research often translates into the use of statistical analysis to make the connection between what is known and what can be learned by research. In quantitative studies, the researcher uses theory deductively and places it towards the beginning of the proposed study (Creswell, 2018). An inductive approach to research starts by gathering data that is relevant to the research topic. Once a substantial amount of data has been collected, the researcher will then stop data collection. At this point, the researcher looks for patterns developing in the data. The result of this analysis would be the formulation of a theory. When researchers take an inductive approach, they move from data to theory, or from specific to general. Qualitative research places great emphasis on the methods used to collect data. It places less emphasis on the analytical techniques to the interpretation of data. A combination of both deductive and inductive is often used for the same piece of research, as described by Ligurgo, Philippette, Fastrez,

Collard and Jacques (2018) paper “A Method combining Deductive and Inductive Principles to Define Work-Related Digital Media Literacy”. The authors present a qualitative research method that combines deductive and inductive approaches to analyse interviews and observations carried out in organisations. An inductive approach suited the small scale of the study into “the interoperability challenges in Intercloud, and how they may be overcome”, and its exploratory nature. Furthermore, an Inductive approach primarily uses a detailed reading of the data to derive concepts, themes, and models. Choosing an inductive approach through thematic analysis (a ‘data-driven’ approach) for this study determines that the objective of the study is to obtain an understanding of a research topic. It will not focus on testing a hypothesis.

3.3 Research strategies

This section examines the research strategies available to the researcher (the third layer of the onion in Figure 8).

3.3.1 Experiments

Experimentation is a research strategy with a defined hypothesis where samples are selected from a known population, different experimental conditions are allocated to each sample with planned changes made to one or more variables, while the other variables are measured or controlled (Saunders, 2003). Experimental research seeks to determine if a specific treatment influences an outcome. The researcher assesses this by providing a specific treatment to one group and withholding it from another and then determining how both groups scored on an outcome (Creswell, 2018). One of the main advantages of experimental research is that it offers the highest levels of control. The procedures involved with experimental research make it possible to isolate specific variables within virtually any topic. This advantage makes it possible to determine if outcomes are viable. The artificiality of the laboratory environment and its consequent inability to perfectly represent the real life situation is a distinct disadvantage. Kingstone, Smilek and Eastwood (2008) declared that “the research performed in labs, and the findings they generate, are in principle and in practice unlikely to be of relevance to the more complex situations that people experience in everyday life”.

3.3.2 Case study

Case studies are a design of inquiry in which the researcher develops an in-depth analysis of a case, often a program, event, activity, process, or one or more individuals (Creswell, 2018). The data collection methods used may be various. They may include questionnaires, interviews, observation and documentary analysis (Saunders, 2003). The case study technique gives the chance to study one aspect of a problem in some depth within a limited time-frame (Bell, 2014). Yin (2013) suggests, case studies can be used to explain, describe or explore events or phenomena in the everyday contexts in which they occur. Various criticisms have been highlighted for case studies such as, lack of generalisation potential, researcher bias and lack of rigor. Case studies are often judged to be unreliable because of a lack of rigor (Seuring, 2008).

3.3.3 Grounded theory

Grounded theory is a design of inquiry from mainly sociology in which the researcher gains a general, abstract theory of a process, action, or interaction grounded in the views of the participants (Creswell, 2018). Saunders (2003) describes Grounded Theory as 'theory building' through a combination of induction and deduction, theory being grounded by continual reference to the data. In grounded theory the questions may be directed toward generating a theory of some process, such as the exploration of a process as to how caregivers and patients interact in a hospital setting (Creswell, 2018). The production of a 'full' Grounded Theory (GT) is a demanding process, and only possible in larger research projects not constrained by time and resources (Braun, 2013).

3.3.4 Ethnography

The ethnographic approach is a design of inquiry coming from sociology in which the researcher examines the shared patterns of behaviours, language, and actions of an intact cultural group in a natural environment over a lengthy period of time; data collection often

entails observations and interviews (Creswell, 2018). Ethnography is ingrained in the inductive approach to research (Saunders, 2003). The central aim of ethnography is to provide rich, holistic insights into people's views and actions, as well as the nature (that is, sights, sounds) of the place they inhabit, through the collection of detailed observations and interviews (Reeves, Kuper and Hodges, 2008). As Brydon (1993) states, "The task of ethnographers is to document the culture, the perspectives and practices, of the people in these settings. The aim is to 'get inside' the way each group of people sees the world". Participant observation also gives ethnographers opportunities to gather first-hand insights into social behaviours that are normally hidden from the public eye. Additionally, ethnographic research can identify, explore, and link social occurrences which, at first glance, have little connection with each other (Reeves et al., 2008). Ethnographic research has its disadvantages. Due to the relatively long periods of time ethnographers spend talking to participants and observing activities, it can be difficult to secure prolonged access, especially if organisations are concerned that the research may show their organisation in a poor light (Ibid). Researcher participation jeopardises the validity of the research in that the subjects may react to the presence of an observer (Saunders, 2003).

3.3.5 Action Research

Action Research is a method of systematic enquiry that practitioners undertake as researchers of their own practice (McNiff, 2013). Parkin (2009) suggests the purpose of undertaking action research is to bring about change in specific contexts. Meyer (2000) explains that action research's strength lies in its focus on generating solutions to practical problems and its ability to empower practitioners, by getting them to engage with research and the subsequent development or implementation activities. Meyer suggests that practitioners can help to identify any problems, explore and implement solutions, and systematically monitor and refine the process and consequences of change. The main disadvantage of action research is that the practitioner evaluates himself or herself and this evaluation has a supposed lack of scientific rigor. Researchers are questioned over a perceived lack of impartiality and bias (Avison and Wood-Harper, 1991).

3.4 Appropriate Research strategies

Having examined each of the different research strategies the researcher decided on the strategies best suited to help answer the research questions (RQs):

- RQ1: What are the interoperability barriers in Intercloud?
- RQ2: How can these barriers be overcome?

3.4.1 Survey

The survey is a research approach involving the structured collection of data from a representative sample of a population (Saunders, 2003). Survey research provides quantitative or numeric description of trends, attitudes, or opinions of a population by studying a sample set of that population. It includes studies using questionnaires or structured interviews for data collection, with the intent of generalising from a sample to a population (Fowler, 2014). The purpose of the survey is to produce statistics and to identify patterns from data analysis allowing comparisons to be made. The main way of collecting information is by asking people questions; their answers represent the data to be analysed. The researcher decided this strategy was best suited to the open and exploratory nature of this study. Data collected by survey may not be as extensive as other methods considering the limited number of questions a survey may contain. As each respondent is presented with the same questions, it is an efficient method of collecting data from a large sample. A challenge in using surveys is in the construction of a valid survey that collects data as the researcher intended (Saunders, 2003). Fowler (2014) suggest that with respect to question design, the researcher must decide the extent to which previous literature regarding the reliability and validity of questions will be drawn upon.

3.5 Research Approach

3.5.1 Research Design

The researcher considered both qualitative and quantitative methods for the research design. Qualitative research is concerned with seeking to obtain richer, comprehensive research data from a smaller number of participants. This suited the small scale of this study, and its exploratory nature. Similar to the subjectivity of the researcher, it is to be noted that research participants also bring their own experiences, values and perspectives to the research. Braun (2013) states that it is “our humanness, our subjectivity” which can be used as a research tool. However, to do qualitative research well, the researcher must be “reflexive”. Reflexivity refers to the process of critically reflecting on the knowledge we produce, and our role in producing that knowledge (Ibid). While realising some data gathered would need to be “quantified” to help answer the research question e.g. re-occurring themes in the data, the researcher decided to use a predominantly qualitative approach.

3.5.2 Research Method

Research methods are the strategies, processes or techniques utilised in the collection of data or evidence for analysis in order to uncover new information or create better understanding of a topic. Creswell (2018) writes that research methods involve the forms of data collection, analysis, and interpretation that researchers propose for their studies. Selection and collection of primary as well as secondary data plays an important role in the research. From the survey research approach, questionnaires and face to face interviews were the main methods considered appropriate for collecting primary data. Interviews are ideally suited to “experience-type” research questions and have been found to be useful in getting a broader understanding of how and why certain things happen and what are the opinions, motivations, interests, feelings of the people involved (Braun, 2013). In qualitative approaches the researcher must aim to achieve a greater degree of closeness to the information provider than is normally the case in a questionnaire. As the research topic is quite specialised the researcher came to the conclusion that finding enough participants for a questionnaire would not be practical and also not provide the flexibility to ask for opinions, or possibility to probe deeper

into a specific question or point of interest. Interviews, though time consuming and resource intensive, emerged as the most suitable tool for qualitative exploratory research. An interview is a purposeful discussion between two or more people (Kahn, 1957). When working with a small sample the aim is to promote the sharing of ideas, described experiences, opinions, views, attitudes and perspectives that have a breadth and depth to them extending beyond that which a structured questionnaire would deliver. The data collection will come from a set of semi-structured interviews that will be conducted with various cloud software service providers and users who are providing and utilising cloud services. The researcher chose a semi-structured interview approach because it is a personal approach and can lead to an open flow of conversation throughout. The research questions were sent to the interviewee to give a tone of the areas of interest (Appendix A), however the sequence of questions on the day were free flowing and not tightly structured. The interviewee was given the freedom to explore the question as they see fit, and each interviewee encouraged to speak from their personal experience. In quantitative research the random sample is predominantly used, aiming at generalisability and applying the results to the wider population (Braun, 2013). In qualitative research the typical approach to sampling is purposive, with the aim of generating “insight and in-depth understanding” of the topic (Patton, 2002).

Purposeful sampling was used by the researcher to obtain participants who were especially knowledgeable about or experienced in Cloud Computing. The researcher specifically selected information-rich interviewees for the most effective use of limited resources (Ibid). The researcher acknowledges they are an advocate for cloud computing and work in the industry thus need to be aware of this and not look for results to reinforce the researcher's opinion or bias. Qualitative data being subjective is thus sometimes critiqued as being unreliable (Rust and Cooil, 1994) and, as stated previously, the researcher needs to acknowledge their own theoretical positions and values at the outset to avoid undeclared bias.

11 semi-structured expert interviews occurred across 2 companies. The first couple of interviews in the set comprised pilot interviews with people the researcher knew well but these were also included in the overall set for analysis. Piloting for interviews is crucial to test the questions and to gain some practice in interviewing (Majid, Othman, Mohamad, Lim and Yusof, 2017). The pilot interviews allowed the researcher to practice the interviewing techniques and make modifications and incorporate suggestions. The researcher chose semi-

structured interviews as they are an effective method for data collection to collect qualitative, open-ended data and also to explore participant thoughts, feelings and beliefs about the topic of Intercloud.

3.6 Limitations

Limitations for this research study include the relative small scale of the study, the limited sample of expert participants and the limited time frame. The researcher concluded that data saturation point was reached with Company A after nine interviews. A limitation of this study was also the small number of participants from Company B, indicating the data saturation was not reached. The researcher found it difficult to obtain more than two expert interviews from Company B.

3.7 Conclusion

This chapter outlined the research approaches and strategies considered for this study. The chapter then outlined the data collection methods and analysis approach chosen and why they were adopted for this study. In this research, the interoperability barriers in Intercloud and how they may be overcome were assessed by conducting qualitative interviews. The researcher conducted 11 interviews with participants from two companies. Some interviews were in person and some online. To analyse the findings in the interviews, the researcher took one Research Question at a time, and used the Toosi framework (Figure 6) to identify themes. The researcher then focussed on each theme or heading from the Toosi framework (Toosi et al., 2014) and discussed what was indicated in interviews about that theme. Having listened back to the interview recordings and transcribing the key points, the researcher had a sense of what themes in the Toosi framework showed up again almost a decade later. This method also showed what extra new themes emerged that weren't in the original framework in 2014 and helped to identify the more pressing issues a decade on.

4 Research Findings

4.1 Introduction

This chapter presents the findings from interviewing 11 cloud experts from 2 companies. The findings are presented using the lens of the 2 core Research Questions (RQs):

- RQ1: What are the interoperability barriers in Intercloud?
- RQ2: How can these barriers be overcome?

The findings are organised under these 2 research question headings. The researcher used the Toosi framework (Figure 6) as the lens to identify common themes in the research and identify new themes and sub-headings.

4.2 Participant Overview

Table 3 shows details of the list of interviewees. There is also information on the “Type” and “Duration” of the interviews. Interviewees were based in Ireland, UK, USA, and Australia. All 11 participants were male and over 40.

Participant	Role	Company	Why?	Type	Date	Duration
P1	Senior Platform Architect	Company A	Thought leader/Cloud expert	In person	Nov 2022	70 mins
P2	Director of Platform Engineering	Company A	Thought leader/Cloud expert	In person	Nov 2022	50 mins
P3	Manager IT	Company A	Thought leader/Cloud expert	MS Teams	Dec 2022	45 mins
P4	Software development lead	Company A	Cloud expert	MS Teams	Dec 2022	55 mins
P5	Senior Devops Engineer	Company B	Cloud expert	In person	Dec 2022	35 mins
P6	System Architect	Company A	Cloud expert	MS Teams	Dec 2022	30 mins

	Principal					
P7	System and network Engineer	Company A	Cloud expert	MS Teams	Dec 2022	35 mins
P8	Enterprise Business Solution Architect	Company A	Thought leader/Product expert	MS Teams	Dec 2022	40 mins
P9	Enterprise Business Solution Architect	Company A	Thought leader/Product expert	In person	Dec 2022	45 mins
P10	Senior System Engineer	Company A	Cloud expert	MS Teams	Dec 2022	40 mins
P11	Senior Devops Engineer	Company B	Cloud expert	Email	Jan 2023	

Table 3: Interview Overview

It was difficult to find participants with the required knowledge and understanding in Intercloud. The interview participants chosen were senior and highly technical experts in cloud computing having worked in the area for 10+ years. They had a vision of where cloud computing had come from and where it is going so were well qualified to give their thoughts and opinions. The interview with P1 was longer in duration than the others. This was due to the researcher knowing P1 well and choosing it as a pilot interview. P1 cleared his calendar to ensure there were no time constraints for the interview. The other participants were under time constraints due to work commitments.

4.3 Company A

Company A was chosen as a source for interview participants as they have been deploying their products to the Cloud for many years and provide a managed cloud service to their customers. They also have a strategy of being cloud agnostic and being able to deploy their products across multiple cloud providers. Company A is a large multinational corporation, founded in 1982, with more than 5,000 employees in over 20 countries. It provides business support systems (BSS) software and services, primarily to the telecommunications industry. Company A is a leader in innovative customer engagement, revenue management and payments solutions. They have a cloud-first architecture and help companies around the world

launch new digital services, expand into new markets, and create dynamic experiences that capture new customers and build brand loyalty. For over 40 years, Company A's technologies and people have helped some of the world's most recognisable brands solve their toughest business challenges and evolve to meet the demands of today's digital economy with future-ready Cloud and on-prem solutions that drive customer experiences. Company A deploys and provides Managed Services in multiple clouds. Company A is a trusted technology provider for leading global brands in telecommunications, retail, financial services, and healthcare. Company A deliver solutions to more than 900 customers in over 120 countries. Company A's cloud of choice is AWS but they also have expertise with Azure and are partnered with both cloud providers. Their products are mostly cloud agnostic.

4.4 Company B

Company B was chosen as a source for interview participants as they produce software for AWS cloud and are experts in AWS. Their software is developed entirely using AWS services. They provide a managed cloud (SaaS) service to their customers. They are a good example of a company that deals entirely with one cloud provider and does not have a requirement for using any other cloud. Company B is a medium sized multinational company with more than 1,500 employees, based in US and Ireland. They have customers in 180+ countries. Company B enables companies to expand internationally quickly and easily. Through their SaaS AWS Cloud based global platform, they help find, hire, onboard, pay, and manage team members, quickly and compliantly in 180+ countries, to expand growth opportunities for their customers – without the hassle of setting up local subsidiaries or branch offices.

4.5 What are the interoperability barriers in Intercloud? (RQ1)

Research question one focussed on the barriers that companies face when considering provisioning an Intercloud for their customers. The question was asked to the interviewees to find out if the main headings/themes described by Toosi (Toosi et al., 2014) were still relevant in 2023?

4.5.1 Themes identified – both old and new

As an open question, RQ1 facilitated the emergence of unprompted themes identified by each interviewee. The prevalence of such themes is presented below in Figure 9 and detailed further in Table 4.

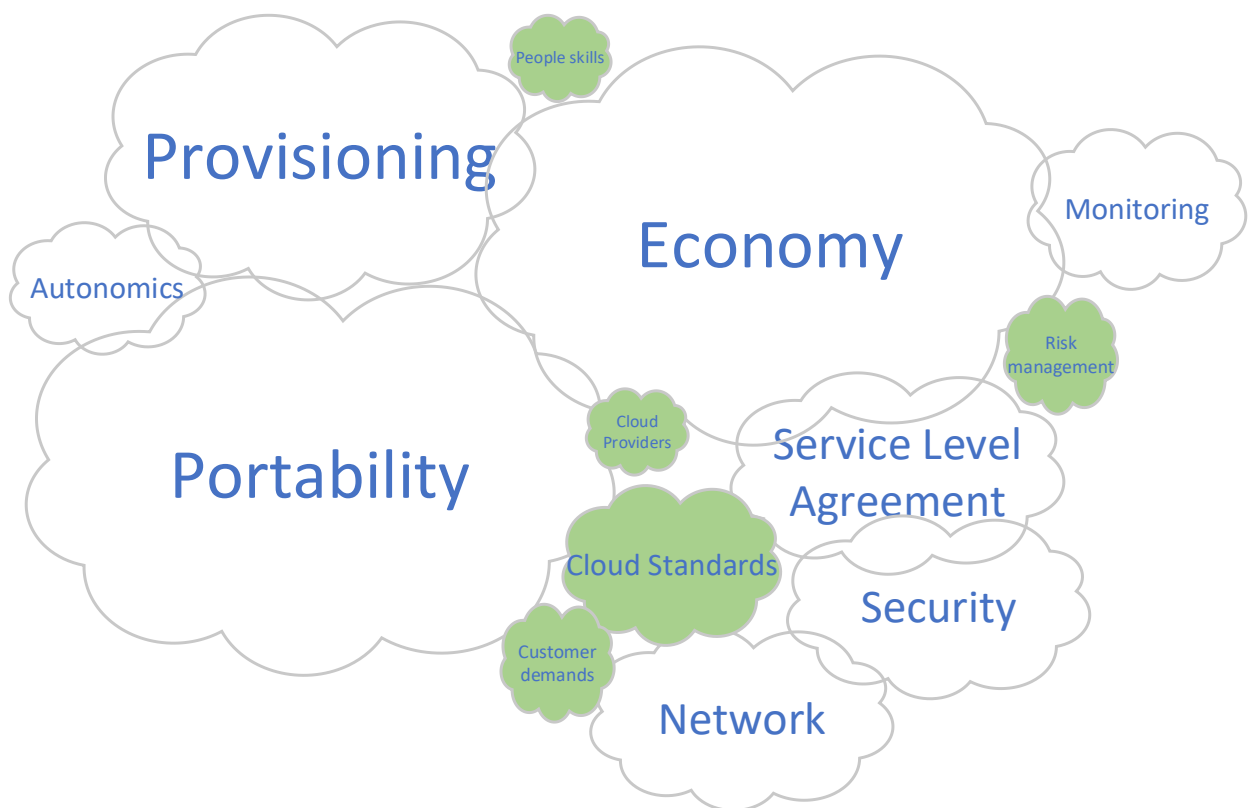


Figure 9: Interview Themes - Green depicts new themes since 2014 (Toosi et al., 2014)

Figure 9 above illustrates that concepts relevant in the original Toosi framework remain relevant a decade on, yet the study identified new thematic areas: findings for each are presented in the following sections.

4.5.2 Ocurring Themes

The researcher identified the themes in the interviews that were common to the headings in the Toosi framework and highlighted the emergence of any new themes. The prevalence of the themes in the interviews were also noted.

Theme	Existing/New	Occurrences	Comment
Portability	Existing	11	2 new sub-headings emerged – Terminology and Services
Economy	Existing	11	
Provisioning	Existing	7	
Service Level Agreements	Existing	6	
Network	Existing	6	
Security	Existing	6	2 new sub-headings emerged – Geopolitical and data sovreignty
Monitoring	Existing	5	
Cloud standards	New	4	
Autonomics	Existing	3	
Customer demands	New	2	
Risk Management	New	2	
Cloud Providers	New	1	
People Skills	New	1	

Table 4: Interview Themes occurrences

The table above shows what themes occurred in the interviews listed in order of decreasing occurrences.

4.6 How can these barriers be overcome? (RQ2)

Research question two focussed on the how the barriers (identified in RQ1) that companies face when considering provisioning an Intercloud for their customers can be overcome. The following sections explain each of the themes and then present the findings for RQ2. The themes are presented in order of decreasing occurrences (as per Table 4: Interview Themes occurrences).

4.6.1 Portability

Portability in cloud computing refers to the ability to transfer applications and data between cloud computing environments, enabling cloud service migration from one cloud provider to another. Portability in the cloud is needed for at least the following three reasons: protection of the end user investments in development; development of a Cloud eco-system and market; exploit the advantage of elasticity and pay-as-you concept (Petcu, 2014)

Data lock-in occurs when transitioning data to another cloud provider's platform is difficult and costly, making customers more dependent (locked-in) on a single cloud storage service. As a way of overcoming data lock-in P1 (Participant 1 interviewee) mentioned a 'Global filesystem' accessible from all clouds may be required for certain applications in an Intercloud. Another possible workaround is to copy required files to multiple places and also intelligent routing of files.

Containers are packages of software that contain all the necessary elements to run in any environment. P2 indicated that containers can give the "portability factor" particularly in use cases where spot instances could be used across cloud providers (move between cloud providers dictated by lower spot prices). He indicated that container orchestration based on spot prices could be configured between clouds spinning up in either one cloud or another as appropriate. P3 indicated that if a company is developing a new micro services based product in the morning they would do it with containers and "not touch" compute. P3 also indicated

that containers are key for a micro services application to run in a multi-cloud. However when a container needs to consume some cloud service external to the container e.g. in the billing world we may want to archive old Event Data Records (EDR), then containers are dependent on the current providers cloud storage services and in this case the containers in their deployment scheme would have to sense where they are being stood up and what native storage service to use. P3 indicated that a company could have their services in containers that could 'swarm' from continent to continent (follow the sun) so services are always close to users when and where they are being used at a particular time of the day, autoscaling as needed in the different regions e.g. Netflix have implemented this type of solution. P6 mentioned that having a container strategy for software applications is essential to having the possibility to run applications anywhere, including on a customer data centre. Leveraging kubernetes as the container orchestration tool that can "run anywhere". He also indicated that it may make sense for added resiliency to run container clusters over multi-cloud but would depend on cost. P7 concurred that the main benefit of Intercloud would be resiliency.

P3 indicated that with an Intercloud the application resiliency could be huge advantage in that e.g. containers could be spun up anywhere – but what about when the application is data dependent? Data has to be able to come with the application and data egress charges could be considerable. P9 also mentioned data egress charges will prevent data portability. P7 indicated that Rsync linux tool could be used to replicate VM between clouds but would be slow and subject to egress charges.

P2 also indicated that some Telco customers may not want to move some or all of their IT infrastructure to cloud as they have a need for their own Data Centre anyway to accommodate network switching infrastructure that can not be in the Cloud.

P10 indicated that restoring from backups are proprietary per cloud due to the way the backups are stored and restoring into a different cloud can be tricky, it can be done using 3rd party tools but they still have some pitfalls and are expensive. P10 concurred with this and indicated that AWS Elastic Block Store (EBS) snapshots can't be restored into another cloud. He did however think the cloud providers were not actively making it more difficult to restore these snapshots to other clouds – it was likely that AWS just developed these services in their own unique way that are not compatible with other Clouds. P4 concurred with this. P7 mentioned that Rubrik Polaris can manage backups of snapshots across clouds. P7 also mentioned AWS

snapshot backups are AWS unique and cannot be used to bring a backup of a VM up on another cloud. Same for Azure or any other Cloud provider.

P5 indicated that their company B's products are migrating to micro services. They use containers and some serverless (AWS lambda) and this could potentially be moved from AWS to Azure for example (with some work) but the main issue would be around High Availability (HA) and Disaster Recovery (DR) as things done differently around HA/DR in other clouds. P5 also mentioned that they only deploy to AWS however their code is stored in Github (not on AWS) and that the container building image process could be the same and used in any cloud but how its deployed to the different clouds would be different. P5 indicated that the redesigning to microservices is in AWS and although spending time and effort in redesigning they are not thinking about making it cloud agnostic but using native AWS services that will inevitably lock them in to AWS. He thought that maybe they should actually be making as many of the micro services as possible cloud agnostic and do a cost base analysis to see if made sense to make them all cloud agnostic.

P6 mentioned the need for skills in multi clouds as a barrier. Usually people are either skilled in one of AWS or Azure but not an expert in both or in multi-clouds. P6 also mentioned that there is no generic cloud certification and that it is an extra expense on companies to certify employees in multiple clouds in order to meet compliance regulations.

P2 indicated that their company is re-architecting their applications to be microservices and eventually they may be in a position of finding the most optimal way of paying for the cloud services using spot instances accross multiple cloud providers. E.g. an hour of compute is cheaper in AWS now but could be cheaper in Azure tomorrow. Controlling and orchestrating this would be a challenge but for Company A the application's design itself (at the moment) is the main limiting factor. P8 says we are still selling on-premise solutions so haven't made the full leap to cloud yet. Their Company is trying to accomodate both on-premise and cloud deployments. P8 thinks that software may be cloud agnostic so could run on different clouds but either one or the other not multiple at the same time. Customers will invest in getting their applications running optimally on one cloud and likely the cloud provider phycally closest to them. He sees no obvious business reason for an Intercloud solution.

On the 2 new sub-headings that emerged under Portability i.e **Terminology** and **Services** – P1 dislikes the AWS naming convention e.g. EC2, kinesis. He believes that the marketing jargon used is a barrier to having standard names across vendors for cloud services. The knock-on effect of non-standard terminology is more training required to implement on different clouds. AWS terminology in particular is seen by P1 as an Intercloud portability issue. P2 mentioned that using propriety services such as AWS Redshift, lambda may save money initially when migrating to AWS cloud but may lead to “lock-in” to AWS long term as these services are less portable. P10 concurred with this and indicated that native services such as AWS lambda won’t port to another cloud, instead the code needs to be re-worked. This takes extra time, resources and training. P10’s belief is that it is easier to just pick one cloud provider and stick with it. P8 mentioned AWS services such as lambda and API GateWay operate in a particular way while the equivalent in Azure are called something different and operate differently so how can they interoperate seamlessly? Without a common framework knitting together different ways of doing things would be a challenge. P9 mentions service lock-in as a barrier to Intercloud. As they look relatively cheap to initially start using, a company will start off using certain cornerstone services from a cloud provider. Then they may add more services and become more and more locked in to that provider. Moving to another cloud then gets more and more difficult. APIs are service specific e.g. AWS s3 APIs. To work across multiple clouds a company may need to re-implement things multiple times. Developers themselves may be able to solve it but would be taking on a lot of extra work. A company can choose to not use the “lock in” type services but this may result in having to do more work at least initially. A particular Cloud Customer in Germany did not want to use any service that would lock them in to AWS. This directive came from the CFO. P9 mentioned there is a serverless framework called ‘serverless.com’, which allows companies to do API calls across multi clouds, this works with lambda and Azure functions and acts as a common API. Using more open source tools may help overcome “lock in”. TM forum is a starting point for having standard APIs. P9 indicated that a software company can’t have an infinite way of doing things in their applications so as to make it work in every cloud, in most cases they have to pick one way of doing it and hope it’s the correct and best way. P9 also indicated companies don’t have the luxury to spend time and resources catering for every cloud possibility.

4.6.2 Economy

Cloud economics is not just about costs in monetary terms, but also about the opportunity costs of the cloud and learning how to manage costs in a highly dynamic environment. There is a business need to constantly analyse what is the return on investment (ROI) of migrating to the cloud or switching current cloud providers. Cloud market, pricing, and accounting & billing are all aspects that need to be considered. The role of cloud brokerage services could greatly benefit buyers and would combine the most cost-effective bundles into one easier to use multi-cloud infrastructure harvesting the full potential of the combination (Georgios, Evangelia, Christos and Maria, 2021).

P6 mentions cost is the biggest challenge deploying Company A's products to public cloud. Products were traditionally built for a data centre, with a 3 tier architecture, (web/app/DB) they scale vertically not horizontally so may be cheaper to put it in an on-prem data centre rather than Cloud. Public clouds charge a premium for their service. We can end up buying large VMs from public cloud and we leave them on all the time which can make them very expensive. P6 conducted many evaluations and looked at moving Company A's data centres into public cloud and it always worked out cheaper to leave it in the on-prem data centre. P3 also indicated that cost above anything else will drive peoples opinions on whether to spend on Intercloud or not. P4 mentioned the possibility of a 'wholesale cloud' appearing as the cloud market matures, similar to "telco wholesale" offering possibly a subset of AWS or Azure services at a lower cost. This could increase the possibility of an Intercloud. P4 indicated that if a new player with 'deep pockets' came in to the market e.g. facebook (an Intercloud for their Metaverse development), or twitter maybe, they could revolutionise the cloud provider market and could increase possibilities of an Intercloud.

P1 mentioned the varying unpredictability of cost for peaks and troughs of using more than one cloud provider was a barrier to an Intercloud. This unpredictability may be overcome if an open source tool was developed to monitor cloud services pricing in real time (financial broker) across all cloud providers. Amazon, Microsoft, Google and Oracle are so large that almost no other company can go to them demanding a better pricing deal. P1 also indicated the main cloud providers also have other businesses interests that are nothing to do with the cloud, so they are not dependent on cloud as their only revenue generation. This puts them in a better

position to not be forced into being more interoperable with other clouds and in having to offer better deals to certain large customers.

P1 indicated that cloud customers are forced to go with the published prices. There is no one organisation or group publishing price comparisons in real-time. High performance compute VM instance types have become more expensive due to slow down in global chip production. P1 gave the example that if using many multiples of compute instances then a small variance in price can add up. P1 believes a "compute market place" trading compute across all providers could be a possibility but this would assume the applications can be ported to other clouds seamlessly. He thinks this portability would not be possible without automation and containers.

P2 indicated that managing expectations and assumptions of customers and sales teams around cost are a big challenge, there's an assumption that moving to cloud will automatically save a company money as no need for physical data centre. P1 indicated that there is also a misconception that cloud means built-in and enhanced resilience, scalability, availability, automatic backups which of course is not necessarily true. It takes time and effort to get these implemented. P2 has heard multiple times in customer sales calls where the assumption is "as it's in the cloud it's already backed up". Sales teams and customers are often surprised to hear that this is not the case and if they require that service there is an added cost.

P2 indicated that one factor to consider if having different parts of an application in multiple clouds is the data egress charges e.g. if sending a call out of AWS and into Azure there is a charge for data out calls and also for the response from Azure to AWS. P6 concurred with this and indicated that in a multi cloud data is replicated out to other clouds and there is a significant cost for that.

P2 indicated that any application that could work well on spot instances may be suitable to run in an Intercloud. Spot instances pricing is based on surplus capacity in the region at that time. All cloud providers provision surplus compute to meet demand but if any capacity is left over they use them for spot instances which can be taken back again if demand suddenly spikes. Spot instances can be up to 90% cheaper but there is no guarantee the instances will be available so are only suitable to non-time critical applications. If an application is designed to deal with spot instances and e.g. a company wants their processing to complete some time this

week, not some time this hour then the savings are considerable. Potentially then if for example Azure is cheaper than AWS then move the workload to AWS. However, moving any required dataset may be a cost to consider due to egress charges. P3 concurred with this and mentioned data egress charges as preventing using a storage service in a different cloud. P8 indicated that there is no business benefit to offering an Intercloud solution unless we re-architect to make use of most optimal pricing, mostly through spot pricing. A mechanism where a company can buy compute on a real-time basis, wherever it works out the cheapest at that time. Light workloads but lots of them, where no persistent data requirements. This could be implemented but what are the cost benefits of it? P4 mentioned Continuous Testing (CT) use cases might be a good fit for multi-cloud i.e cheaper price on another cloud so move the workload.

P2 indicated that in order to design an application that could fit an Intercloud companies would need to do a cost-benefit analysis to see if its worth doing. P2 indicated that a CEO of a company won't want to hear they are locked in to a particular cloud provider as its a risk to the business. When locked-in, a business can be left in a vulnerable position if a) there are price hikes or b) the cloud provider becomes defunct. P6 concurred with this and mentioned the term "hostile vendor" whereby a vendor could change their policies or pricing which makes it harder for a customer to continue doing business with them. P6 indicated that when we move into public cloud we should always try to have an exit strategy, if a company has a multi-cloud strategy then they can insulate themselves from price hikes and data centre outages from a particular cloud provider. P2 mentioned that a big issue with public cloud and SaaS in general is that a company "hands the keys over" and if theres an issue they have to wait for the Cloud Provider to fix it. Companies lose some of that control they had in their own data centre. P4 also mentioned that if Company A could move the workload to another Cloud provider when its cheaper this would be a big advantage and would avoid lock-in. He also indicated that the bigger Cloud provider players may then be forced to re-think their cost models.

P5 indicated that with an Intercloud a company could take the best applicable service for their application from each provider and at the best cost, However, he acknowledges due to interoperability challenges this would be complex to implement right now.

P5 also indicated that salary costs to pay highly skilled people in multiple clouds with possibly multi cloud certifications qualifications would be a significant additional cost. When migrating

to cloud its more cost effective to start using cloud services as they only pay when using them. For Company A an issue is that they want to keep selling their products to customer's on-prem as well as in the cloud. As there are nuances to be considered when running on-prem or in the cloud its difficult to be in both spaces with your products at the same time. P6 mentioned that to get to a point where we are running applications in an active-active or even active-passive mode in multi cloud is currently possible i.e. no technical reason why it couldn't happen, however it would be costly and would the cost be deemed to be worth it? P5 mentioned that when concluding sales contracts there is always pressure to meet all requirements and keep the prices as low as possible.

Unlike P4 and P10, P6 thinks that public clouds are actively blocking the possibility of an Intercloud and they will make offerings like the more you spend with them the cheaper it is. P9 indicated that an Intercloud could benefit consumers as the cloud providers would have to be more price competitive. P2 thought that if smaller cloud vendors banded together and were taking some market share then the larger providers may respond. P11 indicated that for interoperability between platforms, e.g., third party connectivity, where the platforms are on different providers, the biggest barrier is cost. The complexity is how much integration is necessary, from a connectivity perspective it can be done, however, to reduce latency and increase bandwidth will cost.

4.6.3 Provisioning

“The provisioning function determines the resource requirements (volume, type, etc.) based on the SLAs and the concrete resources that are required to replace services while maintaining the guaranteed servicelevel. It must be able to identify bottlenecks when the traffic loads from or to the network vary and to dynamically perform corresponding compensation planning, since the operational characteristics of an application differ from case to case. It must further be able to perform a planning differentiated according to given priorities.” (Aoyama and Sakai, 2011)

P4 indicated that a big issue for using multi-cloud in Company A is the propriety interface per cloud provider, not only public cloud interfaces (AWS, Azure, GCP) but also private cloud e.g. vsphere – where there is a need to know the interfaces for each one and the Command Line Interface (CLI) also. There is no universal interface available for provisioning public and private

cloud. Terraform is an attempt to resolve this via 'infrastructure as code' but this needs plugins installed for it to work. P7 mentioned that Terraform should work in provisioning most clouds. P4 indicated that if a third party company or the open source community could come up with a common interface for multi cloud this could help. P9 also mentioned Terraform as possible solution to provisioning accross multiple clouds. P1 mentioned that although terraform scripts are a big step towards 'infrastructure as code' the same terraform script won't work in every cloud provider. One language that can be interpreted by all cloud providers would resolve this. An open source project could do this.

P1 said "each cloud does things that bit differently" so this can make provisioning in a multi-cloud more complex. P1 also indicated that Company A has some products that are dependent on certain Cloud specific services. One highly used AWS service is lambda. Some additional work and infrastructure changes would be required to make provisioning of these products work elsewhere to AWS.

P1 also indicated that we also need consistant terminology which we don't currently have e.g. EC2 in AWS, VM in Azure/Google. P10 concurred with P1 and indicated that one of the biggest challenges with an Intercloud is differences in terminology for example between AWS and Azure and this also impacts ease of provisioning. P10 thinks things just evolved this way independently. There was a race to get into the cloud so they developed it their own way and independently. This is counter to what P6 thought i.e. Cloud Providers are actively blocking the possibility of an Intercloud.

P10 mentioned in an Intercloud scenario it might be good to have the ability to choose the best and most cost effective service from each vendor for an overall solution. P8 also mentioned that a possible benefit to Intercloud would be having the capability to pick the best of the services from each cloud e.g. Azure may do the best AI service at best price or AWS may do the best storage service at the best price.

P11 said "I've found little need for Intercloud communications, certainly in terms of professional cloud hosted software as a service offerings". P11 asked "why would we want applications to be cloud agnostic?". He indicated that the big three (AWS, Azure, GCP) providers all have very different API's and some fundamental differences in their offerings, and there is little to be gained from being cloud agnostic, barring the case where a provider is

facing a cease-and-desist order. In any case, failure of their platforms would be commonplace, so why introduce the complexity? P11 argues that a company would have to abandon the native cloud interfaces and would introduce a complexity cost. Bearing in mind that complexity increases error rates, in development, test and release time, it is hard to argue the case for embracing multiple cloud providers, with anything other than “a crisp” application program interface acting as a boundary. Though if running on multiple cloud providers, simultaneously, was a requirement, P11 suggests Red hat OpenShift as a good starting point to overcome the barrier.

P1 mentioned the “Cloud native computing foundation” founded to help advance container technology as a way to improve provisioning standards. P1 gave the example of Linux as a prime example of something born out of the open source community that became standard. P4 mentioned that a load balancer based in a local on-prem cloud and spans out to all cloud providers could be used but this would need cost benefit analysis.

4.6.4 Service Level Agreement

“This function enables the selection of Cloud providers and Cloud systems that meet consumer quality standards stated in an SLA. The function matches the consumer’s and provider’s SLAs in order to guarantee quality requirements even in the events of service performance degradation or the occurrence of a disaster. In order to compare quality requirements, the SLA of a cloud system must be defined and published to other Cloud systems using standard formats. This makes it possible to select appropriate providers for interworking by means of comparing (exact match or within a tolerable range) the items of the SLAs. Further, it must be possible to search for resources – including applications and middleware – held by other Cloud systems and, in turn, it must be possible for a Cloud system to be detectable by other Cloud systems” (Aoyama and Sakai, 2011).

P1 indicated that the possibility of cooperation between 2 cloud providers may be possible in certain exceptional circumstances, but any agreement to cooperate between multiple cloud providers would be very difficult. The line from most providers would be “we can give customers Service Level Agreement (SLA) guarantees for the section of an Intercloud we are

responsible for but not for parts we have no control over. This prompted further discussion on the 5G rollout and self drive cars – P1 asked “what happens if connectivity or latencies to a certain provider becomes an issue in decision making of a self drive car?”. He indicated that to enable services like self-drive cars certain criteria need to be met and come with service guarantees. On further investigation the researcher found that decision making for self drive cars is made in the car itself and does not rely on an internet connection.

P2 indicated that there are agreements already in place between Azure and Oracle clouds whereby there is a fast connect for applications running in Azure to an Oracle Database running in Oracle cloud. However latency could still be an issue depending on how close the 2 data centres are. According to P2 the big 2 cloud providers, AWS and Azure, are unlikely to make any formal agreements. P3 indicated that if desired cloud providers could potentially throttle bandwidth to slow down data movement to another cloud provider and that guarantees around this would also need to be agreed. P3 also indicated that that database service offerings are different on each provider e.g. AWS Relational Database Service (RDS) would not be the same as in other providers and this could make agreements more difficult. P2 indicated that Openshift kubernetes and Vmware on AWS & Azure can be deployed directly on AWS & Azure clouds, however there would be a premium cost for this service - a company would end up paying both Vmware and AWS for example. P2 says “Intercloud only makes sense if it saves you money”. P2 indicated that “if applications are designed and built for Intercloud then its possible an Intercloud could be beneficial, however its not in the interest of cloud providers to make them completely cloud portable”. P2 also indicated that if a company is an “Internet of Things” (IOT) provider and theres an outage e.g. as what happened when an outage in AWS locked IOT house security customers out of their own house. Replicating the IOT house lock service customer data across to other clouds could have prevented this issue. There is an extra cost to the data replication but may be worth it as a brand could be destroyed by an outage.

P2 indicated that all clouds are at the mercy of broadband connection. P3 says its a bigger risk of an outage or service degradation by not going with one of the major cloud vendors than with a group of smaller combined cloud providers. P3 indicated that if the smaller cloud providers could step up to adopt a general open security standards as good as Azure and AWS then customers may start to look at them more. E.g. Blue Ocean offer cheaper compute but

security standards may not be as good. However big cloud providers want their customers to be “sticky” and to not have the ability to jump easily to another provider so unlikely to form an Intercloud alliance with any other provider. P5 can’t see any of the main cloud providers making an agreement with anyone to set up an Intercloud. Even if they did make an agreement with a smaller provider it would probably be with a view to take them over.

P6 mentioned he has never been asked about Intercloud in sales calls but would imagine if there was a major cloud provider outage then he would get a lot more questions about it. He indicated that a major failure could really spur on an Intercloud as a business case could then justify it. P6 mentioned in the US there was an App called Parlour that US conservatives built to be able to say what they wanted politically (without moderation) and one day after the insurrection on the US Capitol hill AWS decided to shut them down and it took them 3 months to find an alternative hosting provider they could move their App to. This crippled their business. If a particular cloud provider decides they don’t approve of the content being produced by a particular cloud user they can shut you down. This is an added risk with being over reliant on one cloud provider. P10 indicated that working out an SLA is not a barrier as such, it just needs to be resolved by legal teams and put into the contracts. When exploring the idea with P10 that “that a cloud integration must be enabled on a separated layer detached from both vendors and providers” he indicated that “but who is going to manage it?”. It has to be a consortium which comes together from representative of cloud vendors. Would they agree to participate? It would need to expose what they do under the covers to make it work and providers are unlikely to want to let their competitors have this information.

P8 thought the challenges of Intercloud are no different to the inter data-centre challenges we’ve had since a data centre was invented. Academically interesting to look at but in the business world its about business outcomes, SLA’s, kpi, contractual penalties. We’re not at a stage where we can offer a solution and guarantee it will work accross accross multiple cloud. Too much engineering required.

4.6.5 Security

“When different organizations are involved in providing services for customers, one major issue is that it is difficult to guarantee confidentiality and privacy on data, especially when data

is located in different countries with different laws. Cloud providers in interconnected cloud environments must provide mechanisms to guarantee the security and privacy of sensitive data within legal borders” (Toosi et al., 2014).

P1 indicated that all cloud providers will put an application’s security on the application vendor as opposed to the cloud provider. Security is slightly different in each provider so that puts an extra overhead on the application vendor and also makes portability more difficult.

P2 indicated that some customers e.g. banks, government agencies, will just never move to cloud as they don’t trust that its secure. P8 indicated that an issue in both cloud and on-prem is security policies around integration of customers with other 3rd party cloud solutions.

P2 also indicated that a challenge is to convince customers that Company A has the experience of implementing best practice security, we know what we are doing and have the correct principles that should be followed. He advocated the need to be forthright in our contracts with customers that integration security will be a challenge and take time and effort to get it right. P2 also indicated that even if using the same cloud provider there may be multiple accounts and on-prem to integrate with. Adding another cloud provider is another major security hurdle to overcome.

P2 said “Software providers don’t always do a great job of developing and testing for security from the start”. P10 indicated that at the authentication level going in to the various cloud providers console with single-sign-on is straight forward. P7 concurred when mentioning that SSO can be used to access AWS and Azure consoles. However, he mentioned at the VM level there isn’t a uniform way to synchronise authentication between cloud providers. P7 indicated that something like LDAP could be used as a standard to resolve this barrier. P10 indicated that there are 3rd party tools available to mitigate security issues but must be implemented by the cloud user themselves. The way AWS does IAM and roles is very different to the way Azure does it.

On the 2 new sub-headings that emerged under Security – **Geopolitical** and **data sovereignty**: P5 mentioned that AWS China operates separately from AWS International in order to comply with Chinese laws and regulations. Its similar for Azure in China. They both use different local operators to run them as independent entities. This type of government regulatory is a barrier to an Intercloud.

P1 indicated that there are laws in different regions on how to treat data in transit and at rest. P1 also indicated that other factors to consider for security are data sovereignty, GDPR, Geopolitical. Some customers in the middle east don't want to use cloud as there is no cloud provider in their country and they are not "friendly" with countries that do have cloud data centres in the region. Data breaches outside their "home" country can be very expensive and there is a tendency to keep data local. This can prove difficult in certain regions where there is only one region in a country and a need for an alternative Disaster Recovery (DR) site e.g. Australia. P8 mentioned "Incountry" data encryption service "data residency as a service" is used by Company A to mitigate data residency compliance challenges.

P1 concludes that "Politics and technology don't mix", and that a possible solution to geopolitical concerns and laws may be to beam data to space via satellite for transfer or storage. He also indicated that global agreements on policies where all countries sign up to may help. E.g. global security policies on retiring out of date security standards.

4.6.6 Network

"This function provides central network management tasks in order to provide the highest possible network quality for interworking Cloud systems. It manages networks by monitoring the flow of each service, and by autonomously changing service flows based on the load level of the network. Also, it should enable energy savings, e.g., through partial shutdowns of network equipment" (Aoyama and Sakai, 2011).

Network was mentioned in six interviews but three of these thought that networking connectivity challenges have mostly been overcome. P3 indicated that network setup is standard at this stage but that latency could be an issue if for example consuming cloud storage from a different cloud provider. P10 a network engineer indicated that he couldn't think of any technical barriers with connecting up multiple clouds.

P10 indicated that a company can bring their own company's IP range into the cloud and register them but you can't for example port an AWS IP to another cloud provider as each cloud has their own range and they are linked to a specific provider for routing and geo-location.

P1 indicated that latency is the biggest challenge to deploying Company A's products to the cloud. P2 concurred with this and indicated that latency is an issue for Company A's applications especially the ones that are database intensive and a significant challenge when using any cloud. P2 gave an example of a hybrid cloud application running where the application node is in AWS outpost and database node is in Oracle cloud. They are connected by a WAN link and the data centres are physically only 600 metres apart however latency is still an issue. There is still up to 2ms latency between them driven by number of leaps it needs to go through such as routers, security devices and firewalls, all contributing to the latency. If a database is running in same Availability Zone (data centre) as the application then it would be a sub 1ms latency. P2 also indicated that latency can be improved by writing more efficient code to reduce calls to the database, also by sorting table data and caching data locally. However every 'get' to the database is adding WAN latency. P2 indicated that another solution to the latency issue is to keep the application and database nodes together in the same data centre and could still interoperate with other parts of an application not so latency sensitive in other clouds. P2 contradicts this and indicated that he would not recommend running different parts of same application in multiple clouds. It is better to keep them together but could have different 3rd party parts of an enterprise solution in other clouds talking to each other, as long as they use well designed APIs to interoperate. He also indicated that latency is not so much an issue for well designed APIs. P3 indicated that an Intercloud could help latency by swarming up a container cluster in the region where that service is required at a particular time of the day. P6 mentioned for an Intercloud a large bandwidth direct connect pipe (other than internet) between the 2 or more clouds may be needed.

P5 indicated that having a common network interface and terminology across clouds would make them easier to connect together. P9 indicated that with a Domain Name System (DNS) we can route to different cloud provider end points with the possibility of directing customers to back up sites for fault tolerance. P9 also indicated that if an application is just using an API to hit an application DNS endpoint then does it really matter if the application is in AWS or Azure? He doubts that a customer would care where it is physically located. P2 and 10 both indicated that enterprise solutions with various applications interoperating across multiple cloud accounts and cloud providers is very much in use today in Company A's SaaS offerings.

4.6.7 Monitoring

“The task of this function is to collect and monitor the usage status and dead/alive status of each computing or network resource of a Cloud system, and to determine the need for load distribution or disaster recovery. To this end, it must be possible to – periodically or on a request basis – collect resource information (such as information about the performance and operation of each server, storage unit or network) for each service provided by a Cloud system. It must further be possible to exchange such resource monitoring information among other Cloud systems by means of commonly defined formats” (Aoyama and Sakai, 2011).

P4 and 10 both indicated that there are 3rd party monitoring tools with the “plugins” to link in to and monitor services in the different clouds providers. P7 concurs and indicated that Zabbix should work to monitor for example VMs in any cloud.

P9 mentioned that monitoring for scalability triggers would be different across cloud providers e.g. cloudwatch is used to monitor services and trigger events in AWS. Azure Monitor is used in Azure cloud. These may be used by respective cloud providers to trigger an event within the boundary of that cloud to e.g. add more VMs or containers to a cluster to cope with a spike in demand. He is not aware of a 3rd party tool that exists that could do this across multi cloud.

P9 questioned “how do we capture important logs from application VMs in an Intercloud and put them in a centralised place where they can be useful for analysis of the end to end picture?”. He also indicated that there would be data egress charges for moving this log data to a central location for processing.

4.6.8 Cloud Standards

“The use of standard or agnostic interfaces for cloud services would allow the developers to migrate cloud application among cloud platforms with minimum effort. This alignment need to be achieved at all cloud levels and across different models of clouds (including local/edge clouds)” (Martino, 2015)

Cloud standard guiding principles not being established for Cloud was mentioned as an interoperability challenge by interviewee P3, P4, P5 and P7. P3 mentioned that Company A's development teams develop cloud based solutions in different ways and consume different cloud services that may do the same thing. This lack of consistency leads to issues when it comes to standardising deployments. A set of standards and guidelines on how to consume cloud services within a cloud environment is required. Guidelines around security groups, security policies, storage, backup retention, service service preferences and cloud best practices helps to alleviate deployment issues and cost overruns. Company A has mature Cloud standards and guidelines defined for AWS but need similar for Azure. P3 indicated that standardising services to make them compatible accross clouds would be a big cost to providers. For many companies this would feel like "reinventing the wheel" and most would feel they wouldn't have any compelling reasons to do it. P3 indicated that an Intercloud would be great as systems would be more highly available and more immune to an Availability Zone (AZ) or regional cloud provider outage. Disaster Recovery (DR) would also be easier, if there was a major outage for a particular cloud provider they could switch all resources to another provider. However the automation on this would need some work to ensure it all works if required. P3 indicated that Kubernetes is a good example of an open source project that started small but the larger players had to adopt it as it became more successful. This may also happen in an Intercloud where the small players start it and if get enough traction the big players are forced to join in. Kubernetes is also an example of a framework that is suited to Intercloud. A set of services that can run anywhere. P4 indicated that software development projects in Company A don't encourage enough code reuse. Project budgets should cater to actively encourage development of code designed for re-use. If a project requires something to work in AWS the developer isn't given the flexibility due to budget/time constraints to look at a solution that may be generic accross all clouds. If we looked at things more holistically we may save more money for the company in the longer term. We are worried about our own area and not bigger picture. For example a company wide repository of reuseable code. Rather than many development teams doing similar things in different ways and languages have a standard company wide way of doing similar things. Company A has adopted TM Forum to develop API standards and this will help standardise API development accross projects TM Forum is a global industry association for service providers and their suppliers in the telecommunications industry (TMForum, 2023). Maybe cloud could do something similar where a Cloud provider

working group is responsible for setting the standards across all cloud providers. There are plenty of people writing open source tools to help with making things work between clouds but no overarching forum. P4 also indicated that the big cloud providers seem to have no issue working with private cloud e.g. Amazon ECS Anywhere and Amazon EKS Anywhere, software vendors can run containerised solutions for ECS (Elastic Container Service) and EKS (Elastic Kubernetes Service) outside of the AWS Cloud and run some or all of their offerings on customer on-prem hardware. However, due to proprietary nuances, running container clusters across multi public cloud providers is not so straightforward. P4 indicated that if smaller cloud providers got together to form an Intercloud and began to see some traction that either a large provider would come in and squash them or come in and direct them towards themselves. If the smaller providers started a cloud forum themselves then the bigger providers may join but would likely want to control it to their advantage.

P5 indicated that main issue when deploying to multi cloud is that Company B uses AWS cloud native tools and services and these are defined in their processes. Adopting to processes other than AWS would be an issue for them. P5 concurred that a global cloud body is required to define common cloud processes. P7 indicated that the biggest challenge he has come across in deploying to cloud is cooperation and management of a build out and is concerned that a multi-cloud build would increase the complexity leading to even more disconnect.

4.6.9 Autonomics

P3 indicated that the container orchestration services are all slightly different depending on the cloud vendor used. A container can run anywhere but the container orchestration software can't. According to P3 having a standard orchestration you can use across all clouds will never happen as Cloud providers are blocking this. Cloud vendors implementation of kubernetes is with their own proprietary tools. P4 indicated that containers would help the possibility of using an Intercloud as there is no need to build up software deployments to individual VMs first, Containers just work. However container orchestration of a cluster across more than one public cloud at the same time is not currently possible. P9 mentioned in the context of Company A and a particular product there is a challenge in how to apply the release process to containers.

4.6.10 Customer demands

P8 indicated that customers fundamentally just want a software provider to solve a business challenge they have in their Business Support System (BSS) or charging space. Pre-sales teams offer their solution for a particular business challenge, if it happens to be in one particular public cloud the customer probably won't care as long as we can solve the problem at the right price. If high availability and disaster recovery are required we can solve that also without going across multiple clouds. He has not come across a customer who has ever mandated a solution has to be to be across multiple clouds. A customer may have a preference for one cloud over another as they have more knowledge of how to integrate one over the other but if given a solution at the right price they will generally accept it. P2 on the other hand indicated that usually customers have a preference for one cloud provider and want to go with that one for whatever reason. P8 mentioned as he starts to think about things do we already use an Intercloud? An example given was - when applications making API calls to services such as 'Incountry' to encrypt data before it leaves a country (to meet that country's regulations) or calls to keydoc (ID and credit rating check) so systems can carry out its sales process. APIs enable open and secure integration between multiple clouds over the internet. Inter-application connectivity is possible across multiple clouds via APIs. For example a customer's business support solution (BSS) running connected applications across multiple clouds using an API Gateway as a single point of entry. P10 indicated that he thinks the only way companies would have their applications adapted to run in an Intercloud is if a big enough existing or new customer demands it (and pays for it).

4.6.11 Risk management

P8 indicated that Company A is at a high level of maturity as a business and would see it as a risk to do things quickly without careful consideration. Company A has many old and reliable customers that provide sustainable revenue streams so they need to continue to support these and balance this with introducing new technologies. A question that would be asked is "what's the benefit to Company A of pioneering leading edge technologies across multiple clouds?". If a large enough customer makes a demand for a particular application enhancement and if it's not implemented they will not renew a contract then it may make sense to agree to it. Many

companies innovate based on pressure of losing a contract or if a customer is willing to pay for the enhancement. P9 mentioned that if we change our software applications (some of which are over 25 years old) to become cloud native and as a consequence change the way the application works, there is a risk that the tools and scripts we developed over the years to help us, may become redundant.

4.6.12 Cloud Providers

Many cloud neutral projects and tools have been developed over the years by both open source and commercial organisations. “OpenStack is a platform architecture that provides a framework and APIs for cloud systems. It is an open-source solution that allows development of private or public clouds”. (Sotiriadis, Bessis and Petrakis, 2014). Red Hat OpenShift is a commercial cloud-based Kubernetes platform that helps build applications, with automated installation, upgrades, and life cycle management throughout the container stack. The Cloud Native Computing Foundation (CNCF) is an open-source software foundation that promotes the adoption of cloud-native computing. Kubernetes is the most widely used container orchestration platform, often described as the “Linux of the cloud” as the idea is it can “run anywhere”. Kubernetes is hosted by the Cloud Native Computing Foundation (CNCF). Terraform is an infrastructure as code tool that lets you build, change, and version cloud and on-prem resources. P11 indicated that OpenStack, Red Hat OpenShift, CNCF and terraform all offer cloud vendor neutrality but do so at the price of complexity as they are not easy to implement, and different clouds have nuances to overcome. P11 also indicated that every commercial vendor or cloud provider will have unique selling points to differentiate themselves, cloud providers will take an open source idea but will tailor it to their own cloud services e.g. Amazon Elastic Kubernetes Service (EKS) , potentially locking in customers, not making it easy to switch cloud providers or run their applications across multi-clouds. P11 thinks that cloud providers themselves are the biggest barriers to an Intercloud.

4.6.13 People skills

A recent survey by Forrester Consulting (commissioned by Hashicorp) (Forrester, 2022) indicated that skills shortages ranked as top Multi-Cloud Barrier. The survey found 76% of employers are already using multiple clouds in some fashion, with more than 50% flagging lack of skills among their employees (Forrester, 2022) as a top challenge for their cloud strategy.

Which of the following factors complicate your organization's ability to operationalize multi-cloud? (select all that apply)

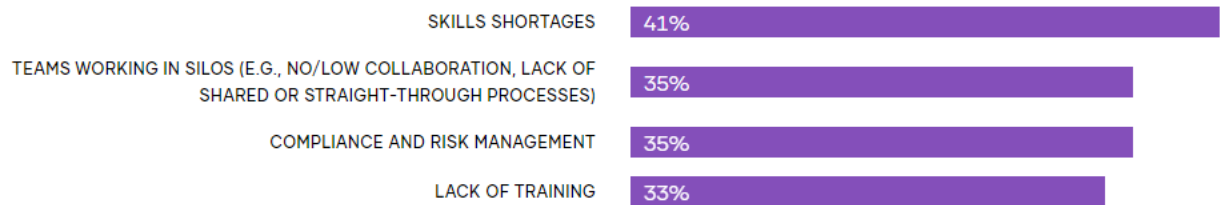


Figure 10: Top challenge for an organisation's cloud strategy (Forrester, 2022)

P10 indicated that knowledge of the different clouds and keeping up with all the new services and constant changes is a major challenge in the cloud. P10 said that “one of the biggest costs to an organisation is not the cloud hosting but the people who have to set it all up, manage and support it”. P10 also indicated that multi-cloud training and certification would help bridge the gap in skill shortages, but would need to be provided by a 3rd party training company as cloud providers only focus on their own services. P7 indicated that training and certification focussing on network interoperability of multi-cloud may help.

4.7 Conclusion

For RQ1 it was evident that interoperability barriers to providing Intercloud for customers still exist today. Barriers such as portability, costs, provisioning, SLAs, network, security, monitoring, and automation remain. Interoperability barriers around network, security,

monitoring, and automation have been significantly reduced in the last decade. The research shows new barriers have emerged though, such as cloud standards, customer demands, risk management and people skills. The research also showed evidence of new security concerns around data sovereignty and geopolitical risk. Figure 12 shows Figure 6 (which is from 2014) updated for today. Although barriers still exist, and new one have emerged, the research for RQ2 suggests possible ways forward to overcome. The research for RQ2 also shows candidate technical solutions to most of the interoperability challenges, however these are not fully embraced by the major cloud providers. This chapter presented the findings of the study, delineated using the two RQs, and providing an outline of both existing and new components to the Toosi model. Chapter 5 presents a discussion on these findings.

5 Discussion and Conclusions

5.1 Introduction

The study addressed the following research questions:

- RQ1: What are the interoperability barriers in Intercloud?
- RQ2: How can these barriers be overcome?

Because there were 2 RQs, the interview structure had two components. This chapter first presents a summary of findings per RQs. It then summarizes the findings per theme heading (Table 4: Interview Themes occurrences) for each of the RQs and compares them to the literature review. This chapter also defines research contributions, limitations and recommends topics for future research.

5.1.1 What are the Interoperability barriers in Intercloud (RQ1)?

The findings of the data analysis in chapter 4 reveal the factors that prevented applications being hosted in an Intercloud. This research provides an updated “taxonomy on Intercloud challenges” (Figure 6) framework as proposed by Toosi et al. (2014). This updated framework is shown in “Taxonomy of Intercloud challenges 2023” (Figure 12). The research showed that all of the main categories of barriers identified in 2014 still exist today. Its not clear whether the challenges in 2014 were listed in any particular order in the original study in Figure 6: Taxonomy of Intercloud challenges (Toosi, Calheiros et al. 2014). However, Figure 12 lists the barriers identified in this study identifying prominence by size of category box. While the sub-categories in Figure 6: Taxonomy of Intercloud challenges (Toosi, Calheiros et al. 2014)⁶ mostly remain today, some have increased notability and have added new sub-headings e.g. “portability” heading with the new sub-headings of “terminology” and “services”, also “security” heading with lesser emphasis on “trust” and “Auth & identity management”, however there is an emergence of 2 new security sub-headings of “geopolitical” and “data sovereignty”. Some headings are slightly less prominent due to technological advances e.g. “network” and “autonomics” and “monitoring”. “Portability” and “Provisioning” are still highly prominent today but have shifted from being technical to more lack of process and consistency

barriers. Despite the technological advances, the research shows that the amount of complexity in creating an Intercloud has actually increased in the last decade with the addition of five new barriers - cloud standards, customer demands, risk management, cloud providers and people skills.

As we have seen with Intercloud, over time the technical barriers are worked out, but non-technical barriers are much more difficult to be solved, and represent real resistance to the progress of Intercloud. The success of a an Intercloud depends on the effectiveness and financial efficiency of the problem it is trying to solve. As evident in Figure 12 with the larger Economy category box. Economics has a high importance and every decision on cloud deployment strategies are made with cost-benefit in mind. If the benefits greatly outweigh the costs, the decision should go ahead; otherwise, it should probably not. Cloud users do not currently have the motivation to move towards embracing an Intercloud. Costs to adapt their applications to be Intercloud compatible are too great. Many are locked-in to certain cloud services and can't be easily ported to other clouds. Cloud providers also continue to make their services proprietary again hindering portability. A lack of global organisation to oversee standards and processes across clouds means cloud providers continue to develop services in silos. Lack of standards also make it more difficult for cloud users to adapt their applications in a consistent manner for Intercloud.

5.1.2 How can these barriers be overcome? (RQ2)

The research suggests some approaches to overcome the interoperability barriers to hosting applications in an Intercloud. This research provides "Intercloud challenges and Solutions" (Figure 11) listed in order of highest prominence.

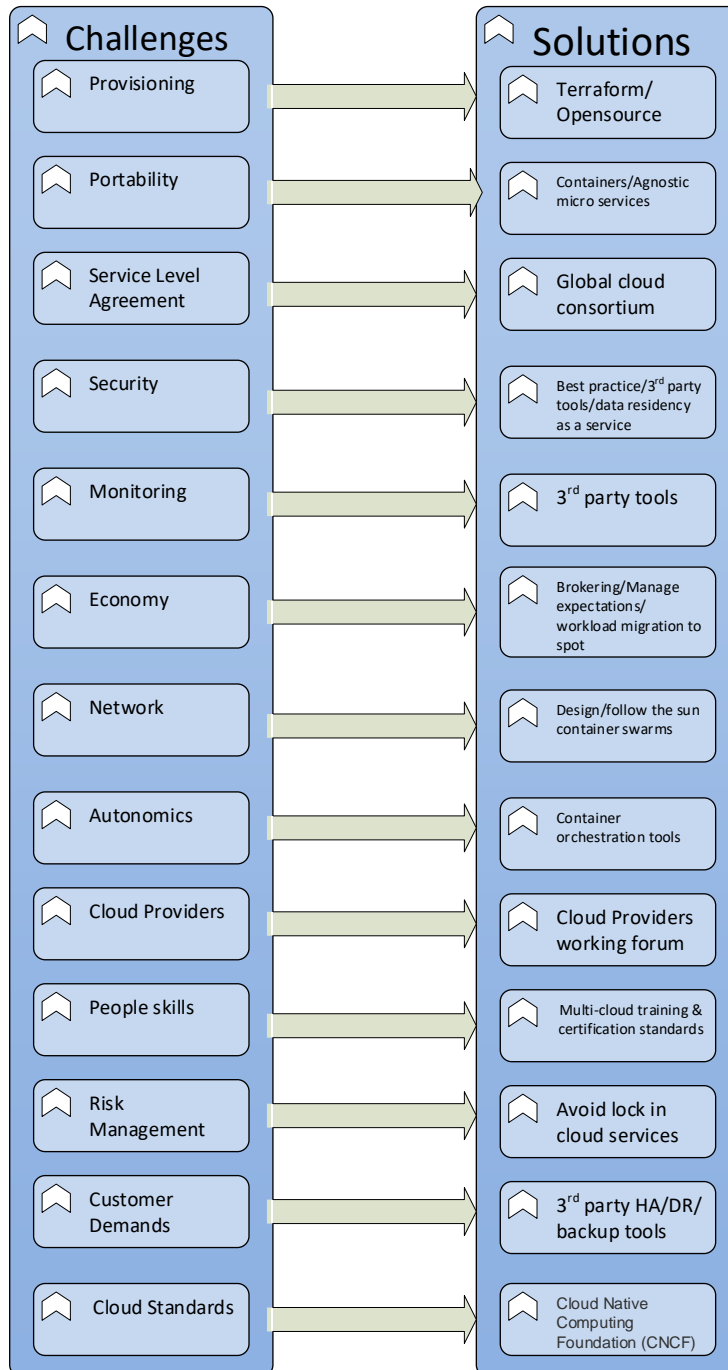


Figure 11: Intercloud Challenges and Solutions

The research and Figure 11 shows that there are ways to resolve most of the barriers to providing an Intercloud for specific use cases. The next sections discuss these in more detail under each of the headings and draws some conclusions. These barriers and how they may be

overcome (findings for RQ1 and RQ2) will be discussed in more detail in the following sections under their specific headings.

(A definition of each theme heading is provided in section 4.6).

5.2 Portability

The research found that the interoperability barriers around Portability of both application VMs and associated data across cloud vendors remains one of the main barriers to an Intercloud. For VM mobility - the main challenge is that VMs require storage and network services from their host cloud vendor, and once a VM is migrated from one cloud provider to another provider, it still requires access to the storage and network services of the source host. Cloud providers store data in their own proprietary format, e.g. AWS S3 and Azure blob which then means users cannot move their data to other cloud providers without considerable cost and technical effort. Defined cloud industry standards and common formats and tools are required to avoid data lock-in. Data portability is hindered by the lack of proper technology and standards and nonportability of the applications and data, “which is exploited by cloud service providers for their own benefits” (Petcu, Macariu, Panica and Crăciun, 2013). Using native cloud services in particular AWS lambda functions is a portability barrier. Two new Portability sub-headings were introduced – **Terminology** and **Services**. Cloud terminology (in particular AWS) is seen as an Intercloud portability issue. The findings from interviews revealed that participants are confused by cloud computing terminology. This finding is in concurrence with study findings by (Mohlameane and Ruxwana, 2014) whereby it was revealed that most cloud users lack understanding of cloud computing concepts due to the terminology. Proprietary services such as AWS Redshift, lambda may save money initially when migrating to AWS cloud but may lead to “lock in” to AWS long term as these services are less portable. This finding is in concurrence with study findings by (Martino, 2015) “In current cloud status, customers are often locked to a specific cloud vendor product or service, and easily transition to a competitor does not exist. Lack of interoperability and portability spans the complete Cloud stack, embracing data, applications, and infrastructure”. The research indicates that Cloud Providers have not made portability between clouds any easier in the last decade and in fact have made it a lot more difficult. “Individual proprietary technologies and access interfaces employed by cloud service providers made it difficult to share resources. Interoperability and portability are

two of the major challenges to be addressed to ensure seamless access and sharing of resources and services” (Chauhan et al., 2019). Portability remains the greatest interoperability barrier to an Intercloud.

The research shows that micro services and containers can help overcome these barriers in some use cases. In a microservices architecture, an application can be made independent of the host environment by encapsulating each of them in containers. Containers are packages of software that contain all the necessary elements to run in any environment. In this way, containers virtualise the operating system and can run anywhere, from a private data center to any of the public clouds. Containers are commonly used to host applications, and they're especially well-suited for these use cases:

- Microservices. Microservices-based applications are made up of many independent components, each deployed in a separate container.
- Continuous Integration/Continuous Development (CI/CD) pipelines.
- Repetitive jobs.
- DevOps.

5.3 Economy

The research found that the interoperability barriers around Economy are still significant today. Although some cloud services can do similar things e.g. for cloud monitoring - AWS has “Cloudwatch” and Azure has “Monitor” they are not interoperable with each other. “Cloud service providers have similar service offerings but different access patterns, making it difficult, time consuming and therefore costly for a cloud user to select an appropriate cloud service as per the application’s requirement” (Chauhan et al., 2019). Unpredictability of cost for peaks and troughs of using more than one cloud provider is an interoperability barrier to an Intercloud. Every cloud provider had their own pricing structure, sizing units, billing cycle, and bill formats. As a direct result, managing cloud bills and costs associated with different cloud providers can become difficult. Cloud broker has been put forward to address the challenge of cloud users to get the best out of cloud providers. The cost variances may be overcome if a Cloud broker monitored cloud services pricing in real time across all cloud providers. A cloud

broker is a body which works as an independent third party between cloud users and cloud providers. Cloud broker negotiates with several cloud providers as per user's requirements and tries to select the best services for the best price. "Cloud broker coordinates the sharing of resources and provides interoperability and portability with other cloud providers" (Ibid). Cloud developers need intelligent brokering support to acquire the resources that best satisfy the initial application requirements and prices and then adapt the brokering policies to the changing requirements of the runtime application (Ibid). A broker with a large number of customers on their books may be more likely to achieve a better pricing deal. However as we have seen in the research analysis their main cloud providers also have other businesses interests that are nothing to do with the cloud, so they are not dependent on cloud as their only revenue generation. This puts them in a better position and less inclined to be forced into being more interoperable with other cloud providers. A "compute market place" trading compute across all providers could be a possibility but this would assume the applications can be ported to other Clouds seamlessly and would require automation and containers. "Proposal of cloud computing is tightly coupled with low cost. Reduction of cost is considered as an important advantage of cloud" (Xinhui et al., 2009). Managing this expectations of customers and sales teams assumptions are a big challenge, there's an incorrect assumption that moving to cloud will automatically save a company money as no need for physical Data Centre. There is also a misconception that cloud means built-in and enhanced resiliance, scalability, availability, automatic backups which of course is not true. It still takes time, effort and money to get these things implemented in the cloud. Having different components of an application in multiple clouds means that data needs to flow in and out of different cloud providers infrastructure. One of the most concerns, when moving services into clouds, is capital expenditure and an ongoing cost is data transfer charges from cloud to client (Zhang, Li, Li, Xing, Yang and Dai, 2015). Data egress charges by cloud providers can be significant and In a multi cloud environment data is constantly replicated out to other clouds making it very expensive. The research suggests that a global agreement on limiting data charges across clouds would help with interoperability.

5.4 Provisioning

The research found that the interoperability barriers around provisioning of cloud services in an Intercloud has made some progress in the last decade but still remains a significant barrier. Emeakaroha, Brandic, Maurer and Dustdar (2013) presented a new approach to facilitate the management of service provisioning using multiple clouds. The approach is based on the integration of a universal cloud message bus system with monitoring techniques that provide Intercloud communication. Also, Senturk, Balakrishnan, Abu-Doleh, Kaya, Malluhi and Çatalyürek (2018) demonstrated a decision making system that facilitates the selection of the suitable cloud provider and configuration together with the capability to switch among multiple providers in an efficient and transparent manner. In their paper, they proposed BIOCLOUD as a single point of entry to a multi-cloud environment. However, there is still no commercial universal interface available for provisioning accross public clouds. Terraform by HashiCorp is an attempt to resolve this via “infrastructure as code”. Terraform is “written in Go, the language in which the cloud environments are created” It is an open-source DevOps tool first released in 2014 but has been enhanced over the last decade. It can be used to build, manage, and define infrastructure across cloud providers. The Terraform tool, also called the Infrastructure Build tool, enables DevOps teams to create and modify infrastructure using code. However, due to proprietary differences it is not possible to run the exact same code across cloud providers, but the basic language is the same. Proprietary services and lack of common terminology hinder the adoption of a single provisioning tool where the same provisionig code can be run accross multi-cloud platforms. Provisioning also covers “Elasticity”, which is automatically scaling up or down resources to meet user demands (which is one of the main benefits cloud gives). “Assuming that the provisioning of the heterogeneous cloud infrastructures is in place, it becomes a challenge to monitor and react upon unexpected degradation of service quality, by identifying the source of the problem, in the specific cloud provider. The coordination and infrastructure re-configuration (possibly involving the other cloud infrastructures) is key to ensure the restoration of SLAs and guarantee the proper behavior of applications and services” (Martino, 2015). Elasticity across multi-cloud is a challenge - how services across clouds are monitored and appropriate provisioning events triggered remains an issue. The research showed that there is a high degree of apathy for provisioning across multiple clouds. Cloud users just expect that there will be issues so why

bother with making things even more complex and more prone to errors by introducing more providers? For most use cases, it is hard to argue the case for embracing multiple cloud providers or trying to provision and run an application across multiple clouds. The research also showed that cloud experts don't expect the challenge of provisioning across multi-clouds to be resolved by cloud providers, the belief is that it will continue to be led by open-source projects.

5.5 Network

The research found that the interoperability barriers around Network connectivity (once designed properly) have for the most part been overcome and it was not seen as prominent a barrier as it was in 2014. These findings echo what was found in more recent literature (Köstler et al., 2021). In this work, the researchers presented a fast and secure network federation approach that enabled adaptable and multi-cloud operations. From their analysis of existing network protocols they were able to demonstrate a secure and performing network federation architecture able to support a wide range of use case scenarios, while preserving network functionality and cloud platform support. Their prototype implementation showed its viability, and the performance evaluation they undertook proved its efficiency. The researchers still see room for improvements in various areas, such as multi-cloud orchestration integration. With the pressures to make everything “connected” (Internet of Things – IoT) and accessible. Reducing the configuration complexity around network interfaces is not only in the interest of cloud users but also in the interest of cloud providers who require network connectivity in order for users to consume their services. Network interoperability “improves the competitiveness of small and mediums IT companies, datacenters and cloud providers, since it offers the possibility of increasing its computing and storage capacity, on an on-demand basis at a reduced cost, and also brings other important benefits, such as vendor lock-in avoidance, ease implementation of high-availability setups, enable service mobility and geographical proximity, and in general, an overall improvement on the Quality of Experience (QoE) for end-users” (Moreno-Vozmediano et al., 2017).

The research also indicated that having a common network interface and terminology across clouds would make them easier to connect together. “The private networks of the VPN protocols are provided at different network layers. OpenVPN and tinc support both the

creation of virtual tap or tun devices in order to act as virtual Ethernet switches or virtual routers. SoftEther provides the same functionality but follows its own terminology (virtual hub/L3 switch) “ (Köstler et al., 2021).

The research shows that latencies between end users and cloud data centres (Availability Zones) are still a concern today particularly in remote regions. This is where an Intercloud can benefit, as Toosi (2014) suggests “It is highly unlikely that a single cloud provider owns data centers in all geographic locations of the world to meet the low-latency access requirement of applications”. The research also shows that Container orchestration tools can also help with latency issues. They can add containers in swarms to Intercloud regions where they are most needed at certain times of the day.

5.6 Service Level Agreements

The research found that the interoperability barriers around Service Level Agreements still remain. “SLA-based cloud service/application management SLAs can be used as an instrument through which cloud services and respective applications can be managed during their life cycle. To this end, SLAs should be able to capture all appropriate information aspects relevant for this management” (Chauhan et al., 2019). However, Cloud services are dynamic and scalable, which means that they can change according to the demand and capacity of the resources. When cloud services are delivered through multiple cloud providers, cloud interoperability introduces complexities and variabilities that make SLAs more difficult to define, measure, and implement. There are third party products that make capturing this SLA information and making sense of it a bit easier, but the challenges outlined in (Toosi et al., 2014) around defining who would be responsible for what remains. Currently, there are still no formal SLAs in place between the major cloud providers in relation to interoperability and federated resources. “Cloud providers define (or negotiate with customers) a service-level agreement (SLA) to specify what they guarantee. In a simple definition, SLA is a contract that describes a service and, most importantly, sets the expected service-level objectives (QoS expectations). It can even encompass more details such as penalties applied to the provider if it does not deliver services according to the servicelevel objectives. Implementation of SLA mechanisms on top of federated resources is still an open question” (Toosi et al., 2014).

Another issue is that cloud providers describe their services with diverse languages, terms, and names. “Moreover, there is not a common understanding regarding service functionalities, their QoS, and metrics among providers and customers. In a heterogeneous environment such as Intercloud, it is difficult to enforce a standard syntax on service description or common metrics” (Ibid).

An international cloud computing foundation such as the Cloud Native Computing Foundation (CNCF) could potentially lead the way in defining what SLAs may look like when there is interoperability between cloud providers. Another candidate for developing a common set of standards across clouds would be the Open Grid Forum (OGF), “an international community dedicated to accelerating grid adoption by providing an open forum for grid innovation and developing open standards for grid software interoperability” (Ibid).

5.7 Security

The research found that the interoperability barriers around data security both at rest and in transit have remained. In the Intercloud scenario, the trust and reputation of a cloud provider affect other cloud providers. Bernstein et al. (2011) suggests that when a business entrusts its data to a cloud provider, it is more vulnerable to security breaches. In an Intercloud enabled federated cloud, the chances of a security breach is higher again due to the involvement of more than one cloud provider, as the data may be replicated and stored in more than one location. This emphasises the need for common data security standards to be implemented across clouds.

The research has indicated that new security concerns around geopolitical and data sovereignty have emerged. Geopolitical risk is the risk associated with wars, terrorist acts, cyber-attacks and tensions between states that affect the normal and peaceful course of international relations. The World Economic Forum's 2018 Global Risk Report warned that "the use of cyber-attacks to target critical infrastructure and strategic industrial sectors could trigger a breakdown in the systems that keep societies functioning". Cyber warfare does not have geographical boundaries in the way that physical conflict does, geopolitics and cybersecurity are now inextricably linked. Data sovereignty is the idea that data are subject to

the laws and governance structures of the country where they are collected. Data sovereignty defines whose rules and regulations data should be subject to. For example, The General Data Protection Regulation (GDPR) is a regulation on data protection and privacy for all individuals within the European Union. It came into operation across the European Union on 25 May 2018. The European Union specifies that data collected from its citizens is subject to the GDPR, regardless of where it is stored. “It was also important to consider legal aspects, i.e., especially requirements given by the general data protection regulation (GDPR), which basically require that all personal data reside in EU or countries which provide the same level of protection” (Lorünser, 2018). The concept of data sovereignty is closely linked with data security in cloud computing. In an Intercloud both data being transferred to different storage points, with possibility of multiple copies stored across multiple clouds in multiple regions not only increases the security risk that the data may be more vulnerable to cyber attack but also that the data may break data sovereignty laws. AWS and Azure China operates separately from their international companies to comply with Chinese laws and regulations using local operators to run them as independent entities. A proposed solution to geo-political concerns and laws may be to beam data to space via satellite for transfer or storage. Cloud Constellation Corporation's is a company aiming to provide a space-based network and cloud data storage service, named SpaceBelt. It has plans for a constellation of 8 satellites able to offer 5 petabytes of data storage and using laser connection links between satellites to transmit data between different locations on Earth. Global agreements on policies where all countries sign up to may help. E.g. global security policies on retiring out of date security standards. Convention 108 constitutes the first binding international instrument which is aimed at protecting the collection and processing of personal data, and which seeks to regulate, at the same time, the cross-border flow of personal data. “The ‘globalisation’ of Convention 108 (developing it into a global data privacy agreement, open to all countries providing the required level of data protection) is also now underway” (Greenleaf, 2013). With rapid changes in how data is gathered and processed, by for example artificial intelligence, the agreement needs to be continually evaluated and amended to stay relevant.

5.8 Monitoring

The research found that the interoperability barriers around Monitoring have been mostly resolved however some challenges still remain for an Intercloud, in line with prior research by Martino (2015) who posted “it becomes a challenge to monitor and react upon unexpected degradation of service quality, by identifying the source of the problem, in the specific cloud provider”.

The research findings suggest that a cloud monitoring solution that encompasses monitoring an application across different cloud environments without any integration problems is required. This can be difficult to achieve due to the differences between the different cloud providers. The Intercloud application and system logs may need to come to some central point for processing. Also parsing multi-cloud performance logs can be difficult due to the wide range of formats. The next generation of multi-cloud monitoring tools should have increased decision-making capabilities, for example based on a log entry an autoscaling event can be triggered with an API call to an appropriate cloud provider service.

5.9 Cloud Standards (new)

The research found that the interoperability barriers around lack of cloud standards is a new but significant barrier identified since 2014. “Formulating standards for cloud computing is the most obvious solution for achieving interoperability and portability in Interclouds” (Kaur et al., 2017). A lot of effort has gone in to developing cloud computing standards but these are not being following by the major cloud providers. The IEEE Working Groups P2301 and P2302 developed comprehensive standards to address migration, management, and interoperability among cloud-computing platforms but these were never adopted. “The EU reports that list of around 20 relevant and active organizations in cloud computing standardization area from which around 150 associated documents, standards and specifications are currently available. Unfortunately, it is still to happen that Cloud market leaders adopt any of them widely” (Chauhan et al., 2019).

The research shows that cloud customers are not demanding standardisation across cloud platforms so not much incentive for cloud providers to align. “The trigger to multi-cloud and

hybrid cloud can be the market force that pushes the adoption of standards by major vendors, breaking down current vendor lock-in situation. Moreover, to enable automatic establishment of chains of contractual relationships across multiple and heterogeneous cloud providers, it will be necessary to analyse and extend when necessary, existing formalisms to describe Cloud service offers to enable service comparability” (Martino, 2015).

The research shows that due to lack of adopting standards we are not at the point where cloud services are easily compared or if dip in quality of service are capable of easy substitution with a similar service from another provider. Some open-source organisations are leading the way in the push for standards to be adopted. The Cloud Native Computing Foundation (CNCF) is an open-source software foundation that promotes the adoption of cloud-native computing. The CNCF, a subsidiary of the Linux Foundation created in 2015, aims to establish a cloud-agnostic community to collaborate on open source projects. The CNCF defines cloud-native computing as the use of open source software, as well as technologies such as containers and microservices applications on cloud computing platforms. “Many organisations will be understandably wary of the lack of control over the information or the infrastructure, or of the possibility of vendor lock-in in the absence of standards” (Marston et al., 2011).

Another organisation involved in pushing for cloud standard adoption is the Open Grid Forum (OGF). Open-source cloud platforms (OCPs) are important for cloud interoperability not only because of the benefits of being open source but also because they are able to mitigate the risk of vendor lock-in by providing interoperable cloud environments. “As OCPs mostly support standard interfaces such as Open Grid Forum (OGF) and Open Cloud Computing Interface (OCCI) applications deployed on OCPs can be easily moved from one IaaS provider to another one implementing these APIs, without having to be modified. Considering the fact that OCPs facilitate cloud interoperability and portability, we study them among Intercloud solutions” (Toosi et al., 2014).

If cloud users begin to adopt cloud standards and they gather momentum in open-source projects, it may push cloud providers to make a move towards also adopting these standards. Cloud interoperability standards would allow applications and workloads to move from one cloud provider to another. Such application migration among clouds would allow companies to select the best priced cloud services and avoid vendor lock-in.

5.10 Autonomics

The research found that the interoperability barriers around autonomics have increased in complexity over the last decade. With the growing complexity of service offerings possible in an Intercloud, system management duties are far too complex and time consuming to be carried out manually. To overcome the issue, the need for automation is essential. Automation in computing refers to the selfmanaging principles while hiding the complexity of the tasks. “Using the holistic techniques provided by autonomic computing, we can handle to a large extent different system requirements such as performance, fault tolerance, reliability, security, QoS, and so forth without manual intervention” (Toosi et al., 2014).

Container orchestration is the automation of much of the operational effort required to run containerised workloads and services. This includes provisioning, deployment, scaling (up and down), networking and load balancing. Kubernetes is a widely used container orchestration tool. It is a portable, extensible, open-source platform that facilitates configuration and automation. The research shows that containers were mentioned as a possible interoperability solution for Intercloud in 10 out of 11 interviews. All the major public clouds offer hosted Kubernetes services via a SaaS architecture. Amazon has Elastic Kubernetes Service. Azure - Azure Kubernetes Service. Google - Google Kubernetes Engine. Because these services couple cloud-based infrastructure with software that helps to automate Kubernetes deployment and management, they are an attractive solution for organisations looking to get up and running quickly with Kubernetes. All these platforms are based on standard, open-source Kubernetes. They provide access to the same Kubernetes tooling and generally support the same types of storage and networking configurations. They look cloud-agnostic, however, public clouds that offer Kubernetes as a hosted service aren't flexible and generic as they may appear. They integrate and depend in various ways on other proprietary services running in the public clouds that host them. And in many cases, these are add-on that cloud providers Kubernetes services use by default. The research shows that there is a misconception that Kubernetes is the easy answer to running your applications anywhere. This needs more consideration before adopting this strategy.

5.11 Customer demands (new)

The research found that Customers are not demanding an Intercloud. Back in 2011 the belief was that an Intercloud “would be driven by consensus among large enterprise customers who insist on interoperability or by vendors recognising that standards development is needed to drive further adoption” (Ortiz, 2011). In the decade that followed this didn’t materialize and large enterprise customers that may have influenced the market were content to stick with one cloud provider to meet their infrastructure needs. Cloud providers didn’t need cloud interoperability to drive adoption, it happened anyway without the need for cloud providers to collaborate. One of the biggest selling points for an Intercloud is “availability” if there is an outage with one provider the application continues to run on another. The literature shows “cloud services are subject to outages or even data loss that could result from reasons as varied as hardware and/or software failure to acts of nature or terrorist attacks” (Marston et al., 2011). However individual cloud providers mitigate against this with the use of Availability Zones (AZ) and regions meaning that in the event of a data center outage there is no single point of failure. Cloud outages do happen and can bring down a cloud providers service in an entire region. With increased geopolitical tension and cyber attacks there is always a risk of a large, prolonged regional outage. If a large regional outage did happen it may make some of the large enterprise customers question do they actually need to have the ability to fail over to another cloud provider or risk revenue loss and damage to their brand image. In critical systems at the very least data should be replicated to another recoverable storage location. There are 3rd party disaster recovery (DR) tools that could be used in Intercloud. A DR tool should help you orchestrate the recovery scenario and, importantly, test it. If the tool is well integrated with your data backup tool, it can also allow you to use backups as a source of recovery data, even if the data is stored in different locations - like in an Intercloud.

5.12 Risk Management (new)

Risk management was not explicitly identified in prior studies in the literature, for example, Toosi et al. (2014), and Grozev and Buyya (2014). The research found that managing risk is a barrier to an Intercloud and was identified in two interviews. Intercloud introduces new risks

that normal risk management procedures may not easily identify, “Risk management processes can fail by ignoring the distributed nature of cloud computing and leaving numerous risks unidentified” (Mackita, Shin and Choe, 2019). Technology risk is a type of business risk which has the potential for any technological failure to disrupt a business. Companies face many types of technology risks, such as information security incidents, cyber-attacks, and service outages. Using cloud increases technology risk. “The inherent structure of cloud users of public cloud are at a higher risk of unlawful intrusion than users of non-cloud system”. (Haines, Horowitz, Guo, Andrijcic and Bogdanor, 2015). Using an Intercloud increases technology risk exponentially. Companies considering an Intercloud would likely do a cost/benefit/risk-based analysis, however if their customers are not demanding an Intercloud then it is unlikely, they will implement it due to increased technological risk. A lot of new technology is useful, but companies need to decide, is it really for them? Does it meet their needs? Implementing an Intercloud like any other new technology means it must be able to integrate into your existing processes to fully realise its potential. Otherwise, you may end up having to needlessly overhaul your whole system, which will take up more time and effort. Employees will also need to be trained on more than one cloud and this is a risk as it adds to training and retaining costs. If a company makes changes to their software applications to become cloud native or Intercloud compatible, they may consequently change the way the application works. There is a risk that tools used to support the application may become redundant. There is also the risk their customers may resist adopting the changes. One way to mitigate the risk of having the ability to implement an Intercloud is to avoid using proprietary cloud services that will lock customers into a particular cloud provider.

5.13 Cloud Providers (new)

The researcher found it difficult to decide if “Cloud Providers” section should be incorporated into “Portability”, for example is it cloud providers causing portability issues or would there be issues anyway? The research found that the cloud providers themselves are one of the biggest barriers to an Intercloud. Cloud customers are “often locked to a specific cloud vendor product or service, and easily transition to a competitor does not exist. Lack of interoperability and portability spans the complete Cloud stack, embracing data, applications and infrastructure” (Martino, 2015). The lack of established cloud standards and interoperability has made it

difficult to move workloads between cloud providers. Without any industry-wide cloud standards, cloud providers have built proprietary cloud services that are not compatible with other clouds - making interoperability more difficult. “The lack of formalization of cloud federations brings difficulties in understanding how they fit in the Interclouds set with specific properties and actuation niches” (Assis and Bittencourt, 2016). One way of avoiding interoperability issues is by working with cloud providers that support initiatives such as the Open Compute Project (OCP) which for the past decade has been trying to do for hardware what open=source has done for software – improve collaboration and produce better products for all users. The research shows that another important piece of the interoperability jigsaw is Kubernetes, an open-source initiative that is making some progress at ‘containerising’ applications so they can theoretically be moved between different cloud services. Unfortunately, there are still issues when it comes to different vendors using different versions of the platform, which creates interoperability issues. The Cloud Industry Forum also warns that using cloud services that rely heavily on bespoke or unique proprietary components may impact your portability to other providers. This is especially true if applications must be re-architected to run on another cloud provider platform. Technology is not a barrier to an Intercloud but the cloud vendors agreeing to standards is the main barrier to overcome.

5.14 People Skills (new)

The research found that finding and retaining skilled staff is an interoperability barrier to an Intercloud. Multiple clouds increase complexity, and technical skills from one platform are not necessarily transferable to another. “Each cloud provider exposes its own interfaces, configurations methods, and software and/or hardware requirements to instantiate and configure so the manual configuration of networked connections for different providers, requiring very experienced users with advanced administrative skills” (Moreno-Vozmediano et al., 2017). There are plenty of cloud certifications to choose from but no one multi-cloud certification, most of them are cloud platform specific. Because there is no industry-standard view of multi-cloud or Intercloud, there are few non-vendor organisations administering certification programs that are not aligned with a specific cloud provider. The Cloud Native Computing Foundation’s (CNCF) Kubernetes certification program comes closest to this model but is limited in that it focuses on one Intercloud approach – containers.

5.15 Further research

The researcher proposes further research confirming the specific findings of this research. In particular, substantiation of the new component headings found in the revised Toosi model (Figure 12). The research should be further developed to explore a broader list of cloud experts from more than two companies. This study interviewed cloud experts from companies using one cloud provider and multi-cloud, the researcher encourages similar research on a company using an Intercloud.

A review of the literature and the research showed cloud brokering in the context of an Intercloud as another potential topic for further research. The literature showed cloud brokering as a potential solution to the lack of interoperability. “Dynamic Configuration, Provisioning, and Orchestration of Cloud Resources, Further evolution of multi-cloud models linked to cloud interoperability developments, leads to a richer Cloud ecosystem in which Cloud Broker manages service negotiations and relationships among Cloud consumers and providers, acting as an intermediary”. (Chauhan et al., 2019). In an interview P9 mentioned machine learning could be used to learn the nuances between the cloud service providers. A broker could then potentially attempt to remove the interoperability abstraction layer by using machine learning and automation to provision and manage cloud interoperability e.g., Infrastructure as code that could be tailored using machine learning to work in each of the clouds.

5.16 Contributions

5.16.1 Methodological

Methodologically the researcher took a deep dive into a set of expert opinions, using a qualitative methodology brought about using semi-structured interviews. These cloud experts came from a variety of job roles within their respective companies. Company A used multi-cloud services and Company B just the one Cloud provider. A pre-determined set of open questions (questions that prompt discussion) was used with the opportunity for the interviewer to explore themes or responses further. During the data analysis, the researcher

took one Research Question at a time and used the Toosi framework (Figure 6) to identify if the themes identified then that still exist today. The researcher focussed on each theme or heading from the Toosi framework (Toosi et al., 2014) and discussed what was indicated in interviews about that theme. The research showed what themes in the Toosi framework showed up again almost a decade later. This method also showed what extra new themes emerged that weren't in the original framework in 2014 and helped to identify the more pressing issues a decade on.

The mechanics of the research gathering in the semi-structured interviews showed that saturation point was reached, as the analysis showed the reoccurrence of the same themes in the interviews. This was predicated by having interviewed experts in the area. This showed that if the research is focused on interviewing experts, then not a lot of interviews are required.

5.16.2 Theoretical

Toosi's research and the original framework identified the interoperability challenges at the time but didn't pin the relative size of each challenge or their relative importance. This research advances Toosi's framework by identifying the 2023 relevance of challenges that existed in 2014 and highlights the prominence of these challenges today.

The research also identified new barriers to Intercloud not identified or not in existence in the original Toosi framework. This study has also positioned new material on top of Toosi's work and discusses how these new findings relate to interoperability. The research provides an updated framework for the coming decade.

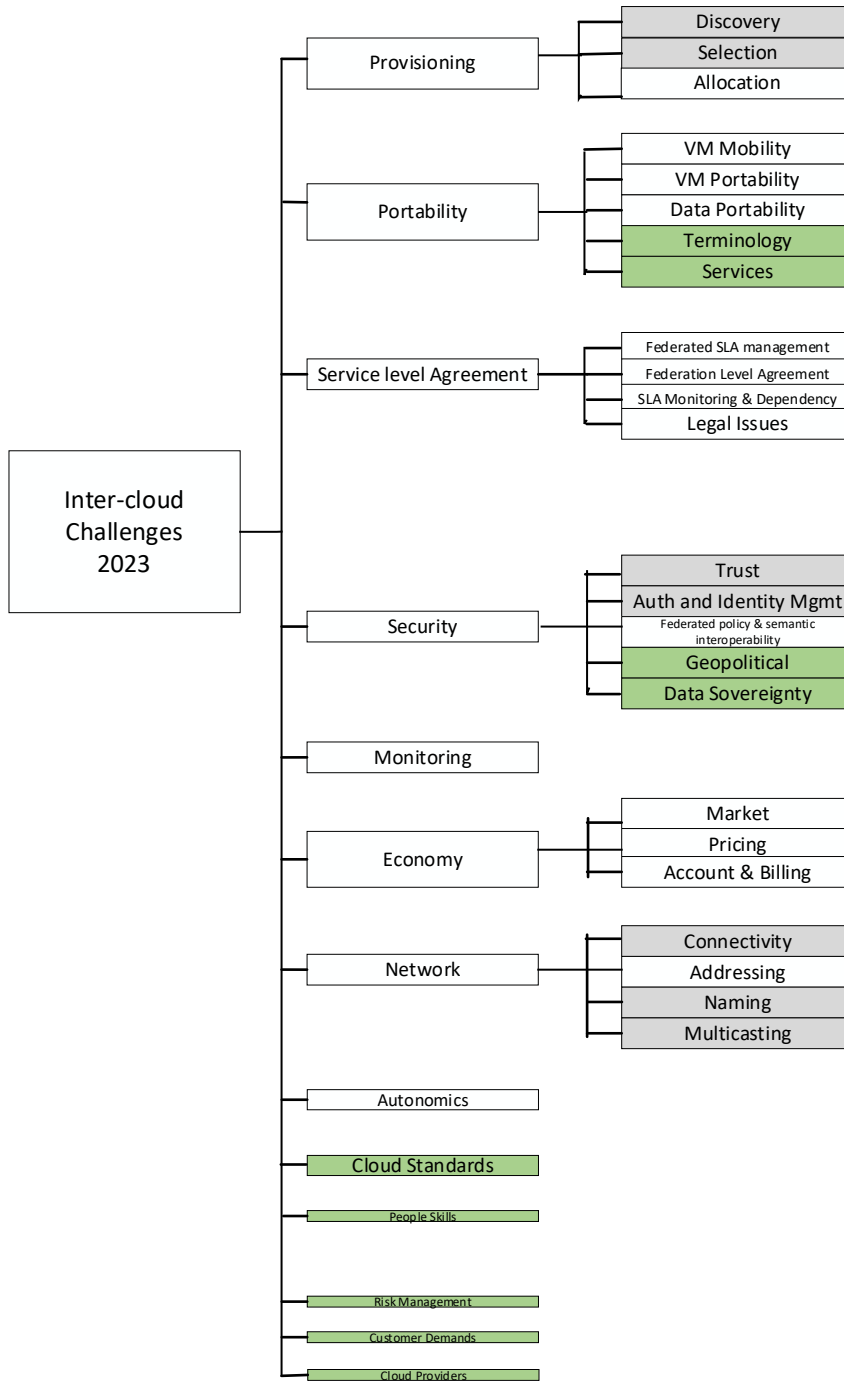


Figure 12: Taxonomy of Intercloud challenges 2023 – Grey depicts not mentioned in interviews - Green depicts new barriers based on this research since 2014 (Toosi, Calheiros et al. 2014)

5.16.3 Practical

An increase in the frequency of cloud provider outages and/or a major global outage of one major cloud service provider could accelerate very quickly the demand for Intercloud. The research shows that that cloud service providers would then need to do the following:

- a) Cease actively promoting proprietary service lock-in and make services more generic and portable.
- b) Standardise terminology, APIs, networking protocols, training, and certification across the cloud platforms.
- c) Sign up to a global agreement on cloud standards.
- d) A standard access interface across all clouds.

This research showed the difficulty in finding Cloud experts to talk about Intercloud. Another difficulty was getting access to these experts as they are very busy and are sought after. The research also showed that a relatively small set of semi-structured interviews across the right type of expert can shed sufficient light on issues and identify solutions.

There are many interoperability related barriers to Intercloud, but they are surmountable. The research suggested ways to surmount them (Figure 11). It may however take some time for cloud providers to be able to provide robust solutions in intercloud to their customers. In 5 years', time a revisit of the Toosi model may be warranted to re-evaluate interoperability and Intercloud.

5.17 Limitations

Limitations for this research study include the limited sample of participants for Company B. The researcher concluded that data saturation point was reached with Company A after nine interviews. A limitation of this study was just two participants from Company B, indicating the data saturation was not reached. The researcher only knew one participant personally in Company B and this made it more difficult to obtain interviews.

Another limitation was only having participants from two companies, one company using just one cloud and the other company using multi-cloud. Although more difficult to find, the study would have been enriched by having participants from a company actively using Intercloud. This would have given data to compare against data from companies not using Intercloud.

Use of only one framework (Toosi et al., 2014) to identify themes was also a limiting factor. Analysis of another framework could have been compared against the Toosi model for any missed barriers to Intercloud.

5.18 Conclusion

This study revealed that despite the technological advances in the last decade, the amount of complexity in creating an Intercloud has increased in the last decade with the existing barriers for the most part remaining, some increasing notability, and the addition of five new barriers - cloud standards, customer demands, risk management, cloud providers and people skills. Cloud providers over the last decade have become more siloed, continuing the path of making their cloud services offering more and more proprietary and bespoke. Interview participant 10 (P10) indicated that “technology is not a barrier to an Intercloud but the cloud vendors agreeing to it is the main barrier to overcome”. The groundwork of standardising cloud interoperability was put in place back in 2014 but it was never acted on by cloud providers and it never developed or progressed. Cloud adoption was happening at a huge scale anyway, so cloud providers didn’t need to think about interoperability – it was all about market share and locking-in customers. The study also revealed that the large cloud enterprise customers have never pressurised the major cloud providers to open to the idea of an Intercloud. It would probably take a major global and sustained outage of a major cloud provider to prompt customers to demand higher availability and disaster recovery options that cloud interoperability brings. There is a lot of talk in the industry about containers and Kubernetes being able to run anywhere, but it is important to understand that proprietary cloud versions of Kubernetes e.g., EKS, AKS, GKE take the complexity away and do not need in-depth knowledge about the platform’s infrastructure to get up and running quickly however they are mostly limited to running on their respective cloud platform. To run a Kubernetes in a multi-cloud or Intercloud would require an open-source Kubernetes, these are complex to configure,

deploy and manage and need to be understood implicitly by the people managing them. This study revealed what is evidently currently lacking is the willingness and joint up thinking required from the major cloud providers to make an Intercloud a working reality.

Appendix A: The Interview Guide

Email sent to interview candidates:

Dear <Name>,

I am currently carrying out research in fulfilment of a Research Master's degree at University of Galway, Ireland. The degree is supported by CSG. My study aims to identify and understand the challenges and barriers facing software service providers using Intercloud to host their software. I hope that the study can be of value to CSG.

The title is: "Overcoming interoperability barriers to Intercloud adoption."

The following two core research questions (RQs) emerged:

- RQ1: What are the interoperability barriers in Intercloud?
- RQ2: How can these barriers be overcome?

Considering your experience, I would like to interview you to gather your personal opinions and thoughts on these 2 questions.

You would be one of about 10 people I plan to interview at CSG and intend to interview others outside the company over the coming weeks.

I'm not expecting interviewees to have in-depth knowledge in the technical aspects of Intercloud, but looking for opinions and thoughts based on what you already know. I provide a brief outline of Intercloud below, as a working definition for the purposes of the study.

If you agree, the interview will take place in the next few weeks, at a time convenient to you, and take between 45 minutes to 1 hour. To assist me in recapping the discussion, it will be audio recorded. Microsoft Teams would be the preferred method of contact. The interview would be 1:1, and you and anything you contribute will remain anonymous.

I hope you will consider my request to be interviewed, however please do not feel under any obligation to participate. If you wish to obtain any more information about the study to inform you of your decision, please do not hesitate to contact me either by email or we can set up a quick call. I look forward to hearing from you soon.

Thanks,

Paul.

There are many definitions for Intercloud - the following is a working definition for the study.

Intercloud definition:

The term Intercloud has been described as a cloud of clouds, essentially, an Intercloud allows for the dynamic coordination and distribution of load among a set of cloud data centres. Intercloud means that integration must take place between at least two services, with each service on a different cloud infrastructure. Intercloud is important for use cases where you are seeking to integrate data and analytics workflow across different services/clouds. Intercloud computing has been formally defined as “a cloud model that, for the purpose of guaranteeing service quality, such as the performance and availability of each service, allows on-demand reassignment of resources and transfer of workload through a interworking of cloud systems of different cloud providers based on coordination of each consumers requirements for service quality with each providers SLA and use of standard interfaces” (Grozev and Buyya, 2014).

Supplemental Interview Questions:

- What would be the most common challenges your company would face in deploying your company’s solutions involving cloud services?
- Are any of your solutions currently deployed in a hybrid or multicloud model?
- What do you think are the main benefits of an Intercloud and could it help resolve any of the challenges identified in the previous question?
- Have you ever come across an example of Intercloud being trialed/used?
- Do you think an Intercloud could benefit your company in deploying and maintaining its solutions involving cloud services?

- Do you think its really feasible with current technology and mindsets to have a functioning and secure Intercloud or is it just pie in the sky - aspirational but unrealistic?
- If it is feasible then are the larger cloud providers actively blocking its development?
- Assuming that it is feasible (literature seems to support that it could be) it appears that interoperability is the main barrier (again the literature supports this – Toosi). What do you think are the technical and administrative interoperability barriers to Intercloud?
- How do you think these barriers can be overcome?
- There are a large group of professionals that believe clouds' integration must be enabled on a separated layer detached from both vendors and providers. Thoughts on this?
- Go through Toosi's headings/themes and ask for thoughts?

REFERENCES

- Ahmed, U., Raza, I. and Hussain, S. (2019) *Trust Evaluation in Cross-Cloud Federation: Survey and Requirement Analysis*, ACM computing surveys, 52 (1), pp. 1-37.
- Aoyama, T. and Sakai, H. (2011) *Inter-Cloud Computing*, Business & information systems engineering, 3 (3), pp. 173-177.
- Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010) *A view of cloud computing*, Communications of the ACM, 53 (4), pp. 50-58.
- Assis, M. R. M. and Bittencourt, L. F. (2016) *A survey on cloud federation architectures: Identifying functional and non-functional properties*, Journal of network and computer applications, 72 51-71.
- Avison, D. E. and Wood-Harper, A. T. (1991) *Information systems development research : an exploration of ideas in practice*, Computer journal, 34 (2), pp. 98-112.
- Azumah, K. K., Sørensen, L. T., Montella, R. and Kosta, S. (2021) *Process mining-constrained scheduling in the hybrid cloud*, Concurrency and computation, 33 (4), pp. n/a.
- Bell, J. (2014) *Doing Your Research Project A Guide For First-Time Researchers*.
- Bernstein, D., Vij, D. and Diamond, S. (2011) *An Intercloud Cloud Computing Economy - Technology, Governance, and Market Blueprints*, IEEE, 2011, pp. 293-299.
- Bohli, J. M., Gruschka, N., Jensen, M., Iacono, L. L. and Marnau, N. (2013) *Security and Privacy-Enhancing Multicloud Architectures*, IEEE transactions on dependable and secure computing, 10 (4), pp. 212-224.
- Braun, V. (2013) *Successful qualitative research : a practical guide for beginners*.
- Brydon, A. (1993) *What's Wrong with Ethnography?*, Martin Hammersley, New York: Routledge, 1992, 230 pp, Canadian journal of law and society, 8 (2), pp. 227-229.
- Buyya, R., Ranjan, R. and Calheiros, R. N. (2010) *InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services*, 13-31.

- Celesti, A., Galletta, A., Fazio, M. and Villari, M. (2019) *Towards Hybrid Multi-Cloud Storage Systems: Understanding How to Perform Data Transfer*, Big data research, 16 1-17.
- Chauhan, S. S., Pilli, E. S., Joshi, R. C., Singh, G. and Govil, M. C. (2019) *Brokering in interconnected cloud computing environments: A survey*, Journal of parallel and distributed computing, 133 193-209.
- Chenail, R. (2016) *Interviewing the Investigator: Strategies for Addressing Instrumentation and Researcher Bias Concerns in Qualitative Research*, Qualitative report.
- Creswell, J. W. (2018) *Research Design Qualitative, Quantitative, and Mixed Methods Approaches*.
- Elgedawy, I. (2015) *SULTAN: a composite data consistency approach for SaaS multi-cloud deployment*, UCC IEEE Press, 2015, pp. 122-131.
- Emeakaroha, V. C., Brandic, I., Maurer, M. and Dustdar, S. (2013) *Cloud resource provisioning and SLA enforcement via LoM2HiS framework: CLOUD RESOURCE PROVISIONING AND SLA ENFORCEMENT*, Concurrency and computation, 25 (10), pp. 1462-1481.
- Forrester (2022) *Unlocking Multicloud's Operational Potential*, Forrester Consulting.
- Fowler, F. J. (2014) *Survey research methods*.
- Gao, Y., Guan, H., Qi, Z., Song, T., Huan, F. and Liu, L. (2014) *Service level agreement based energy-efficient resource management in cloud data centers*, Computers & electrical engineering, 40 (5), pp. 1621-1633.
- Gartner (2022) <https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending>.
- Georgios, C., Evangelia, F., Christos, M. and Maria, N. (2021) *Exploring cost-efficient bundling in a multi-cloud environment*, Simulation modelling practice and theory, 111 102338.
- Golden, B. (2013) *Amazon web services for dummies*, John Wiley & Sons.
- Gomes, E. R., Vo, Q. B. and Kowalczyk, R. (2012) *Pure exchange markets for resource sharing in federated clouds*, Concurrency and computation, 24 (9), pp. 977-991.

- Greenleaf, G. (2013) *'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?*, *The computer law and security report*, 29 (4), pp. 430-436.
- Grozev, N. and Buyya, R. (2014) *Inter-Cloud architectures and application brokering: taxonomy and survey*, *Software, practice & experience*, 44 (3), pp. 369-390.
- Haimes, Y. Y., Horowitz, B. M., Guo, Z., Andrijcic, E. and Bogdanor, J. (2015) *Assessing Systemic Risk to Cloud-Computing Technology as Complex Interconnected Systems of Systems*, *Systems engineering*, 18 (3), pp. 284-299.
- Kahn, R. L. (1957) *The dynamics of interviewing : theory, technique, and cases*.
- Kaur, K., Sharma, D. R. and Kahlon, D. R. (2017) *Interoperability and Portability Approaches in Inter-Connected Clouds: A Review*, *ACM computing surveys*, 50 (4), pp. 1-40.
- Kingstone, A., Smilek, D. and Eastwood, J. D. (2008) *Cognitive Ethology: A new approach for studying human cognition*, *The British journal of psychology*, 99 (3), pp. 317.
- Kogias, D. G., Xevgenis, M. G. and Patrikakis, C. Z. (2016) *Cloud Federation and the Evolution of Cloud Computing*, *Computer (Long Beach, Calif.)*, 49 (11), pp. 96-99.
- Köstler, J., Gebauer, S. and Reiser, H. P. (2021) *Network Federation for Inter-cloud Operations*, Cham: Springer International Publishing, Cham, pp. 21-37.
- Kurze, T. K., Markus, Bermbachy, David; Lenkz, Alexander; Taiy, Stefan; Kunze, Marcel (2011) *Cloud federation. In Proceedings of the 2nd International Conference on Cloud Computing, GRIDs, and Virtualization. 32–38.*
- Lahmar, F. and Mezni, H. (2018) *Multicloud service composition: A survey of current approaches and issues*, *Journal of software : evolution and process*, 30 (10), pp. e1947-n/a.
- Ligurgo, V., Philippette, T., Fastrez, P., Collard, A.-S. and Jacques, J. (2018) *A Method Combining Deductive and Inductive Principles to Define Work-Related Digital Media Literacy Competences*, 245-254.
- Lorünser, T. (2018) *Secure and Robust Multi-Cloud Storage for the Public Sector*.
- Mackita, M., Shin, S.-Y. and Choe, T.-Y. (2019) *ERM OCTAVE: A Risk Management Framework for IT Systems Which Adopt Cloud Computing*, *Future internet*, 11 (9), pp. 195.

- Majid, M. A. A., Othman, M., Mohamad, S. F., Lim, S. A. H. and Yusof, A. (2017) *Piloting for Interviews in Qualitative Research: Operationalization and Lessons Learnt*, International journal of academic research in business and social sciences, 7 (4), pp.
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011) *Cloud computing — The business perspective*, Decision Support Systems, 51 (1), pp. 176-189.
- Martino, B. D. (2015) *Inter-cloud Challenges, Expectations and Issues Cluster Position Paper*, Google Scholar.
- McNiff, J. (2013) *Action Research: Principles and practice*.
- Meyer, J. (2000) *Qualitative research in health care: Using qualitative methods in health related action research*, BMJ. British medical journal (Clinical research ed.), 320 (7228), pp. 178-181.
- Mohlameane, M. and Ruxwana, N. (2014) *The Awareness of Cloud Computing: A Case Study of South African SMEs*, International journal of trade, economics and finance, 6-11.
- Moreno-Vozmediano, R., Montero, R. S., Huedo, E. and Llorente, I. M. (2017) *Implementation and Provisioning of Federated Networks in Hybrid Clouds*, Journal of grid computing, 15 (2), pp. 141-160.
- Ortiz, S. (2011) *The Problem with Cloud-Computing Standardization*, Computer (Long Beach, Calif.), 44 (7), pp. 13-16.
- Parkin, P. (2009) *Managing change in healthcare using action research*.
- Patton, M. Q. (2002) *Qualitative research and evaluation methods*.
- Petcu, D. (2013) *Multi-Cloud: Expectations and Current Approaches*.
- Petcu, D. (2014) *Consuming Resources and Services from Multiple Clouds: From Terminology to Cloudware Support*, Journal of grid computing, 12 (2), pp. 321-345.
- Petcu, D., Macariu, G., Panica, S. and Crăciun, C. (2013) *Portable Cloud applications—From theory to practice*, Future generation computer systems, 29 (6), pp. 1417-1430.

- Radhika, E. G. and Sudha Sadasivam, G. (2021) *Budget optimized dynamic virtual machine provisioning in hybrid cloud using fuzzy analytic hierarchy process*, Expert systems with applications, 183 115398.
- Reeves, S., Kuper, A. and Hodges, B. D. (2008) *Qualitative research methodologies: ethnography*, BMJ, 337 (7668), pp. 81-514.
- Rust, R. T. and Cooil, B. (1994) *Reliability Measures for Qualitative Data: Theory and Implications*, Journal of marketing research, 31 (1), pp. 1.
- Saunders, M. (2003) *Research methods for business students*.
- Senturk, I. F., Balakrishnan, P., Abu-Doleh, A., Kaya, K., Malluhi, Q. and Çatalyürek, Ü. V. (2018) *A resource provisioning framework for bioinformatics applications in multi-cloud environments*, Future generation computer systems, 78 379-391.
- Seuring, S. A. (2008) *Assessing the rigor of case study research in supply chain management*, Supply chain management, 13 (2), pp. 128-137.
- Sotiriadis, S., Bessis, N. and Petrakis, E. G. M. (2014) *An Inter-Cloud Architecture for Future Internet Infrastructures*, Cham: Springer International Publishing, Cham, pp. 206-216.
- The-Economist (2021) <https://www.economist.com/business/the-battle-of-the-computing-clouds-is-intensifying/21806813>.
- TMForum (2023) www.tmforum.org, pp. TM Forum is a global industry association for service providers and their suppliers in the telecommunications industry.
- Toosi, A. N., Calheiros, R. N. and Buyya, R. (2014) *Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey*, ACM computing surveys, 47 (1), pp. 1-47.
- Turner, M. J. (2021) *Ten Tips for Powering Resilient, Autonomous IT Operations with Policy, Programmability & Observability*, IDC directions 2021.
- Ünver, M. B. (2019) *What cloud interoperability connotes for EU policy making: Recurrence of old problems or new ones looming on the horizon?*, Telecommunications policy, 43 (2), pp. 154-170.
- Wilson, J. (2014) *Essentials of Business Research: A Guide to Doing Your Research Project*.

Wu, W., Wang, J., Lu, K., Qi, W., Shan, F. and Luo, J. (2020) *Providing Service Continuity in Clouds Under Power Outage*, IEEE transactions on services computing, 13 (5), pp. 930-943.

Xinhui, L., Ying, L., Tiancheng, L., Jie, Q. and Fengchun, W. (2009) *The Method and Tool of Cost Analysis for Cloud Computing*, ICLOUD, 93-100.

Xu, X. (2012) *From cloud computing to cloud manufacturing*, Robotics and computer-integrated manufacturing, 28 (1), pp. 75-86.

Yin, R. K. (2013) *Yin, R. K. (2009). Case study research: Design and methods (4th Ed.). Thousand Oaks, CA: Sage*, The Canadian Journal of Action Research, 14 (1), pp. 69-71.

Zhang, Q., Li, S., Li, Z., Xing, Y., Yang, Z. and Dai, Y. (2015) *CHARM: A Cost-Efficient Multi-Cloud Data Hosting Scheme with High Availability*, IEEE transactions on cloud computing, 3 (3), pp. 372-386.