UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering, Mathematics & Computer Science

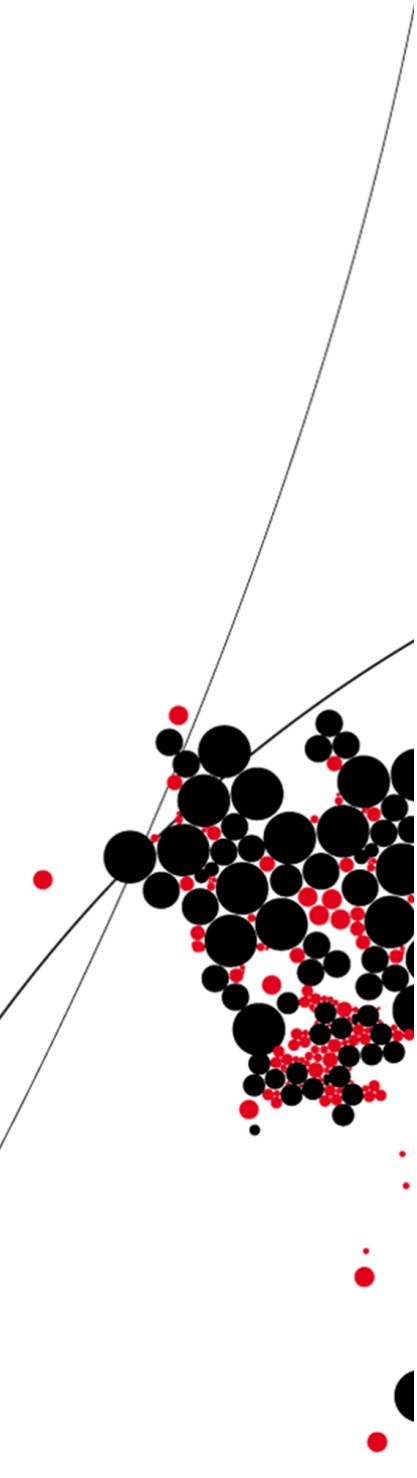
GOVERNANCE of CLOUD STORAGE

A secure cloud storage strategy to maximize data sovereignty

Toofan Shafee

M.Sc. Thesis Project

June 2022



Supervisors:
dr. ing. F.W. Hahn
dr. A. Abhishta

Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Engineering (Computer Engineering)

Preface

Dear reader,
Thank you for your interest and time in reading my master thesis. With this thesis, my master studies has come to a successful end. During the past years I have been developing my personal, academic and professional skills. But now, my 'student life' at the University of Twente, the years of hard working full of ups and downs ended with this thesis and a new challenge will be on the way.

This master study (Computer Science, Cyber Security Specialization) is broad which fortunately I could learn a lot about various areas of expertise and gained a broad spectrum of knowledge about risks and security in cyber domain - in particular about Cloud. The subject of this study stems from my personal interest which has motivated me enormously. I came to this topic indirectly through my work experience for several clients.

Although, a few months after the start of my master study at University the Covid-19 measures came into effect but thanks to the university with its rapid switch to online education and fortunately I have not suffered a study delay due to this Pandemic. In any case, I will remember this master as a period of great pleasure. I hope this study provides you with interesting insights and wish you pleasant reading.

Kind regards,
Toofan Shafee

Abstract

Cloud services - in particular cloud storage service - are providing millions of clients with the huge capacity and other business benefits that they require. Although it should not be ignored that this expansive growth can also bring some drawbacks. Among others, new security and privacy challenges such as the data sovereignty is very potential. Currently, in organisations, decision-making about choosing the right cloud service provider (CSP) and the management of cloud migration is a complex task. In order to aid organisations during the cloud migration process that enables them to make the right choice for data protection and assigning the appropriate security measure, this study introduces a cloud storage security strategy to minimize the data security risks - data sovereignty. Through a systematic literature review of more than 60 papers and interviews with 16 security consultants / specialists various potential factors has been considered and discussed. Based on these factors, a security strategy as a useful solution is developed that aids to fill the security gaps during the cloud adoption.

The main contribution of this study is a security strategy that can assess in improving the security of company's data during the data transmission - from decision-making about the cloud provider till the end of migration process. Furthermore, with combination of academic and practical sources provided in this study, a comprehensive view on the cloud storage security risks and migration process is presented. Including the important factors that should be taken into account in transmission process that provides effective security countermeasures and an improved security strategy for the organisation.

Keywords
Cloud Security, Data Sovereignty, Cloud Risks, Security Strategy, Cloud Storage

Acknowledgments

This thesis marks the end of my studies at the University of Twente. I would like to thank people who were important to the development of this thesis. First and foremost, I cannot express enough gratitude to my committee for their continued support and encouragemen, I would like to extend a huge thanks my supervisors from University of Twente, Prof. Florian Hahn, Prof.Abhishta Abhishta and Yasir Haq for their valuable comments and suggestions. I wholeheartedly appreciate their guidance and feedbacks. Of course also a big thanks to my program coordinator at University of Twente Pro. Andreas Peter, who often helped me during my whole master study. Furthermore, I would like to thank the interviewees for their time invested in my research and shared their knowledge and experiences with me to improve the result of this study.

And, last but not least, I would like to thank my family for their support these past years and in particular during the development of this thesis. Without the help and support from all these mentioned people surrounding me, this thesis would not have been possible.

Contents

List of Figures

List of acronyms

CC	Cloud Computing
IT	Information Technology
CSP	Cloud Service Provider
NSA	National Security Agency
IaaS	Infrastructur as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
StaaS	Storage as a Service
NIST	National Institute of Standard and Technology
CIA	Confidentiality, Integrity and Availability
SLA	Service Level Agreement
API	Application Program Interface
SR	Systematic Review
IS	Information Security
SSI	Semi-Structured Interview
DPA	Data Protection Authority
GDPR	General data Protection Regulation
BMIS	Business Model for Information Security
AWS	Amazon Web Service
QCA	Qualitative Content Analysis

2FA 2/Two factor Authentication

MFA Multi-factor Authentication

IAM Identity & Access Management

RQ Research Question

PQ Preliminary Question

Chapter 1

Introduction

With the rapid cloud adoption trend at many organisations across the globe, how the sovereignty of data can be maximized? It is actually a good question that required enough serious attention. In recent years, many organizations and enterprises across the globe have adopted and are using cloud computing as a novel IT solution in a large scale. It is inevitable that this trend is continuing to grow significantly, specially with the emergence of COVID-19 Pandemic. We see that since 2020 the usage of cloud solutions by customers increased in a higher degree, this is evident by a survey conducted by Flexera [6] and shows that in 2020 due to COVID-19, many countries across the world implemented stay-at-home policies for consumers, work-from-home policies for employees and using the cloud services even more than it was planed. The remarkable point is here that the way we handle information is rapidly changing and making data security more challenging than ever. Previously, during the last decades, user's data was primarily stored in the machines themselves or on external medias. Users / business owners felt confident that as long as they physically secured these devices, their data was also safe. But by the emergence of cloud computing, the data moves to the cloud and there are growing concerns about data security and privacy in cloud environment. For instance, the high-profile hacking attacks, reports of widespread government surveillance - primarily by US authorities - and big revelations such as Snowden's revelation in 2013 have confirmed the security and privacy gaps in the cloud infrastructures which motivated users and policymakers around the globe to rethink about their decisions.

As the focus of this study is cloud solutions, specifically the introducing of the cloud storage comes with a wide range of security threats, among all data sovereignty as a potential risk for data owner. Because by outsourcing the data, the data owners will almost lose full control of their data physically, then the security and sometimes safety concerns become a major challenge.

1.1 Motivation

The evolution of Cloud Computing (CC) solution has significantly impacted organisations driving their businesses by providing IT services over a network, shared resources such as software and storage to customers as a service on demand to achieve their goals. This has caused an increased dependency, such that most organizations, today, fundamentally depend on cloud services and both private and public sectors are accelerating adoption of this solution. If we notice well, when cloud and the business are aligned in an organization, clouds provide exactly what the business needs and in this way the business is able to deliver what the market needs. However, cloud computing offers tremendous opportunities in this digital age where the value is created from data, it comes also with a set of challenges and risks. Among all, information security and privacy is one of the top risks relevant to cloud computing which means that confidential information should not end up in the wrong hands.

1.1.1 Risk

Despite the advantages and importance given to cloud computing by practitioners, cloud computing comes with certain risks. For instance, when the hardware is owned by and located at the CSP, resources are shared with other customers and data is transported over the public internet, the control of data is a big challenge. That is not the only, if we look back, the history of the IT industry has also witnessed several high profile revelations that shows the surveillance and access of governments to citizen's data, the processing of user data by service providers without informed consent and big data leaks due to the lack of sufficient security measures. For instance, in the series of these revelations, the USA has been one of the governments with mass surveillance and access power to the public information that was in the headlines of the news several tims. At the same time, it is obvious that the big CSPs are Americans and their data centers are also located in USA territory. Recently, in particular after the Snowden's revelation, cloud storage for many organisations and the global technical infrastructure of the internet seem to challenge the sovereignty. Here the focus is driven by concerns about government access to sensitive public and private sector data. This means, sovereignty could not be simply ignored once it was clear that technology could be used for political gain. In addition, the last Facebook and LinkedIn big data leaks also added to the concerns of data owners and make them think about secure way for preserving their data privacy in remote environments. Hosting sensitive data on cloud infrastructure located in another country with different jurisdiction and without a clear understanding of the laws

governing both the enterprise contracted to host the data and the storage location of the data, poses a significant risk to organisations (including governmental organisations) and the adoption of public cloud environments. To make it more specific, for instance when dealing with sensitive personal, economic or strategic data, which may be subject to specific data privacy legislation in the country where the data originates from. The mentioned challenge highlights the importance of trust which a fundamental component that guarantees the sustainability of the relationship between a service or product provider and the consumer.

On the other hand, there is a lack of knowledge in organizations on how cloud computing impacts the confidentiality of data stored, processed and transmitted in cloud computing environments. In fact, lack of understanding information security at the strategic level when deciding to move to cloud create potential risk, such that they decide to move even sensitive data and important applications to the cloud, without the concerns about how they can protect it there abound. As a consequence, lack of sufficient cyber security knowledge when prioritizing the financial benefits over business data immunity is a serious problem that currently challenges many organizations. This means that most often, organisations are simply outsourcing their part/whole infrastructure through the purchase of cloud. In fact the problem with this approach is that too little effort is being made to understand the value, control and cost of the information security that an organisation should hold.

1.1.2 Current situation

According to my personal experience in this field (two years of experience as cyber security consultant), sometimes the perceptions of decision makers about cloud at companies have wondered me that however there are many risks associated with cloud adoption but the business owners and decision makers are not aware and trust more than needed in cloud security. We have seen that decisions regarding the selection of cloud service providers have been made on ad-hoc basis based on recommendations or on the reputation of the service provider. Obviously, it can be seen how it has become common for users to outsource their data to the cloud without being concerned about how the security of the storage is managed. In fact, the trend of moving to the cloud is inevitable and this way of resource consumption provides each organisation with greater agility, but the key issue to be addressed remains the security and privacy of information and trustworthiness of the CSPs. This issue — often also discussed under the term of digital/data sovereignty — should be taken seriously. One of the key solution to assist in addressing these challenges and realizing the value of cloud in organizations is a secure strategy in cloud governance which can establish an approach for the organizations to reduce risks, maintain busi-

ness alignment and maximize of value of cloud computing through a combination of people, process, and technology. The increasing immersion of digital technologies in supply chains, critical infrastructures and the lives of citizens raises cyber security to a matter of strategic importance, so as part of secure strategy the governments are also responsible to assist to develop sovereign digital infrastructure and regulatory frameworks governance mechanisms to control data in alignment with their political, national security and economic agendas. As evaluating pre-adoption choices at early stages is cost-effective to mitigate risks of probable losses due to wrong or unjustified selection decisions, therefor, through this study, I am going to develop a secure strategy to help organisation with management and preservation of data sovereignty in cloud storage in early stages.

1.2 Research question(s) and goals

The previous section discussed the current situation of cloud security and challenges. To protect the organisation's valuable asset - sensitive data - in cloud storage, organisations need to be capable of making the right decision about adopting cloud service. Knowing which security measures are needed to be taken to mitigate security risks from customer's side is also vital.
Before assigning the right measures, it is of significance to know the risks and its impacts. Therefore, the aim of this paper is investigating about the potential risks and challenges of the cloud storage, in particular data sovereignty and its impacts then defining a secure strategy for assisting business owner and decision makers in organizations during migration to clouds. Improving the decision-making capability of the organisations about the security factor in cyber domain is the first step of securing the organisation's critical data. With this aim, identifying the relevant data sovereignty problem and discuss them to have better planning and policy to overcome those issues is of the importance. The research impacts of this study are specifically twofold. First, helping organisations aiming to move to cloud with letting them to know about the security risks and downside. Second, giving the mentioned risks, helping to create a cloud security strategy that can also serve as an input for the Dutch national authorities (as this research is conducted on the scope of The Netherlands) to search for new security mechanisms to govern their citizen's information and sensitive data in cloud infrastructures. As currently , according to literature, there is no available cloud storage security strategy that organisations use in the process of migration. In order to achieve the research objectives, the necessary knowledge will have to be obtained and combined. This research is based on one main research question that encompasses on different preliminary questions which then those deal with separate but interrelated phenomena. The following main

research question will guide this research:

RQ: How can we design a secure cloud storage strategy to maximize the data sovereignty?
To answer the main research question, some preliminary questions (PQ) need to be answered. These preliminary questions provide scientific perspectives on the problem:

1. *PQ1: What is cloud technology?*
   First of all, the background information about the cloud computing should be provided. This preliminary question aims to explain the details of cloud computing.

2. *PQ2: What is data sovereignty?*
   This preliminary question states the data sovereignty and how it can impact the benefits of the cloud computing which are offered the users. It identifies those factors and risks which are critical during cloud adoption. In order to manage the risks efficiently, understanding the essential of the risk is of significance.

3. *PQ3: What are the different cloud storage strategies that are discussed in literature?*
   When migrating to cloud, strategies must be available to facilitate the migration process. This preliminary question compares and contrasts those cloud strategies.

4. *PQ4: Do they facilitate data sovereignty?*
   This preliminary question is builds upon the previous question. How efficient are or not the current available cloud strategies is the aim of this preliminary question.

5. *PQ5: What is the data and how data classifications influences the security controls needed to preserve the sovereignty of data in cloud?*
   The main goal of this preliminary question is describing the data and presents the influence of data classification on security of the data. Because after classifying and knowing the sensitivity of data, the appropriate control can be assigned.

1.3 Expected outcome

Cloud adoption can have huge impacts on the global security of an organization. The decision to migrate critical data or information systems to the cloud must consider

several factors besides only considering direct management and financial benefits. Currently, the biggest challenge for organizations during migrating and implementing successful cloud technology is managing the security part. Selecting, evaluating and implementing the suitable cloud storage while considering the security part, is a challenging task for many organisations. Therefore, knowing the relevant factors through a secure strategy is of vital importance to improve the security of the organisation's outsourced data, and would be a giant step in the right direction. The outcome of this study is a developed cloud storage security strategy for cloud migration which is based on the current security issues (data sovereignty). It will help decision makers and business owners while making decision to move to clouds, to which degree clouds are trustworthy for their sensitive data and ensure their sovereignty over stored data.

1.4 Research contribution

This study's original contributions are to:
1. Highlight the most critical challenges of cloud storage adoption in organisations and show that decisions on migrating data to the cloud should not simply be driven by cost considerations but should also take other significant factors such as the security into account.

2. Formulate a cloud storage security strategy, which provides a guide map that support the decision making during the adoption of cloud service in an organisation.

3: Address several knowledge gaps on the organisational changes seen during cloud adoption by a secure strategy.

4: Eventually, it particularly contributes to the areas of IT strategy, IT governance, enterprise architecture by stating a path for organisational development from a cloud security perspective.

1.5 Paper organization

This section describes the structure of the report.

The thesis report consists of six chapters, of which this introductory chapter was the first. The remainder of this report is organized as follows: Chapter 2 gives theoretical background information about Cloud Computing, Data Sovereignty and

Cloud Strategies. Then in Chapter 3, an overview of the research methodology by linking the research questions to research methods is presented. Chapter 4 presents the interview answers and also the output of the interviews. This is followed by Chapter 5 which combines the collected information from literature and experts interview. Then based on them formulate a security strategy for cloud storage which should help organisation during cloud migration. In Chapter 6, the results will be discussed and in the following the conclusions, limitations and recommendations are given.

Chapter 2

Background and Related Works

This chapter presents the scientific background of the research and the definitions used in this document. To get a better understanding about cloud computing, its service & deployment models, first, cloud computing and its features are introduced and detailed with findings on its benefits and challenges. Secondly, data sovereignty and its conception are presented. In the following, different available cloud strategies are explored and eventually data and impact of data classification is explained.

2.1 Related Works

Recently, cloud solution is seemed to become an efficient option for renting of storage infrastructure services for many companies. Of course this is with the perception that the security of stored data is totally relying on cloud provider with minimal management efforts. This means, mostly, business owners believe that they have to depend on cloud provider for the security of their own data which may or may not be 100 percent guaranteed. However, it should not be ignored that there are various privacy and security issues that can not be ensured, among all data sovereignty is the most remarkable. In order to evaluate the existence and also seriousness of the mentioned security challenges in cloud storage, we have reviewed several papers which are focused on this topic. In the following, we highlighted several view points that emphasise the importance of cloud storage security issue.
According to Marc en et al in [7], despite all the benefits that cloud solutions can bring for businesses, but there is still a serious drawback and that is the issue of data control. As soon as the business data gets transferred to the cloud, the outsourced data is exposed to several kind of the risks such loss, abuse and manipulation. This is due to lake of the users ability to know about their data location (in reality) and who accesses their data. To address this issue, they developed the FlexCloud project (pi - Cloud), aiming to provide the users with the ability to outsource their data and have

still some control on their data.

In [8], Neal et al also emphasise the importance of business data control and in general control of nation's sensitive data. They stated how countries around the world, specifically EU nations, are concerned about their stored sensitive information in the cloud. Although data localization can be considered as a secure option by many experts, but they explained their viewpoint opposite regarding this option. They believe that data localization can not be an efficient alternative as it leads to increasing the fragmentation of cyberspace and endangers the goal of promoting an open, secure, stable, accessible and peaceful ICT environment, which the international community endorses. They also proposed a 7-action mechanism for states to address the data sovereignty issue. Their proposed mechanism consist of the following actions: a) Formulate a Domestic Policy for Cloud Storage and Take a Position on 'Data Sovereignty', b) Enact Rules for the Distribution or Sharing of Sensitive Data, c) Clearly Classify Data, d) Enter into Bilateral Agreements with the US, UK and EU, e) Advise Departments of the Challenge, f) Mandate International Interaction and g) Cultivate Sovereign CSPs.

In 2020, Kushawa & Watson presented through their other paper [9] their findings about how Canada deals with the cloud security challenges, specifically data control. They stated that despite Canada highly believes in the efficiency of clouds but it emphasises that technical and economical benefits should not be caused that the complexities of international law and politics be neglected. Canada is also concerned about its data security and believes that its citizens data, stored outside the Canada exposed to various potential risks. Due to this concerns, The government designed national strategies regarding the cloud adoption for Canadian to address the data sovereignty issue. As a part of the strategies, Canada signed contracts with two large CSPs such as Microsoft and Amazon to commonly operate and offer their services in Canada under a Canadian corporation. Furthermore, both Microsoft Canada Inc. and Amazon Web Services Canada Inc. offer their Canadian customers the option to host their data in Canadian data centres.

Focusing this concern, Vurukonda and Rao in [10] also argued the way current business owners adopt cloud services. They believes when an organisation transfers data to the cloud environment, CSPs have full command on cloud applications, hardware and client's data. Then with full control over the data, they can perform any malicious tasks such as copy, destroying, modifying, etc. They believe there should be mechanism and policy or strategies that can protect the data when moving data to cloud from end-user side as well.

During our research and reviewing scientific papers, we found some more interesting papers which are relevant to our topic. These papers also discuss the security

ID	Authors	Date	Topic Type	Source Type
S1	Khan et al. [11]	2012	Data sovereignty	Conference Proceedings
S2	Kaaniche et al. [12]	2017	Data sovereignty	Journal
S3	Ullah et al. [13]	2013	Data sovereignty	Journal
S4	Trabelsi et al. [14]	2012	Data sovereignty	Conference Proceedings
S5	Kandah et al. [15]	2015	Data sovereignty	Conference Proceedings
S6	El-Ghazzar et al. [16]	2016	Cloud adoption strategy	Journal
S7	Anggraini et al. [17]	2019	Cloud adoption strategy	Conference Proceedings
S8	Al-Ruithe et al. [18]	2018	Cloud adoption stratey	Journal
S9	De Paula et al. [19]	2016	Cloud adoption strategy	Conference Proceedings
S10	Kyriakou et al. [20]	2019	Cloud adoption strategy	Journal
S11	Guo et al. [21]	2016	cloud adoption strategy	Conference Proceedings
S12	El-Gazzar er al. [22]	2015	Cloud adoption strategy	Conference Proceedings
S13	Utomo et al. [3]	2020	Cloud adoption strategy	Conference Proceedings
S14	Hussain et al. [23]	2017	Cloud security challenges	Journal
S15	Shukla et al. [24]	2016	Cloud security challenges	Conference Proceedings
S16	Efozia et al. [25]	2017	Cloud security challenges	Conference Proceedings
S16	Murali et al. [26]	2016	Cloud security challenges	Conference Proceedings
S17	Grover et al. [27]	2014	Cloud security challenges	Conference Proceedings

Table 2.1: Some more studies included in the literature review

issue of the cloud storage and provide various solutions including development of general cloud strategies/ frameworks to address them. The Table 3.1 provides the details of these papers.

2.2 Background

2.2.1 Cloud Computing

In order to explain the cloud computing, we would like to refer to the formal definition by the National Institute of Standards and Technology (NIST) [28] which is often referenced in studies and it is used in this research as well:

DEF1: *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* That means, cloud computing is a method of computing where computing resources are easy to obtain and access, simple to use, cheap and just work. Eventually, cloud computing is a general term for anything that involves delivering hosted services over the Internet. It delivers divers IT capabilities as services-on-demand. To understand the importance of cloud computing and its adoption, we must understand its principal characteristics or features, its delivery and deployment models. According to the NIST definition, the key characteristics of cloud computing include the following: [28] [29] [30]:

- **On-demand self-service:** The customer / end user can unilaterally provision computing capabilities, such as server settings and network storage when needed, without any interaction from the provider's IT administrator.

- **Universal network access:** All the capabilities are available over the network and accessed through internet and client platforms, such as mobile phones, laptops, netbooks, tablet computers and so on.

- **Resource pooling:** The provider's computing resources are pooled to serve multiple end-users using different physical and virtual resources dynamically assigned and reassigned according to the end-user needs. The pooled resources include storage, processing, memory, network bandwidth, and virtual machines.

- **Rapid elasticity:** The capabilities can be rapidly and elastically provisioned (in some cases automatically) to quickly scale out and rapidly released to quickly

scale in. To the end-user, the capabilities available for provisioning often appear to be unlimited (or boundless) and acquirable.

- **Measured services:** Cloud computing has the capability to measure the access to the cloud resources. For example, due to the providing transparency about the amount of usage for both customer and service provider, the usage of the resources is monitored, controlled and reported.

2.2.2 Cloud Deployment Models

In general, cloud computing comes in four primary deployment models such as public, community, private, and hybrid. The figure 2.1 depicts the general cloud computing elements.

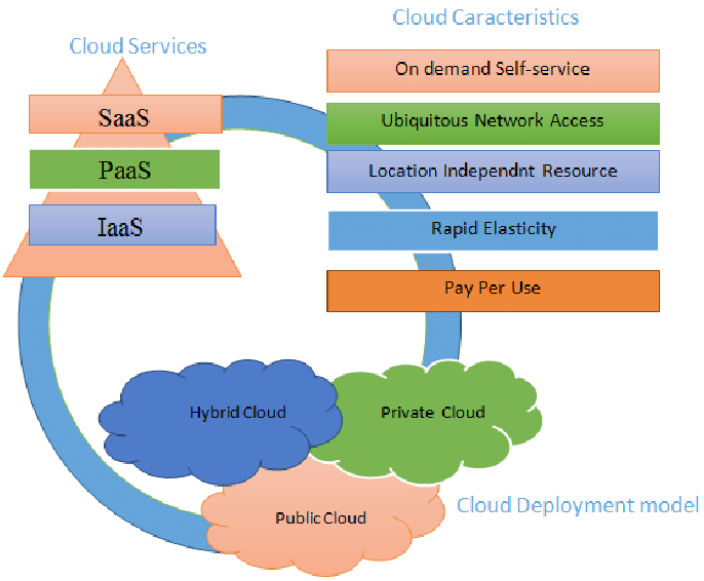


Figure 2.1: Schematic presentation of cloud computing elements [1]

1. **Public Cloud**
   The public cloud is the most commonly referenced regarding the cloud computing solution. This cloud infrastructure is made available to the general public or a large industry group via web applications as well as web services and is owned by an organization selling cloud services. The cloud service on offer in a public cloud is often provisioned through a SaaS, PaaS or IaaS setting, for example, a public CSP such as Google which makes its Software-as-a-Service (SaaS) offering like Gmail available to a wide range of cloud customers [31]. It is publicly offered to many cloud customers without restriction by a cloud service provider. [31] [32]. The term public doesn't mean that users' data is publicly visible.

   In this model, as mentioned before, the infrastructure and applications are owned and hosted by the organization selling cloud services. Again here, the customer has no visibility over the location of the cloud infrastructure, the infrastructure is shared between organizations [33].

2. **Private Cloud**
   The second type of cloud computing is 'Private cloud'. This cloud infrastructure is operated solely for an organization. In other words, in this model the service access is limited and the customer has some control / ownership of the service implementation [31] [33] [32]. Furthermore, It can be managed by the organization or a third party and can exist on premises or off premises. This type of cloud provides an organization a single point of control for security, manageability, privacy, audit, compliance and governance [34] [32] [35]. This means, the infrastructure policies are governed by a single organization where workloads and data can be moved to and from internal and external data centers. For instance, an enterprise IT, building a private cloud service used only by its enterprise. Or an other example, a virtual private cloud (the same as the example above, except replace 'enterprise IT' with 'third-party provider') and community clouds (the same as a virtual private cloud, except opened up to a specific and limited set of different enterprises).

3. **Community Cloud**
   This type of cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns and goals such as mission, security requirements, policy, and compliance considerations [31] [33] [35]. This model of cloud offers higher level of privacy, security and policy compliances. It can be managed by the organizations or a third party and can exist on premises or off premises [33] [32]. For instance, all the government agencies in a city can share the same cloud but not the non government

agencies. Popular example of this model is Google Gov.

4. **Hybrid Cloud**
   Hybrid cloud refers to the cloud computing infrastructure composed by two or more clouds (private, public, or community). This cloud deployment model exists due to mixed needs of an organization as it is a form of bridging two different type of cloud infrastructure [31] [33] [32] [35]. For instance, an organizations host its critical and secure applications in private clouds to have them in their control but not so critical applications are hosted in the public cloud.

2.2.3 Cloud Service Models

Cloud computing consists of various types of services that are delivered to the users as on-demand. Depending on the type of cloud (private, public or hybrid), there are the three most common service models (IaaS, PaaS, SaaS) where currently the industry has been successfully adopting as an alternative cost effective solution compared to the traditional in house Information Technology (IT) solutions.

1. **Infrastructure as a Service (IaaS)**
   IaaS is one of the common cloud computing model in which an organization outsourcers the equipment used to support operations including storage, hardware, servers and networking components. [30] [33] [32] [29]. Figure 2.2 illustrates the SaaS model.
   In this model, all the processing requirements such as storage, CPUs, networking hardware, servers, and virtualization technology are hosted by the cloud service providers on their on-premise data centers. Accordingly, the end users only pay for on-demand computing resources they need [33] [30]. Moreover, the customers do not administer or maintain the underlined cloud computing system but have total power over the systems operating such as space, applications implemented and perhaps regulator that is limited for networking selection components [33] [30]. Example of this service is Amazon EC2 and Amazon S3.

   As the focus of this study is the cloud storage (belongs to this service model), we dive a little bit deeper into the details of the cloud storage service.

   - **Cloud storage service:** The exponential growth of electronic data in current era and the need to keep this data for longer period has made the business owners and individual to think how they should manage and use their data. Cloud providers came with a novel and impressive solution under the term of 'cloud storage service' to store all user's data in

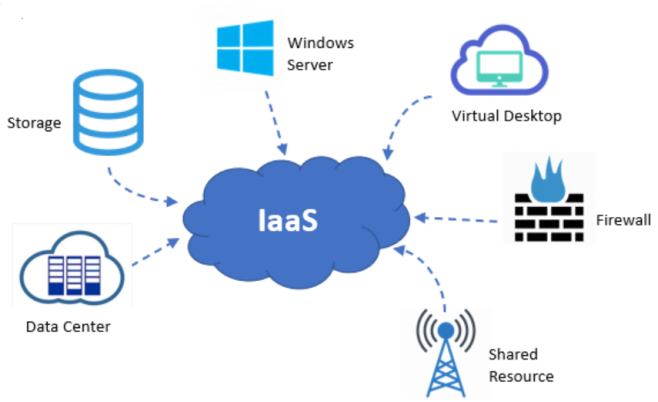


Figure 2.2: Infrastructure as a Service [2]

the internet. This cloud service offers a large pool of storage for user with three significant features such as: Availability, Durability (sustainable and protected from crashes) and Performance (speed of the data access) [35]. In this model, the data is maintained, operated and managed by cloud storage service providers on storage servers in large data centers. [29] Actually, this solution seems to portend a major change in how to store information and run applications. The storage possibility in clouds and synchronization services let users access their digital data any time, from anywhere and with any device (smartphone, tablet, or desktop PC) [33] [29]. Although such cloud services are generally seen as advantageous to end-users, in terms of flexibility of access and scalability of costs, these benefits come at a price - lose of data control.

2. **Platform as a Service (PaaS)**
   PaaS is one of the cloud service models that provides the end users an environment that can be used by developers and organizations to host, develop, run, test and deploy their applications and software's through platforms over the internet without installing base software's on their computers. [30] [32]. Figure 2.3 shows the PaaS model.

   One of the benefits PaaS offers is its cost efficiency. Due to the high costs associated with buying developmental software's, PaaS provides a cheaper alternative, as the disadvantages of directly owing such software is passed on to CSP, in addition cloud customers have the ability to enjoy benefits of elasticity, efficiency and workload management [31]

   This model is a cost-effective solution that suits the business needs of small to medium-sized organizations. Example of this service is Windows Azure.

3. **Software as a Service (SaaS)**

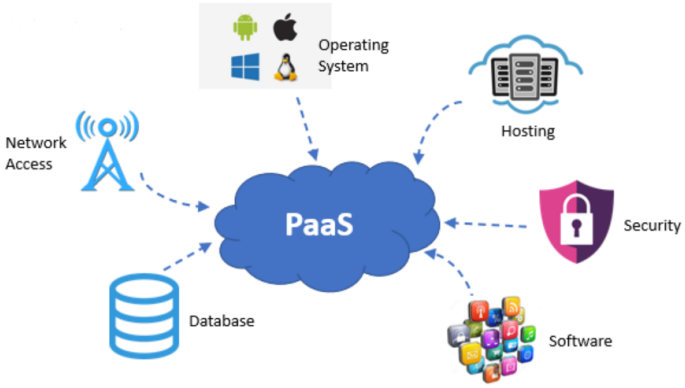


Figure 2.3: Platform as a Service [2]

In addition to the above aforementioned cloud service models, SaaS is also another common service model that provides the end users the software which is hosted off site by the third party. The customer does not need to worry about the updates and the underlying infrastructure needs [30], as it is the responsibility of the service provider. Figure 2.4 depicts SaaS model.
In this model, provider facilitates the end-user with licensed applications running on a cloud infrastructure through a customer interface such as a web browser over the internet. They are managed completely including by cloud providers - updating and patching are in the provider's responsibility- on pay-per-use pricing pattern [33] [30]. Customers do not need to manage or control the underlying cloud infrastructure including network, servers, operating systems or storage [32] [30]. It is based on the concept of renting an application from a service provider rather than buying, installing and running software yourself. Example of this service is Google docs and Dropbox.

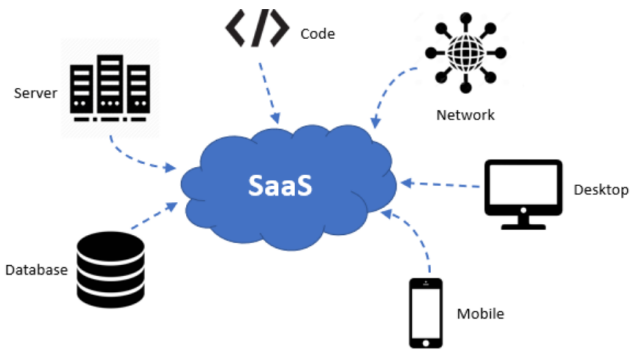


Figure 2.4: Software as a Service [2]

2.2.4 Security Threats in Cloud Computing Models

Cloud computing is a way to access the services and resources. But expert in this field believes and of course it is evident that the cloud computing brings also some threats that compromise the CIA (Confidentiality, Integrity and Availability) of the resources.
Different security risks that threaten the cloud services are discussed below.

- Invalid Storage: There is the possibility that data is stored in an inappropriate storage spaces, because if the data is stored in the right storage space then the CSP must be paid for this and of course that is not cost efficient for the service provider [36].

- Insecure Interfaces and APIs: As users are provided with many available APIs to use and there is also the possibilities to build combinations of other APIs, known as Mashups. Here, those interfaces have serious standardization problems which makes difficult to apply a consistent security policy and the consequence is that many times access control, authentication, entry treatment, traffic of encrypted data, monitoring of activities, among other security aspects are neglected, offering a huge risk to cloud computing [37] [34] [36].

- Malicious Insiders: This threat represents attacks of an active cloud administrator or business partner from the cloud provider that is authorized and has some access level and compromised the CIA of information stored in the cloud [37] [29] [34] [36].

- Shared Technology Issues: Considering the IaaS model, some components of this architecture can not be configured for the scalability demanded from the model, making necessary to implement virtual machine monitoring to manage its resources. What makes it vulnerable is that most of the time, this layer does not have an adequate defense strategy and does not exert a good monitoring of network security [37] [36].

- Data Loss or Leakage: Any exclusion, change or improper appropriation of some data in the cloud is results in data leakage or loss [37] [29] [36]. This threat can be very potential for cloud storage.

- Account or Service Hijacking: Phishing, fraud and vulnerability exploration, besides password credentials used in distributed ways, has empowered this threat regarding cloud solutions [37] [29].

- Lack of user control (data sovereignty): As soon as the data goes through the CSP infrastructure, the control of the data by data owner is lost. So how can a

consumer maintain control over their data when it is stored at third party hand and processed in the cloud. Moreover, in the case of requesting data back from CSP, it is also difficult to get data back from the cloud and avoid vendor lock-in [29] [34] [36].

- Control over Data Lifecycle: Another significant challenge about cloud is being ensured that the user has full control over the lifecycle of their data and in a deletion. It means, how to be sure that data that should be deleted are actually deleted and are not recoverable by a cloud vendor [29]

- Virtualization: Virtualization is the foundational component of cloud computing which assists in delivering the core values of cloud computing. In order to run a guest operating system as a virtual machine in a host operating system, a special function called hypervisor is required. At the same time, technique poses a serious risks to the stored data in the cloud because a hypervisor can become a primary target if it is vulnerable. Or if it is compromised, the whole system can be compromised and hence the data [34] [36].

- Data Interception: Because the data in cloud is segmented and distributed in transit, this creates some threats due to the vulnerability and fragility of the computing technology. Specifically, sniffing and spoofing, third party attacks and reply attacks [34].

- Data Center: It is obvious that CSP provide several copies from the user's data stored on their serviers in the case if needed, they can be provided. This can resulted in few risks. One of the risks is that if any information that is stored on servers and they are not used for a long time, it is possible to be removed from the storage servers. Or another risk is the multiple copies copied from the data by the service provider which can also lead to data theft or leakage [36].

- Data Protection: One of the significant challenge in adoption of cloud computing is the security of the data. In particular, this concern related to the personal information which maybe used for certain purposes [36].

2.3 Data Sovereignty

Until 2013, exactly when Edward Snowden has made the headlines by his revelation about bulk information collection programs of the US and UK security agencies, the term of 'data sovereignty' was not very common in cyber domain. However, regularly the concept of data sovereignty has been used in other domains such as politics, industries and law but still it lacks a fixed definition [38]. To know what

'data sovereignty' is, we would like to refer to Baezner and Robin (2018) that they define the data sovereignty as a state's ability to control data originating and passing through their territory and includes set of measures employed to achieve that control. In the same way, Peterson et al (2011) defines it as a way to limit the transfer and storage of data to a specific territory [39].

Eventually, to make the data sovereignty concept more clear, in the following it will be explained in details. In the current data decade where data represents the lifeblood of every organization, when data is stored in cloud in many different countries having various jurisdiction, this data is shared across country borders. Then it can be subject to these different jurisdiction. Under different data protection laws, a user's data sovereignty can be violated when a third party is using data in breach of another person's contractual or other rights or in a way that causes that other person to be in breach of their own legal or regulatory duties. More specifically a breach of data sovereignty is likely to happen in a situation where:

- A third party (typically but not always a government agency);
- has the power to access the data of another individual (for example cloud customer);
- where that data is in the possession of the customer or someone else on the customer's behalf (the cloud service provider);
- with or without the consent or knowledge of the customer and/or the cloud service provider.

Finally, data sovereignty refers to the concept that the data an organization collects, stores, and processes is subject to the nation's laws and general best practices where it is physically located [40]. In general, the concept mostly relates to issues of control about who can access and process data. As a consequence of the Snowden 2013 revelations in relevant to NSA and USA mass surveillance programs, a wide fear in international level is created. This fear and concern made the states across the globe to frame laws and regulation (e.g. European GDPR) towards securing their data.

2.3.1 Data Sovereignty in the Cloud

Currently in the age of digitization, data and information has emerged as a central commodity in most modern technologies and applications [39]. As cloud solution has caused a fundamental shift in the delivery of IT services, most of the computing activities including the storage of data (in some causes even sensitive data) has been also shifted into the cloud. This trend shows the way of moving from a

peer-to-peer decentralized computing environment to a centralized client-server environment that possess huge processing power and storage capacities. [39] . At the same time, these data represents the intangible assets of every organisation which outsourcing them results in direct lose of control over the data. So, it should not also be ignored that when these data-driven technologies yield benefits and potentials, but also confront the organisations with challenges in retaining control over their data and lack of the trust and transparency behind the blurry cloud infrastructure. There are different serious concerns regarding cloud storage, but as the focus of this study is data sovereignty' or 'data control', among all, the following are the most significant challenges to be highlighted [41] [42] [4]:

1. Losing of physical control over the data and therefore must then rely on the cloud provider for security.
2. By the outsourcing the data, CSPs agree by a SLA (Service Level Agreement) contract regarding the data preservation including the geographical region. But verifying that CSPs are meeting their contractual obligation is another great issue.
3. Dishonest CSP is also key concern. As a CSP, having full control over data can intentionally move data to other regions, to more easily leak information or to avoid legal liability.
4. The insider threats can be also more crucial, especially cloud administrators who gaining more control over the customers' data.
5. Laws and regulations of the hosting country is an other form of risk that threats an organisation's data. When the data is stored outside of a country and is subject to the laws and general practices created by the hosting country, data sovereignty comes into play. It is a complex legal issue that can affect organisations worldwide.
6. Even in the case that CSP encrypts the customer's data both during transit and at rest, still CSP can also easily decrypt it and access it.
7. The governmental agencies or private organizations using the courts can force CSPs to turn over the data or the relevant encryption keys. Often data owners may not even know that such a legal process or court order has been executed. It is also obvious that American security agencies intercept Internet traffic on a regular basis.
8. The change in the overall organisation security, because virtualization introduces new vulnerabilities and there could be conflicts between customers and cloud providers who are both attempting to harden their security procedures.

Thus, it should be noticed that by the emergence of cloud storage, data sovereignty has also created a new rich security issue for nations in the world. This means that organisations around the world share the control of their data with third party when they are stored in the cloud. Here, lack of full data sovereignty has the potential to damage the owners of the data and in specific cause even the governments. This means, sensitive data of a country could be subject to foreign laws and be disclosed to another government. For example, cloud service providers operating in the United States can be legally forced to give third parties access to other nation's data without telling the owners.

Recently, with multiple high-profile data breaches, some governments have been started thinking for taking extra measures to prevent their citizens' personal information from falling into the wrong hands. Particularly, the attention has been directed to issues arising from storage of business and personal data in the cloud in USA and Asian clouds. The more the level of dependency on cloud solutions increases, the more the effects of not having control over the content or infrastructure become apparent. This means, when users decide to store their files on cloud, indirectly the data will be owned by the cloud provider. Although, many cloud users are not aware of this risks but with a full trust get attracted by advantages that can be derived from cloud in terms of costs and flexibility. The implications are many [41]:

- users are giving away their content under a false ideal of community;
- they are giving away their privacy for the sake of a more personalized service;
- they are giving away their rights in the name of comfort and accessibility;

But, most importantly, they are giving away their freedoms and (very frequently) they do not even realize it.

Eventually, data sovereignty is a significant issue, which is often not sufficiently taken into account. The above mentioned risks and issues concerned some states around the world which has leaded to some data sovereignty proposals to be implemented. Among all Germany, China and Russia trying to better regulate their data sovereignty requirements against the domination of the US communications infrastructure and services. [39]. For example, in Germany, this efforts resulted to some potential proposals including national email, localised routing of Internet traffic, undersea fiber optic cables and localised data. In the same way, Australia and India began to manage their data control and solve the sovereignty concerns. As an efficient step towards data control measure, India blocked 59 Chines App due to 'data sovereignty and security' [43]. Or even Canada that made some specific contracts with cloud provider regarding storing of its data in within the Canada territory with cooperation of Canadians. The mentioned examples indicate the severity of the

danger and risk regarding the data control that active countries in cyber domain are concerned and try to address it. It is usual that some hosting countries or jurisdictions may have much worse IT and data security or privacy protections for the data. That means that legal and technical support for adequate online security, confidentiality, privacy and/or data protection vary greatly from country to country [42].

2.4 Strategy

The management of the current complex ICT infrastructure is a challenging task. Recent advanced solutions such as cloud computing, posed a range of extremely serious security and privacy risks such as leakage of sensitive information and surveillance, resulting in significant impact to business continuity. These issues need to be considered as vital factors for business. During last decade, data security and privacy concerns are widely recognized as a significant impediment to consumer confidence in cloud computing. Normally, when an organization that decides to move to the cloud, this transition must always start with a specific strategy that outlines what it wishes to achieve in measurable terms. The term 'strategy' is a familiar word in business context and it is heard mostly at different levels. Different business leaders and business theorists think different about it. In [44] the strategy is described as the way the business operations work together to achieve agreed business objectives in long term. This can be figured out through first recognizing the organization goals and then determining the direction and scope of them over the long term. The author in this paper believes strategy represents a company's resources, strengths, vulnerabilities and opportunities. In general, strategies are formulated with the aim of meeting set business goals. It should be considered that the emergence of the new technological solutions and their related risks push business owners to rethink their strategies and adapt them to address cloud-related risks.

2.4.1 Types of cloud storage strategy

As one of the most potential challenges in cloud storage was explored and important threats were highlighted in Subsection 2.3.1, we were also interested to review the literature to find out the available strategies and approaches that can address this. Because to adopt a cloud service, alongside the desire to benefits from all the offered services, a customized strategy is of significance. The selection and execution of a migration strategy amongst the possible, situational and commonly used options is a critical part of cloud migration process. A strategy that also considers the privacy and security as serious factors of cloud adoption and should be determined during the migration process. To understand the context and which strategies are

currently available, we decided to search through the existed scientific literature and collect information about the current available strategies used in IT industry. The review (including the studies provided in Table 2.1) revealed that the current existed strategies fallen into two different and significant categories.
One category includes the widely used strategies by organisations in practice. It shows that organisations currently follow those strategies based on their popularity in the procedure of transformation to cloud that CSPs offer. However they are not enough efficient because they don't consider all important factors to preserve the data control enough. In fact, those can be named as general propose cloud adoption strategies. Here Six R's [45] is a common example of those general propose cloud adoption strategies which is offered by CSPs.

- **Six Rs (Rehost, Replatform, Repurchase, Refactor, Retire and Retain):** It is developed by Amazon (extended version of 5 Rs which was developed by Gartner - namely Rehost, Refactor, Revise, Rebuild and Replace) [46]. Via the AWS Cloud Enterprise Strategy Blog, they have been made public and became popular. Today in different organisations, any of these strategies is proposed by the CSP and used as a fundamental guideline for almost any cloud transformation. The general factors considered in these strategies are summarised as following:
  - Options of data storage and replication in a multi-cloud setup;
  - Optimizing data mobility to reduce cost;
  - Parameters for structuring a data storage strategy;
  - Determining the best-fit storage option based on the requirement;
  - Offerings from various cloud platforms and more.

As mentioned above, the focus of those strategies are primarily based on the perceptions about cost reduction, ease of use and convenience, reliability, sharing and collaboration. The lack of security support and privacy factor is still seen as a downside. In this way, cloud service providers offer the businesses unmatched operational agility, velocity, efficiency, flexibility and productivity in their services. However, for example ensuring only the authorised personnel have access to the stored data in the cloud or the data is not seen by other authorities is still the most critical aspects of cloud security that should be important parts of the cloud migration strategy. Opposite to what is perceived by some business owners, when storing data in cloud, the security responsibility of the data is not only by the CSPs but it is also by the organisation which owns the data. When an organisation plan to transmit data to cloud infrastructure, it is imperative that it take measures to protect its data according to a secure strategy. Although, the result of our review revealed that unfortunately

there is no unique well formulated security strategy for clouds that can warrant the data sovereignty in cloud.

At the same time, the other category consist of different migration strategies and frameworks that have been introduced in the literature but due to being unknown for decision-makers, they are not very common. Among all, 3 examples of these are presented below:

- **SLA-DO:** Before explaining the SLA-DO strategy, it is important to understand what Service-level agreements (SLA) is, as it has become an essential part of cloud services. In cloud context, a SLA can be expected to mediate consumers' expectations with respect to cloud service provision [21]. That means, it is kind of agreements between CSPs and cloud users that represents the understanding about the expected level of service to be delivered.

  SLA-DO strategy is based on genetic algorithms (algorithms that brings the higher optimization cost) and has been developed as a novel data distribution strategy for clouds [21]. It focuses on the trade-off of service qualities and resource utilization on multiple cloud storage systems to provide a more appropriate block-level data distribution strategy for cloud storage providers. SLA-DO is consisted of new data placing policy and existing distribution optimization method for cloud storage provider and users to improve their SLAs compliance and resource utilization. It significantly pushes up SLAs compliance, resource utilization, security guarantees and multiple cloud environmental adaptability at the same time.
  In order to evaluate the quality of cloud storage services in this strategy, a quality evaluation model is created which is composed of four metrics (privacy, availability, throughput, transfer time) of SLAs and an essential metric - storage cost - for cloud storage service providers [21].
  In fact, this strategy can provide a way of higher SLAs conformance and resource utilization to place data blocks. However it is developed to address one of the significant concerns - privacy - which has big influence on cloud storage adoption but with the commercialization of cloud storage services, still the security is not supported enough and needs to be developed.

- **Goal Oriented Requirements Engineering (GORE):** It helps cloud users to manage requirement mismatches or gaps between user goals and CSP by screening, matching, and negotiating their requirements against cloud services. In particular, it evaluate the strategic decisions, satisfaction of the technical and operational goals, cost and value of such decisions and the trade-offs involved in moving to the cloud [47] [3]. This method is also novel solution

which aims at providing systematic guidance for organisations evaluating the choice and risks in moving to and adopting a cloud. Using this method and analysing of the mismatches at early stage can inform the existence of risks. This means, the approach advocates risk mitigation in early stages of cloud adoption.

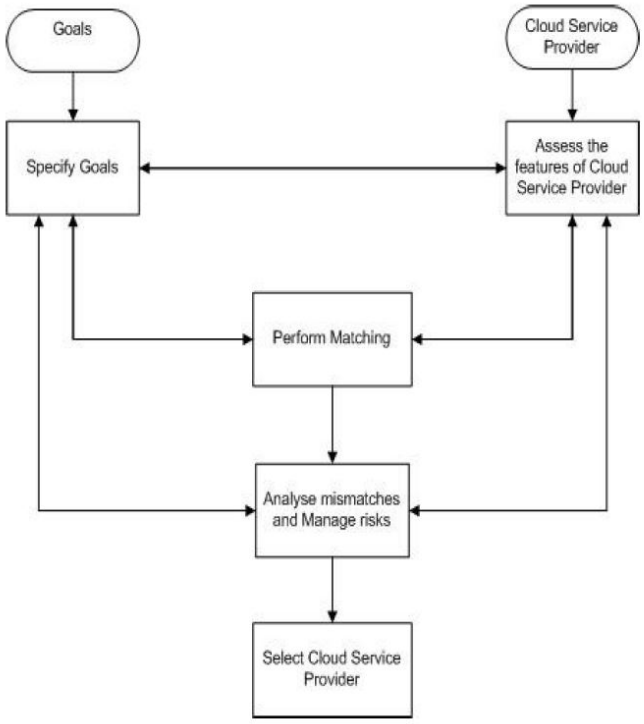


Figure 2.5: Steps for cloud adoption in GORE [3]

Of important considerations in each step (shown in Figure 2.5) in this method are [3] [21] :
a) Define and elicit goals - Three main categories of goal are defined in this method such as: (i) strategic or business goals, (ii) core or high-level goals – the main drivers to utilize cloud services, and finally (iii) operational goals (for instance, data encryption, backup mechanism, password protection, etc).
b) Identify and assess the cloud service providers - evaluating if the features satisfy the defined goals,
c) Conduct scoring and matching - collecting useful information about CSP and scoring them by matching specific cloud services to the identified goals. This process includes the analysis of CSP's satisfaction and gaining the opinions of the users regarding their experience with that CSP. Or as an alternative, some clouds may offer the user trial period where the user self can see the degree of satisfaction of the cloud.

d) Assess the gaps and manage risks - assessment of the gaps then solve those that are possible and evaluate for balancing trade-offs with risks.
e) Select the cloud service provider - the optimal CSP is selected according to specific factors. Those factors to assess the worthiness of each CSP for selection are: value, cost and risk.
In this method, again the security factor is not considered enough. Because it is mentioned as a general evaluation of the CSP to assure that the cloud service / CPS meets the pre-defined goals. In other words, risks are not specifically defined to take the appropriate measures accordingly. As a result, we can deduce that this strategy or framework with insufficient focus on the security can not address the available security challenges in cloud enough.

- **Toolkit for adopting cloud:** As its name indicates, it provides a collection of tools and techniques that support decision making during the adoption of cloud computing in an organisation. Actually it helps decision-makers to view the cloud migration procedure from multiple perspectives and concerns. The main factors considered in this approach are (shown in Figure 2.6) [3] [4]:

  - Assessment of technology appropriateness;
  - Assessment of cost estimation and energy consumption;
  - Assessment of socio-political impacts from stakeholder perspectives.

  In addition, this toolkit has the ability to assess the feasibility of using the cloud services in a organization without needing an external help such as consultants. Another important ability of this toolkit is helping the decision makers to verify the claims made by IT consultancies and cloud service providers. The approach is based on a framework that organizes the concerns of decision makers and match those to available tools with the ability of addressing concerns identified. Because the tools enable decision makers to focus on and model different attributes of their organizations / IT systems. For instance, by modeling hardware infrastructure and applications, it becomes possible to estimate the costs of running that specific system or moving the data in the cloud and then decide whether adopting that cloud infrastructure would be cost effective or not.

  Figure 2.6 provides an overview of the processes included in Cloud Adoption Toolkit method and how it can be used. It proposes to incorporate the following five techniques including Cost Modeling tool (a tool that addresses the challenges of cost analysis) that is believed to be potentially useful [4]:
  a) Technology Suitability Analysis - Assess the technical fit (supports decision

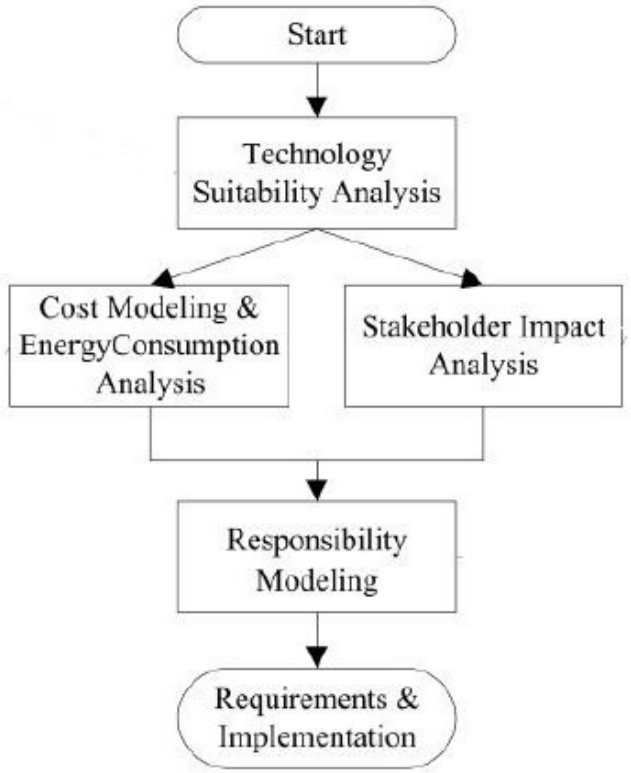


Figure 2.6: The cloud adoption Toolkit & conceptual framework [4]

makers in determining whether cloud technology exhibits the appropriate technological characteristics to support their proposed system);
b) Energy Consumption Analysis - Assess the cost and energy consumption associated with the use of cloud solution (support decision maker in obtaining accurate estimates of the costs and energy consumption associated with using cloud services and support system architects in doing an evaluation of the design of the proposed service in the term of its operational costs);
c) Stakeholder Impact Analysis - Assess organisational fit (identifies the potential impact of proposed changes to work activity brought about by the system in term of: i) practicalities (time, resources, capabilities), ii) social factors (value, status satisfaction), iii) political factors (fairness of the procedures, fairness of distribution or benefits, drawbacks and risks));
d) Responsibility Modeling and Cost Modeling - Assess the operational feasibility (identifies the potential viability of the proposed system by mapping responsibilities and i) verifying that a workable set of responsibilities will bring about about the desired non-functional characteristics of the system, ii) determining the socio-political acceptability of the strategic dependencies between

organisations and departments).
Of course business owners are free to use other mature available tools in each step. What is obvious is that the main focus of this approach is cost and financial benefits which again the security factor is not considered enough.

After reviewing the several literature and presenting the above mentioned strategies and methods as examples, we noticed that none of them take data security factor into account. Understanding the organizational benefits and drawbacks is not enough when moving to cloud. The security and safety of the data in cloud requires more strategic decision which general propose cloud strategies do not satisfy the security needs of the data or in particular data sovereignty . In practice in some causes (according to our personal experience) there are even organisations that do not have an adequate strategy or practical system for minimizing or dealing with risks raised related to clouds. However, in the cause of those organisation that have a 'general business strategy', they follow that for data migration to cloud as well and for security aspect basically they accept standard cloud providers strategy which is not recommended from security perspective. Because, in fact their existing document or data management policies and strategies may not cover, data control, jurisdiction or location, nor recognise challenges thrown up by a somewhat hybridising cloud services environment. Consequently, without a cloud storage security strategy it will often not be clear how the security function contributes to the overall aims of the organisation's data assets. A successful cloud transition is all about having and following a security strategy to take informed, and thoughtful decisions on the various elements including data control that makes up the cloud.

2.5 Data & Data Classification

Before explaining the data classification and its impacts on organisation information security, it is important to know what data is in a company. We can say data is the main business asset when using technology. This data can be any organisational information, from 'public' to 'top secret' information.

In order to align the appropriate security measure and protect the organisation's data in cloud environment, 'Data classification' is a an important and essential step in security risk management. It helps to identify the types of data that are being processed and stored in cloud environments owned or operated by a third party. Moreover, it helps to making a determination on the sensitivity of the data and the likely impact should the data face compromise, loss, or misuse [48].

As data classification has a huge impact on the security of the data, according to the previous research, it has been used since decades back to help organisation

take the needed security measures. Storing data in a cloud storage and considering 'data sovereignty', data classification is a starting point for determining the appropriate level of controls for the confidentiality, integrity, and availability of data based on risk to the organization. In general, data classification level is associated with a baseline (depends on any national/regional regulations) set of security controls that provide protection against vulnerabilities, threats and risks commensurate with the designated protection level.

2.6 Conclusion

The rapid growing trend of cloud computing has led many organisations and even individuals moving their computing operations including sensitive data to the cloud without being enough aware about its security issues. Considering the current security situation in cyber domain, the main goal of this chapter was investigating specifically about the cloud storage security challenges - 'data sovereignty' - and providing background information before defining a security strategy to help organisations with preserving data security during moving to cloud storage environment. To achieve this goal, one main research question was formulated as follow:

- **RQ: How to design a secure cloud storage strategy that minimize the data sovereignty?**

In order to answer this main research question, some preliminary questions were formulated. Then to provide the appropriate answers to each of those preliminary question, an extensive systematic literature review was conducted. In this Chapter, attempted the answer the following 5 preliminary-questions:

1. *PQ1: What is cloud technology?*
   This Chapter started with providing the answer to the first preliminary question aiming to gain understanding of cloud computing, its features, deployment models and services according to the reviewed literature. It was explained that CC has emerged as one of the most influential technologies on a global basis. This solution comes in different deployment models such as 'Public Cloud', 'Community Cloud', 'Private Cloud' and 'Hybrid Cloud'. Each with different characteristics that provides different enterprises what they need. Although there are various type of cloud services, but the three most common types are: Saas, IaaS and PaaS. They differ according to the type of capabilities or level of abstraction that is available to the cloud service customer.

PQ2: What is data sovereignty?

To provide an appropriate answer to this question, a separate literature review was conducted. As a result, in Subsection 2.3 of this Chapter data sovereignty is described as a serious challenge to everyone from governmental level to individual aiming to adopt cloud storage and it is here to stay. When using the cloud storage, the data is transferred into cloud platform in different geographical area under different jurisdictions. It is obviously mentioned that once data is placed in cloud data centers, the data owners lost their direct control over their data sources and this control is shared with CSP. Moreover, those data can be threaten by several potential risks such as losing of control over data, dishonest CSP, different laws and regulations than the origin country, malicious administrators and etc. Finally, before data migration to cloud, several factors should be considered including security and data sovereignty.

PQ3: What are the different cloud storage strategies that are discussed in literature?

Cloud adoption is a complex procedure. When an organization decides to use cloud storage and transfer its data to the cloud, this transition must be managed properly and securely. The literature review results indicate that it is perceived that flexibility and scalability offered by cloud services will easily address all the business demands, but the suitability of cloud services from the security and privacy perspective requires a secure cloud strategy not a general propose strategy of an organisation. It would be always better to start with a specific security strategy that outlines what a organisation wishes to achieve (in the term of security), the resources, strengths, vulnerabilities and opportunities. Because strategies help organisations to define the way their business operations should work together to achieve the agreed business objectives in long term. Since migrating to cloud storage has a huge impact on the whole organisation, it was interesting to find out that with the rapid grow of cloud adoption what kind of cloud storage strategies have been developed and are used today in companies. As the result of our research, we found that there is not a pre-defined strategy specific for cloud security and privacy. However there are some general purpose strategies which can be divided into categories. Those strategies which are widely used and offered by CSP (the strategy that CSP owns) and the other kind of strategies which are only presented in the literature but they are not known very well in practice. Among all, four strategies and methods explained in Chapter 2 (Six Rs, SLA-DO, GORE and Toolkit for adopting cloud) are presented in this paper as examples which all of them do not consider the security factor properly as they are general purpose strategies. Moreover, this review identified a lack of maturity in decision

making based on an suitable strategy to support secure cloud migration. In order to address the stated problem - data sovereignty- developing a 'secure' strategy that considers the security aspect as a vital factor is of significance.

SQP: Do they facilitate data sovereignty?
To provide answer to this question, various related literature were reviewed. The review results showed that in organisations the flexibility and scalability that cloud services offer address all the relevant business requirements, but the security and privacy factor are not very ideal from the security and privacy perspective. Because the cloud services are used widely by organisations of different sizes and the security aspect is one of the most important factor, we tried to find out what kind of cloud storage strategies are currently available and also used today in companies. As mentioned earliser, the review revealed that currently there is no unique efficient strategy that cover all the needed factors including security of data in the cloud storage. According to the literature and researches previously done by experts in this field, an organisation aiming adopt cloud services, follows its general company strategy or cloud provider's strategy which does not consider the security and privacy aspect enough.

SQP: What is the data and how data classifications influences the security controls needed to preserve the confidentiality of data on cloud?
Data is the main business asset when using technology. This data can be any organisational information, from 'public' to 'top secret' information. In order to protect the data, data classification is an effective way of preserving the security. In the context of information security, classification of data is based on its level of sensitivity and the impact to that organisation. Classification of data can be considered as the initial step towards data security. Because identifying the type of data (based on the sensitivity), the appropriate security measure can be assigned. Eventually, data classification has a significant influence on the security of data.

Chapter 3

Methodology

This Chapter presents the details of the methods used to explore the existing literature (using systematic literature review), the practices (using an interview study) and developing the secure strategy for cloud storage.

3.1 Phase I

3.1.1 Literature review

In order to provide a balanced and objective summary that is relevant to meeting a particular need for information, we followed the guidelines defined by Kitchenham et al [49] in the process of systematic review for literature.

A systematic (literature) review is “a means of evaluating and interpreting all available research relevant to a particular research question or topic area or phenomenon of interest” [49]. We decided to use this methodology because through this method, we can collates all relevant empirical evidence in order to provide a complete interpretation of research results. In other words, it can help us best to deliver a clear and comprehensive overview of available evidence on our research topic.

This methodology consist of several discrete activities, included in three stages: Planning the Review, Conducting the Review, Reporting the Review. Figure 3.1 depicts the general steps.

This literature review significantly uses the process of citation chaining which allows a thorough search, both forward (forward citations) and backward (backward citations), using a specific literature as a starting point to find more relevant papers.

a. **Planing the review Identifying the review needs:** Search through literature to collect information about: a) Cloud Computing features, service and deploy-

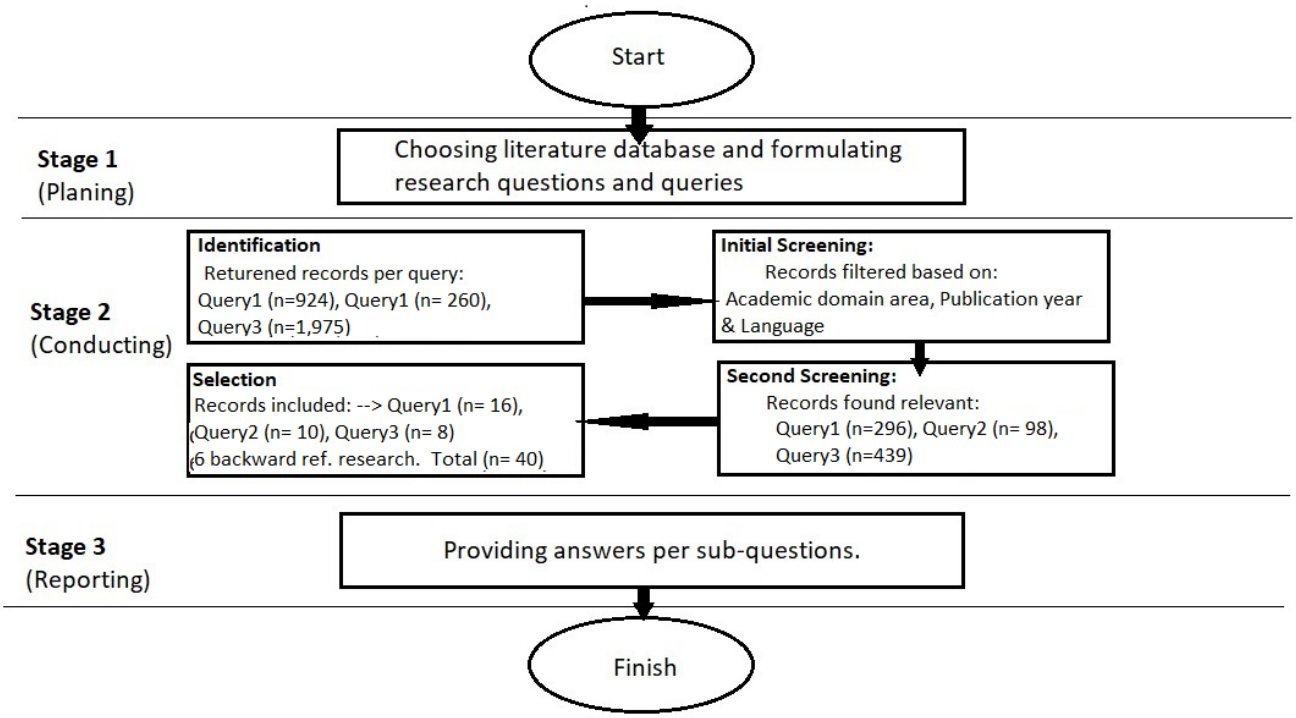


Figure 3.1: Overview of the literature review methodology

ment models, b) Cloud storage security issue, specifically 'data sovereignty' and c) Current existed strategies to identify migration opportunities to the cloud and factors that are considered, d) Data and impacts of data classification on security and privacy of data.

Specifying research questions and search queries: The most critical element of planing the literature review is to formulate the research question(s) and also the right queries to find the information - defining clear, unambiguous queries before beginning the review work. According to the target of this investigation, the following main research question was formulated:

- RQ: How can we design a secure cloud storage strategy to maximize the data sovereignty?

Then, we defined some review protocols/ strategy and eligibility criteria for the study. We decided to consider only English literature. Depending on each (preliminary)question, the specific publication years was determined. After specifying the scientific domain, Scopus as an online database / search engine for collecting the information was also selected. As it is obvious, the literature review provides the structured background necessary to perform the investigation of the

research question(s). So, in order to find the relevant information for each (preliminary)question in an easier, quicker or more efficient way, we decided to run separate queries for different preliminary-question. Eventually, in the construction of the search terms of queries, we considered the following criteria:

- Keywords related to research questions;
- Identification of alternative terms and synonyms of keywords as search terms;
- Searching for information by using the AND and OR logical operator as connectors.

Research Time Frame: According to the update process and modification in the records of the Scopus database, it should be mentioned that this systematic literature review was conducted from April 2021 to Septembre 2021.

b. **Conducting the review** As mentioned earlier, this literature review is carried out using Scopus as an initial online source on the internet by using related search terms. Because Scopus contains comprehensive valid scientific information and also literature which mostly including updated contents in the area of cloud security.

   - To find the available online literature relevant to the **first preliminary-questions**, we conducted a Scopus search that considered the keywords in the following query: *cloud AND computing* AND iaas AND paas AND saas)*

     After first execution of the query, it returned in total 924 records. For this (preliminary)question, the initial filtering through the Scopus options was carried out based on the following parameters:

     – We limited the subject domain only to ”Computer Science” and exclude all other domains.
     – We filtered the publication year between 2010 -2021, as we was interested in the recent publication relevant to cloud computing. Because cloud topic is not a very old research topic.
     – We limited to source type to Journal, Conference Proceedings and Book.
     – We only considered records in the English language.

     Then, the number of the records was reduced to 296 records.

     eligibility criteria:
     After the Scopus filtering options, we started manually screening the papers based on the following eligibility criteria.

As the search terms was applied to the titles, abstracts, and keywords of the articles in Scopus, in following of the Scopus filtering options, we tried to determine the relevant studies by considering their titles manually. For this (preliminary)question, the main topic of studies must be cloud computing (CC), cloud types, cloud service and deployment models. Because the aim of this (preliminary)question was to understand the concept of the cloud and its features. According to these criteria, the more relevant papers were selected for the next stage of reviewing. In the next stage, for the articles that were identified as more relevant, we conducted a deeper assessment by reviewing their abstract, introduction and conclusions or sometimes table of contents if their (main) focus was cloud types, services, deployment models. Finally, 17 papers (including 1 backward reference search) were selected that present general introduction of the mentioned cloud features.

- For the **second (preliminary) question** the following Scopus query was used:
  ("data sovereignty" OR "data control" OR "data ownership" OR "data centralization" OR "data localization" OR "data sovereignty in cyber space" OR "data storage security issue" AND "cloud's" OR "cloud computing" OR "cloud storage security issue" OR "cloud services").

  This query returned 260 records. The irrelevant papers were excluded in the initial screening through Scopus options based on the following parameters:

  (a) We excluded the studies that were from other academic domains and limited only to "computer Science", "Decision Science" and "Business, Management and Accounting". Because we found these subject domains more closed and relevant to my search topic.

  (b) We only considered records in the English language.

  Then, the number of the records was reduced to 98 records.

  eligibility criteria: This review was more concept-centric as it classifies and presents the publications according to the specific security issue (data sovereignty). More review's eligibility criteria for this (preliminary)question was defined as follow:

  – After that we applied the search terms to the titles, abstracts, and keywords of the articles in the identified electronic database (Scopus) and filtered the records through Scopus options, we ordered the results by relevance and a first assessment to determine their significance and this was performed by considering their titles. Titles that clearly reflected that articles were outside the scope of the SR (systematic review) were

excluded. However, titles are not always clear indicators of what an article is about, as “clever” titles can sometimes obscure the actual content of an article. In such cases, the articles were included for review in the next stage.

- In the next stage, for the articles that were identified as potentially significant, we conducted a deeper assessment by reviewing their abstract, introduction and conclusions or table of contents if their (main) focus was cloud storage security issues or data sovereignty in cloud. Some papers discussed security challenges for cloud computing in general and sometimes do not refer explicitly to data sovereignty. We tried to identify and select those studies that emphasised the significance of the data sovereignty and data control by data owner in cloud environment.
- Finally, the articles that were deemed significant(those studies were eligible for inclusion in the review if they presented ’cloud storage security risks’ and their focus was ’data sovereignty’) were read in their entirety. Furthermore, as the research question was concerned with ”cloud security and data sovereignty” and its potential impacts on organisations, studies focusing on other cloud security problems were excluded.
  Finally, 12 papers (including 2 backward reference search) were eligible to be included.

- For the last (preliminary) questions, the following query was used considered the keywords: *(cloud AND adopt* AND strategy OR ”cloud adopting policy”)*.
  This query returned 1,975 records, which was very large number of records. The irrelevant papers were excluded through initial screening through Scopus options based on the following parameters:

  (a) We excluded the studies that were from other academic domains and limited to ”computer Science”, ”Decision Science” and ”Business, Management and Accounting”. Because from our point of view these subject domains more close relevant to our research topic.

  (b) We filtered the publication year between 2015 -2021, as We were interested in the more recent publication relevant to cloud adoption strategies.

  (c) We limited the source type to Journal, Conference Proceedings and Book.

  (d) We only considered records in the English language.

  Then, the number of the records was reduced to 439 records.

eligibility criteria: For this (preliminary)questions review, 'cloud adoption strategy' or 'strategies for cloud migration' must be the main topic of the Papers. First of all, the same as previous, we applied the search terms to the titles, abstracts, and keywords of the articles in the Scopus database. Considering the titles, we could select 47 records which were more relevant. Then we conducted a deeper assessment by reviewing the abstract of all those papers (one by one manually) if their (main) focus was cloud strategy or business strategy for cloud adoption. Where it was not clear enough from the title and the abstract alone, if the publication complied with the criteria the whole publication was scanned in whole. Eventually a decision for inclusion/exclusion was made.
For this (preliminary)questions, 11 (including 3 backward reference search) papers were eligible.

c. **Reporting the result**
In this phase, the finding are presented in the form of the answers for the related questions.

3.1.2 Interviews

To gain information about the facts, current trend of the cloud adoption, cloud selection considerations in practice and identify the existed cloud migration strategies, a semi-structured interview (SSI) was deployed. We decided to use this method because semi-structured interview is a combination of both structured interviewing and unstructured interviewing, and it has both of their advantages. In this way, the interviewees can explain her/his thoughts and even if needed ask questions to the interviewers during the interview, which this encourages them to give more useful information, such as their opinions about core subject issue [50]. The flexibility of this approach, particularly compared to structured interviews, also allows for the discovery or elaboration of information that is important for the research. During the interviews, new questions were added to enable a dynamic conversation, which helps to get more in-depth information, when possible. Then it was analysed how practically business owners and decision makers deal with this procedure in Dutch organisations. The results of these interviews are used to determine the current status of the cloud adoption trend, cloud customer's perception, concerns and security challenges in organisations.
The practical steps for designing and conducting semi-structured interviews are: Setting of objectives, Selecting and recruiting the respondents, Drafting the questions and interview guide, techniques for this type of interviewing, and analyzing the information gathered.

a. **Setting of objectives** The objectives of the interviews are:
To understand the perspective of organizations about the cloud storage. What risks concern them when storing their data in third party environments. How they define their factors for cloud adoptions and how they control their data practically.

b. **Selecting the participants** One of the significant criteria considered in selecting the interviewees is that the participants should work in organisations relate to various sectors but with the common characteristic that all the interviewees should have knowledge and experience in cyber security field. For example, they should have high level responsibility and they should be involved in making decision or their advises have influence on organisation level. Considering these criteria, we believe that their responds according to their knowledge and experience will provide a valuable insight on our research.

c. **Drafting the questions** The sets of questions were formulated with different purposes. The first part of the questions are formulated with the aim of profiling the interviewee and get some general information about her/his knowledge, experience in the relevant organisation and the view point he/ she has regarding cloud security. For example, the daily activities of the participants and the security capacity of the organisation. Second part (core part) includes two sets of questions which aims to get information from two perspectives regarding cloud adoption and the reasons to migrate to cloud and how they select a cloud provider. The second part is focused on security factors, their strategies, how they evaluate the security of cloud environment and how they control their data. After formulating the questions, the research supervisor confirmation was requested. According to the feedback, the questions were revised where needed.
An complete list of the interview questions is provided in Appendix A.1

d. **Interview guide** The interviews have been conducted in October and December 2021, as mentioned earlier with the aim to collect practices within Dutch organisations regarding cloud security and common cloud security strategies. The most of the organisations were government organisations which we intentionally selected. As they own and process more sensitive data.

Due to the corona pandemic, it was preferred to conduct all interviews online via Microsoft Teams application. Before the interview took place, respondents were informed about the research details and given assurance about ethical principles such as anonymity and confidentiality. The participants received the consent form before the interview by email. In case the participants consented to session recordings being made, after receiving the aforementioned explanation verbally,

the Microsoft Teams 'record' option was used to record the session.

e. **Analyse** Exploring the previous steps, in this stage we extract the answers from the gathered information and provide the results. With this aim, the qualitative content analysis (QCA) was used to analyse the information collected in interview transcript.
This data analysis method involves the Identification biases, Defining the code/patterns and interconnection, Searching for patterns and Drawing the conclusions. Qualitative data analysis includes in general the following steps [51]:

- **Identifying biases:** This step is one of the most important. Before starting the interviews, two types of biases were specified: a) Participant biases: the questions that are open-ended were designed to prevent the participants from simply agreeing or disagreeing and guide him or her to provide a truthful and honest answer. Moreover, the questions were designed in a manner that allows the participant to feel accepted, no matter what the answer is.
  b) Researcher biases: We considered that all the data obtained and analysed it with a clear and unbiased mind. We continually re-evaluate the impressions and responses, and ensure that pre-existing assumptions are kept at bay. Moreover, in order to prevent that any word or phrase introduce any biases during the interview, we tried to keep it simple. After the interview responses were documented, we started to review several times to get familiar the contents and specify the biases.
- **Defining the code/patterns and interconnections:** In order to analyze the collected data, first the patterns or codes must be specified/defined. This process is the core of qualitative data analysis. It is as the process of fragmenting and classifying text to form explanations and comprehensive themes in the data. To achieve this step, we tried to go through all the collected data and label words, phrases and sections of text (either using words or phrase) that relate to the asked questions.
- **Searching for the codes/patterns:** After defining the codes/patterns, then we started the analysis. As it is a cyclic process that involves going back and forth to the data, we reviewed the interview transcripts and searched for relations of the texts with the defined codes, compared and categorised the data.
- **Drawing conclusions:** This is the final step in qualitative data analysis. After interpreting the data, the result of the analysis is presented.

Nr	Description	Code
1	Technoloy is always hackable	Risk
2	We don't have any idea what happen for our data at background	Risk
3	Control of data is still a challenge	Concern
4	current security measure for data protection will not be secure maybe for next months	Security Issue
5	The influence of security specialist on the cloud selection is not enough	Cloud selection challenge
6	The security is not considered as important as it should be during cloud selection	Cloud selection challenge
7		

Table 3.1: Codes/Patterns

3.2 Phase II

3.2.1 Developing the cloud strategy

While information security is increasingly dependent on business-driven parameters and interfaces to a variety of organisational units and departments, so to cover both technical and managerial aspects in an organisational environment, a secure strategy should consider all those parameters and aspects.

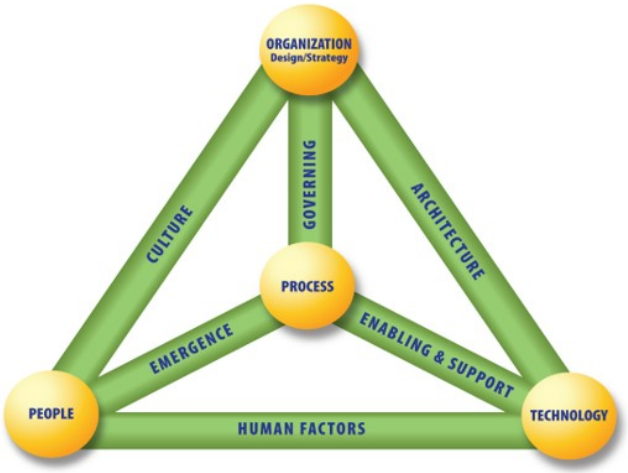


Figure 3.2: BMIS - Business Model for Information Security [5]

Therefor to develop a security strategy for cloud storage that outlines approaches

and key organisational factors influencing the success or failure of security, the BMIS (Business Model for Information Security) is used.

BMIS is a three dimensional Model, visualized as a pyramid (see Figure 3.2), a model for systemic security management which was created at the University of Southern California (USC) Marshall School of Business Institute for Critical Information Infrastructure Protection (USA) [52].

All aspects of the Model interact with each other and of course have impact on each other. If any part of the Model is changed, not addressed, or managed inappropriately, it will distort the balance of the Model. It takes a business-oriented approach to managing information security more effectively [52].

The main elements of this model are as follow: Organization Design and Strategy, People, process and Technology with the six dynamic interconnections that link the elements together. The links are: Governing, Culture, Enabling and support, Emergence, Human factors and Architecture.

Chapter 4

Interviews

This chapter provides the approach, process, answers and analysis of the interview answers.

4.1 Interview approach

The interview was conducted to explore the opinions, experiences and motivations of individual participants and also collecting practical information about the cloud security strategies and methods used in companies when adopting cloud services. Therefore we decided to conduct semi-structured interviews with 16 Cyber Security Specialists / Experts/ Consultants of medium to large governmental and no-governmental organisations located in The Netherlands. As mentioned in previous Chapter, Semi-structured interview was chosen because it consists of several key questions that help to define the areas to be explored and also allows the interviewer or interviewee to dive deep in order to pursue an idea or response in more details.

In order to design the interview in a way that address the aims and objectives of the research, we tried to schedule it imperative to ask questions that are likely to yield as much information about the importance of cloud security and the efficiency of the current in use security strategies as possible. With this aim, we designed to start with questions that participants can answer easily and then proceed to more difficult or sensitive topics. In fact, this helps put respondents at ease, build up confidence and rapport and consequently led to generate rich data that subsequently developed the interview further.

4.2 Participants

In total, 53 organizations were contacted, some requiring multiple points of contact (e.g. initial message, explanation of the research, introduction by work colleagues).

Participant	Role	Sector
P1	CISO	Governmental organisation
P2	CISO	Governmental organisation
P3	Cyber Security Specialist	Health organisation
p4	Cyber Security Specialist	Finance
P5	ISO	Health organisation
P6	Cyber Security Engineer	IT-Company
P7	Cyber Security Engineer	IT-Company
P8	Security Manager	Children Health
P9	Security & Risk Consultant	Construction Company
P10	Security Specialist	Cloud service provider
P11	Security Specialist	Cloud service provider
P12	Cyber Security Consultant	Cyber Security Consultuncy
P13	Cyber Security Consultant	Cyber Security Consultuncy
P14	Cyber Risk Specialist	Finance
P15	CISO	Governmental organisation
P16	Security Adviser	Governmental Organisation

Table 4.1: Overview of the participants

Finally, after advertising on LinkedIn and direct contact via email and telephone, 16 participants from 15 companies volunteered to participate in my study. However, it took more time than expected to find willing participants.
The list of interview participants is presented in the Table 4.1.

All the participants of this research are active in cyber domain right now with different roles such as CISO, Cyber Security Consultant, Security Specialist/Adviser and also Cloud security specialist. The participants are working in various companies in different sectors among others, in Microsoft and Amazon company. They all have had between 2 and 25 years of work experience in IT-Security and Cyber-Security field.

4.3 Interview Protocol

In order to conduct the interview, we followed the principle of funnel protocols. According to this principle, we started to ask broad questions leading to more focused questions. The format of the interview with its details is as follow:

- **Formalities:** This part was started by the introduction of the author, the research, the goals of the interview and also the significance and potential ben-

efits of the study. After that, informing the interview participant of their rights and the confidentiality/anonymity/consent form. Moreover, we asked the participants if they have any questions. Finally, we mentioned once again for permission to record the session. In total, it took 5 minutes of the interview time.

- **Background information:** In this part, the participants were asked to describe their names, work position, experience period and responsibilities. In the following, they were asked some more questions which mostly focused on the daily activities of the participants and the security capacity of the organisation. 10 minutes of the interview time was scheduled to be used for this part.

- **Core questions:** We dedicated 40 minutes of the interview time to this part. Because this part followed the main questions about the research topic that included personal and professional opinions and practices. This section served to introduce the participant to the topic of the research and to define the scope. The questions of this part, provided the researcher with an indication of the participants' experience and perspective.

- **Concluding:** Eventually, during the last 5 minutes, in this part of interview, the participants were asked if the interview participant has any more questions or points to mention. Furthermore, they were told that they will receive the transcript of the interview. As the last, the interview was ended up by thanking them for their time and cooperation.

4.4 Interview answers

In this section, the interview answers are presented and analyzed. We tried to divide the results of the interview into different subsections. Each part is structured according to the main topics discussed during the interview, generally outlining the participants' position regarding the main subject and making use of quotes given by them. First subsection provides demography. The second subsection presents the personal perspective of participants regarding to the security and security risks of storing the personal data in cloud storage. Second subsection presents the organisational perspective on storing the organisation's different types of data in cloud and discuss the security risks and concerns.

4.4.1 Demography

In this section, the answer for the questions from 1 until 6 are provided. First, we tried to ask the participants some questions about their background study, experience and the activities which belongs to their positions in organisations where they work in. 5 of the participants who occupied a high level cyber security position in their organisations, had no background study related to Cyber Security or Information Security or IT Security. The rest had some related background study as 6 of them were specialized in cloud security. On the other side, all of them had several years of experience in cyber domain. 3 of the participants had several years of work experience in some famous cloud companies. More important, some of the participants as cyber security advisor/consultant had experience of working in several organisations at the same time. This also aimed us to get information about cloud transition in more companies in The Netherlands.

4.4.2 Cloud security risks and concerns from personal perspective

Through this subsection, the questions from 7 until 15 are anwsered. This discussion theme covers the participants personal concerns regarding storing their personal data in cloud storage. How they care about their data and based on which factors do the select the appropriate cloud service provider. More important, how they protect their data in cloud storage.

Storing personal information in cloud

When they were asked if they use the cloud services for their personal information and activities, all of them had the same answer (Yes). They confirmed that they

use different kind of cloud services including storage service for their daily activities. In the term of security, they had different perspectives. Most of the participants indicated that the cloud storage is not the very secure option to store very sensitive data such as ID-card, Payment details and etc. They emphasised to store their very sensitive data offline. Among them, some other participants (P1, P9, P15) mentioned that our data can not be very interesting to be targeted by any attacker and putting them in cloud can help us to keep our data more safe and longer than offline.

Data Sovereignty

The participants were asked about data sovereignty issue and how they think regarding cloud storage. All of them were aware that they are using different cloud services in large scale in their daily life. But only 3 participants (P4, P10, P11) were familiar with this term and the rest had no idea what its relation is with cloud storage and how it should be perceived. P1 mentioned that it is not possible to catch full control of our data when we share them with a third party. He added that it is more difficult for us to control where our data is stored, we don't know what happens to our data behind the scenes. In general, most of them did not add enough input to this topic.

Cloud security concerns

The respondents were asked to mention their biggest security concerns regarding of storing their personal data in third party's environment. Again here, most of the participants shared the same concerns. Generally, the risks or threats that were mentioned almost by all the participants are: malicious insider, dishonest service provider and data lose. In addition, there are some other concerns that were mentioned by some participants as P9 believed that all IT-solutions are at end capable of being hacked, so eventually cloud can be one of them. P12 stated his concern regarding some Nation's power in getting access to cloud's data. In this same way, P13 also described his concerns in two factors: 1)It is not clear who access our data in cloud and he gave the example of ”Black-Box” that cloud looks like a black box, ”our data goes in and then we don't know more about it”, 2) Data alteration. Moreover, ”Identity Theft” was mentioned as an other risk by P8. All of them confirmed that the cloud solution is an efficient fact that helps the individual in large scale in term of availability and functionality. Even they said sometime there is no other option than cloud to use for different proposes. But still it has also its own drawbacks in term of security and privacy.

Comparison of on-premise and cloud storage security

The participants were asked to explain their own opinions and confidence about the security of the on-premise and cloud storage. Whether or not they feel enough

secure to keep their personal data on-premise or in cloud. They believed that both have their own advantages and risks. P12 described his opinion as follow: ”Both has their own risks, if you store locally, you need to manage everything yourself and that is sometimes not feasible in the term of technical and knowledge. But if you store your information in cloud, it is somewhere else that still that has issue”. In the same way, P2 expressed: ”I don’t see a lot difference from security perspective. But generally risk surface of data in cloud is higher. On the other hand, to take proper action and control and knowledge on-prem is also a big risk. When we move to cloud we have more assurance, guaranty because they have better knowledge and professionality than on-prem”. P3 said ”The risk of cloud is significantly less than om-prem (if everything configured correctly)”. ” In addition, p13 believed that it depends on which cloud it is, because public clouds are insecure than private. He stated that by default clouds are more secure because they have more budget, knowledge and expertise than on-prem. Among all, one other participants (P7) had different perspective. He mentioned that both has the same security level ”On-prem as a security consultant I know how to protect my data and what can happen, if it goes on clouds I know which security measure and compliance should be and etc. so from my perspective both are the same”. Eventually, the shared idea was that most of the participant were ready to keep their sensitive data in cloud under personal security measure like storing in encrypted form. They mentioned several factors that make them to prefer storing data in cloud than locally. Those important and common factors that they mentioned were: technical measure, professionality and cost. Two of the Participants (P2 , P12) stated that they don’t store their sensitive data in cloud even under strong security measure such as encryption.

Trust in Cloud Service Provider (CSP)

The participants were also asked to share their perspectives about trusting in CSP. It was difficult for them to clearly state their opinions, as P7 explained: ”it is hard to say ”Yes or No”, because we need to trust these CSPs otherwise we can not use their services”. The response of P2 about trusting in CSP was ”yes”, because he believed the whole model is secure. He claimed CSPs have the state of art security, they response very good, they are more secure than local security measures. In the same way, P12 stated his perspective in this way: ” the current big CSPs are in United States certified for HIPPA and ISO 27001 and they know how to be secure. If our data is stolen somewhere else, we will never know what will happen. We do not know actually about all the incidents that happened at the back stage.” In contrast, P13 said ”I review their reports regularly and I do not see their employee breach every week information of clients. So this proves that they are enough secure than on-prem”. In the following, When they were provided with several options (Microsoft, Amazon Google or..) to rank the more trustworthy CSP, Microsoft was the first choice

by 15 respondents but only the employee of the Amazon selected for Amazon. In general, the trust level of all the participants was almost the same. They emphasised they need to trust the CSP to some degree and they must accept the risk otherwise they have no other alternative.

4.4.3 Cloud security risks and concerns from organisation perspective

In the second part of the interview, participants were asked about organisation viewpoint regarding to the security of cloud storage. The questions from 16 until 28 are answered through this section. How they select the right cloud service provider and in general how they manage the migration procedure is discussed in this section.

Cloud security strategies

The respondents were asked about their experiences with cloud migration and their familiarity with cloud security strategy (if they know). Almost all of them confirmed that the cloud migration takes place with not enough consideration on the security factor. P12 explained his experience about cloud migration in two ways: 1) left and shift approach and 2) following some pre-defined frameworks (dedicated to his own organisation). An other participant (P7) believed that it depends on companies. he stated ”if we think about application and network, we always start with test (penetration test of etc) first, but still some companies prefer to move everything first and the test should be later. It means there is no unique method”. P2 claimed they have their own cloud security strategy and according to that the data is classified and not every data should go to cloud. In the same way, P14 stated that they have no specifically security strategy, but a general purpose strategy for their organisation. Moreover he mentioned that Security-by-Design has been always the option for us to follow. Moreover, P5 expressed ” we relied on experience of other organisations as guidance. It was totally based on partners experience”.

The shared and core factors between all participants were cost-efficiency, functionality and availability that influence the security aspect to come less in consideration. All of them stressed the importance of following a specific/unique security strategy as a basis on which organisations can protect their assets in third party’s environment.

The influence of (Cloud) Security specialist on cloud migration procedure

With the question about the influence of the security specialists on making the final decision regarding cloud migration, again almost all the participants had the same viewpoints. They mentioned that organisations ask them as specialist in this field

for advice, sometimes their consultations are accepted by decision makers sometimes not. P14 explained the influence of security consultants/specialist during cloud adoption in this way: ”it is not very good, there has been always problems because we are not understood enough”. P12 also believed the influence of security specialist during decision making is not enough as he said in large projects I see CISO and security advisers are involved but not in small ones. As common perspective, they all also emphasised that influence of them is not enough. They believed that there is still large space to be developed and the security specialist with enough knowledge about the risk surface should influence more the cloud migration procedure in the term of the security.

Organisational data and data control

The participants were asked about the migration of the cooperation data and the required security measure to protect those data in cloud environment. One of the participants (P2) explained that in his company, they try to control their data in cloud by double-encryption. Further, he said they have several policies for data at rest and in transition which they have to comply with these. A the end, he also mentioned these measures are not the only ones but they are enough strong. P14 shared the methods for controlling their data as such: ”we have 3 different classes of data. we use encryption measure at rest and in transit. we use our internal tool to generate the keys for our encryption and we keep all the key materials locally. We call it double-encryption. On less sensitive data we only use CSP’s encryption but for our very sensitive data our own encryption algorithm and CSP’s encryption”. In the same way, P12 described the way his organisation tries to control its data. He explained that he prefers encryption measure with considering of how the key is managed and who protects and stores the secrets. He added that he finds it smart to do it self or a third party. He believed that at this moment, this encryption method and Two Factor Authentication (2FA) are the most strong controlling methods. Among others, P7 stated his opinion differently. He believed that we need to have a security model in place which is not only limited to network security or application security but the whole stuff, like from workstation where end user uses the service to protect the whole system. He mentioned that if a user clicks on a link and infect the system, this can improve and impact the whole infrastructure and even the servers. He emphasised the security control should not cover only the provider side but also client side (on-prem) as well. Following this opinions, P13 was convinced that Identity & Access Management is the right way to control the data in cloud.

Eventually, the shared opinion by all respondents shows that currently with the rapid adoption of cloud services by organisations, there is not appropriate known data protection mechanism at organisational level. In fact, that is due to the lack

of enough available knowledge and capacity in organisations. They shared their experiences in different organisations which in most causes they have no data classification before transmitting organisation data to cloud. They emphasised that data classification is the initial step regarding to data protection. According to their experience, usually organisations transmit all kind of the data with different sensitivity level to cloud without any specific security measure which means they totally rely on CSP security measure. Finally, most of them agreed that encryption, Identity & Access Management and Two Factor Authentication are the important measures to control organisational data to some degree.

Cloud selection factors

In response to the organisational perspective on cloud selection factors/criteria, respondents argued differently. Most of the respondents found cloud selection a challenging task for organisations. Because most of the time organisations consider the other factors such as cost-efficiency, availability, functionality, scalability more important than security. P14 mentioned the certifications, security statements, price and of course professionality the important factors when selecting cloud service. P12 considered data-location, key management & access management, cost, availability and professionality significant elements in cloud service. In this way, P2 found data-location, compliance, the process agreement and certifications important factors. P13 stated important factors from his viewpoint as such: certification, audit right (if the CSP allows) and also looking for to find whether that service provider has had any security incident in its history. The rest of the shared opinions of all participants were data-location, assurance, cost, availability and privacy statements.

GAIA-X

At the end of interview, the participants were asked to share their perspective about GAIA-X - as a European cloud development project and if they can trust more in this pure European platform than no-European. First of all, not all the participants were aware of this project. Only 4 of the participants (P2, P12, P13, P14) knew it. P12 stated:"I am very interested to know about output of this European initiative. What they want to eventually deliver. Some people think it is going to be a European based cloud competitor in market which I do not think this can happen". P2 had different idea, he said:" I can not trust in it, because I follow zero-policy. I do not trust any provider's security measure but rather I trust in my own security measure and that is why I encrypt my data". In the same way, P13 described his idea as such: "I heard about it but I personally believe it is still not pure European, because if you deep in details of it, there are other no-European parties who are involved in this project. I can not fully trust it". Finally P14 added that being European or non-European is not the matter, being enough mature in security and prove its ability in protecting the

customer's data is more important. It needs at least 10 years experience to show its ability and competes with other big market players.

Main barriers during cloud migration

We tried to find the most challenging barriers the companies faces during migration. The participants provided us their information based on their experience. P14 mentioned the lack of related knowledge and mis-configuration as biggest barriers during transition. P6 claimed that the main challenge is that the security appliances with the cloud are forgotten or being done later. Other opinion by P12 was that organisations are not fully ready to move to cloud on the time of migration and this transition without consideration of pre-defined requirements are big problem during the migration phase. P13 stated differently, he claimed he has never faced barriers, because he believed migrating is about one click. But he felt the lack of knowledge of this field in companies can be considered as a barrier. Finally, what they all had as shared perspective was the lack of knowledge of cloud security, lack of framework or strategy to follow and implement cloud solutions.

Security measure to increase the data control

The final part of the interview contained questions about the suggestion and recommendation in order to increase the control of data owner over the data in cloud environment. The respondents were asked which current security measure can increase the security of data or which security measures should be combined that can increase the data control more. The respondents provided almost shared opinions. For instance, the most mentioned recommendation was the proper encryption as strong security measure that currently can be assign.

4.4.4 Conclusion of interview answers

Based on the data collected from the interviews, it can be concluded that however cloud storage has its own security risks but they are consciously accepted by organisations. The participants emphasised that cloud solutions, including cloud storage have their specific risks. They agreed on various factors that threats the data in clouds, such as malicious insider, mis-configuration, issues with IAM and also loss of control over the data. Data-Sovereignty was not very familiar term for most of the participants but when it was explained to them, they confirmed it is absolutely an other potential risk. What interesting we found was that they argued that although these cloud services have their own risks but we need to accept them. They explained how trust in CSPs is difficult but still we, as users of clouds need to trust them to some degree. Participants had different opinions regarding the security of storing data in cloud vs on-premise. As some of them argued cloud storage has higher risk level but most of the participants believed that both have their own risks

which at the end leads to the same results. They emphasised, storing data on-premise or in cloud, we need to take the right security measures otherwise both can be insecure. Furthermore, they found the cloud migration a long and challenging process that needs to take place based on pre-defined procedure or strategy that assure the security factor as well. Right now, the lack of this strategy is one of the big issues in organisations. This can be the result of the immaturity of the topic in organisations as the cyber security is new field and still needs to be developed and considered by business owners. They stated that this immaturity also effects the influence of cyber security specialists role on organisational decisions regarding IT projects. They repeatedly indicated that the current situation should be improved and influence of security specialists/experts needs to be developed. Participants argued that data in cloud environments can be protected through some efficient security measures such as 2FA, encryption and efficient IAM. They believed, in current age, these 3 are the strongest security measures that help us in increasing our control over the data in third party infrastructure. In addition to this, they also stated that during cloud selection, some other essential factors are of importance to be considered such as data location, security relevant Certifications, assurance & privacy statements, audit rapports and Security models. Finally, GAIA-X as an European cloud alternative was presented to the participants to get their perspectives in the term of security. They had various opinions, as some of them found it not important if the cloud is European or non-European, because they claimed the right security measures are more important. On the other hand, some other believed that it can not be pure European as different non-European actors are involved in this project. They believed this dependency will still stay for long-term. So generally, almost all the participants stated GAIA-X can not be preferred only according to its nature as European cloud to non-Europeans.

4.5 Analysis

Exploration and the analysis of the interview answers and perspectives of the participants resulted in several shared and different opinions. We tried to discuss different topics from two perspectives (personal and organisational). In this way, we can understand how different participants make decision when they want to protect their own data in comparison of their organisational data as the responsible to that organisation.

4.5.1 Shared perspectives:

As mentioned earlier, during the exploration and analysis of the answers, we noticed that the participants provided us with some shared views regarding some specific topics. This subsection, presents the analysis of topics that participants had the same views about it. Table 4.2 presents the summary of those shared views discussed during the interview.

The interview answers revealed that all the participants have the same security concerns. Data loss, loss of control over the data, insider threats, hackability of IT and data access managements are currently the key concerns about the cloud storage. It does not matter what kind of data (personal or organisational), these security risks threaten the data security. At the same time, we need to trust the CSPs otherwise we should not use their solutions. This means we need to accept the above mentioned risks when storing our data in cloud. Moreover, exploring the answers, another shared opinion is observed about the cloud security strategy. No one of the participants mentioned specific well-defined cloud security strategy. This also creates another challenge in the procedure of cloud adoption / migration that some of participants practically experienced it. They also felt the lack of a solid security strategy that business owners can base their migration on that. Another important point that this analysis shows is the influence of the security experts on the organisation during cloud adoption. Here, two other important facts play efficient roles in almost every organisation. First: lack of relevant knowledge and Second: immaturity of security field in organisations. Interview answers shows that business owners prefer to rely on their internal capacity even in the case of the cloud and security. For example, they try to not hire relevant cloud (security) specialist during cloud adoption if they do not have the needed knowledge and expertise. Of course it should be also mentioned that this fact is the result of the second fact. Because the the cyber security topic is not an old and mature filed, so business owners do not pay enough attention on this fact. The interview answers also revealed that currently the available security measures which can help business owners to protect the data and maintain their control over their data (to some degree) are proper IAM, efficient encryption and 2FA. Furthermore, as an earlier step towards insuring the security and privacy of the data in cloud , setting the proper cloud selection factors and criteria has significance impact on the data security. Factors such as data location, security relevant certifications & also privacy statements and availability & assurance were the most important factors that were shared focus of almost all the participant during cloud selection. Table 4.2 presents the general shared perspectives of the respondents.

4.5.2 Different perspectives:

The analysis shows also different point of views about some topics. In the following, the different perspectives of the participants are presented. Table 4.3 presents the summary of these different views discussed during the interview.

Discussing the security of the cloud storage and on-premise data storage with different participants confirmed that generally both have the same level in the term of security. That means, the participants stated that the security level is almost the same, however some of them believed the cloud includes more security risks than on-premise and also some other participants claimed storing data locally is more secure. The arguments of some participants indicate that clouds bring more assurance as they have enough professional human resource, more expertise, budgets and etc. Moreover, they added that storing data in cloud, the CSP is responsible for all the relevant management including the security and they are specialised in this which they can do it properly as well. The current situation of the cyber domain and cyber incident rates shows the capability of the CSPs against the current cyber risks and threats, which means that CSPs function enough good against them. However, storing data on-premise has also its own security risks and challenges which mostly is not easy to address them due to lack of relevant factors such as budget, knowledge, assurance and etc. Finally, the analysis of this section resulted that both (cloud and on-premis) have their own security weaknesses and also security benefits. Because those participants who were specialised in cloud security and also had long time experience in cyber domain including CSPs, argued that without strong and proper security measure from the client side, the data can not also be protected in the cloud environment under the CSP's security measure. However, storing and protection of data locally has financial cost, needs enough knowledge and capacity which is a big challenge.

Another difference between the opinions of the participants was about the GAIA-X topic. Currently, all the CSPs are American-based organisations, so trusting in these CSPs by European clients is also a big challenge. When having a local cloud, the trust issue can be addressed at some level. The answers of the participants were different because they saw it from different perspectives. For the personal data, some of the participants were totally fine every where (in/outside of Europe) the data is located. For organisational data, most of them hesitated and they indicated the 'data location' is one of the important requirements when selecting the cloud storage. In addition, according to the answers of the some participants, pure European cloud which has enough maturity level that can be comparable with non-European has been always a preference but it can not happen soon. This means, the GAIA-X as an European solution can not be acceptable in short term. Eventually, this study

showed that GAIA-X needs to get enough experience, reputation and also prove its purity in the European market in order to build trust and then the European clients can switch to it. Table 4.3 presents different perspectives of the respondents.

4.6 Conclusion

This section concludes this chapter and present the result of the interview with a comparison with literature review.

The interview was conducted to get practical information regarding cloud security issues with a focus on data sovereignty and how they address this issue. As presented in the previous subsection, there are several cloud security issues including data sovereignty which organisation practically experience them. Currently, with the rapid adoption of cloud by organisation, the lack of knowledge is one of the main challenges that organisations face. Through the interview with 16 participants, we found that the biggest challenge in cloud migration is not only the lack of solid security strategy, but lack of knowledge & expertise is also an other big issue. This is according to what all of the participants also emphasised that insufficient cloud security manpower effects the proper cloud adoption. In fact, cloud relevant knowledge and efficient cloud security strategy are the main factors that can help in maintaining the control over data in cloud environments. In other words, being familiar with the cloud related risks and threats, having the right knowledge & expertise leads to proper selection of cloud security model, appropriate security measures which eventually assure the organisation security. By referencing to the previous Chapters (specific Chap.2) the results of systematic literature review also revealed the same security risks that interview participants mentioned. As the lack of cloud security strategy was also strongly confirmed in available literature.

Eventually, comparing the results of literature review and expert's interview, we can notice that successful and secure cloud migration requires combination of several significant factors such as involvement of security experts with the relevant knowledge, availability of cloud security strategy that the migration should be based on it and selecting of the right tools & technologies.

In order to address / reduce these risks and maximizing the data sovereignty, the main solution is developing a cloud security strategy. As this study investigates the cloud storage related security risks, impacts of data-sovereignty, it also provides a solution that address those risks as much as possible. In the next Chapter (Chap.5), a new cloud storage security strategy is formulated and presented. This strategy is based on the issues and challenges discovered from available literature and also

mentioned during interviews by experts. Considering those risks, we are trying to minimize their potential impacts and improve the security of data in cloud.

Inductive category	Shared views
Security Risk / Concern	- Loss of data. - Insider threats/insider mistakes. - IT is hackable, exploitable and tracable. - Loss of data control. - Misconfiguration - Unauthorised (Nation) access to the data. - Difficulty to verify the agreed points in contract and SLA.
Trust in CSP	- CSPs should be trustworthy to some degree.
Cloud Security Strategy	- There exist no specific cloud security strategy.
Influence of Security Expert	- It is 'OK' for now but it can be developed.
Data Control	- Efficient IAM. - Encryption. - Two Factor Authentication.
Cloud Selection factors	- Data location. - Security Certifications & audit reports. - Assurance & Availability. - Privacy Statements.
Migration barriers	- Change in the company security posture and taking long time. - Lack of knowledge.

Table 4.2: Summary of the shared views of respondents about topics mentioned in interview.

Inductive category	Different views
Security of Cloud vs On-Premise	- It depends on the security measures, the security level can be the same. - Data on-Premise is more secured. - Cloud has higher risk level. - Clouds is more secure because they have more budget, knowledge and expertise. - Data in cloud has more assurance, guarantee because they have better knowledge and professionality than on-premise.
GATA-X	- It depends on local government decision. - It would not stay pure European. - It would be more controllable. - It will still have the professionality issue. - It must get maturity in security level. - European or no-European does not matter, security measures are more important. - It depends on the type of company and the type of data. It can be an option for European clients. - It depends on the factors a company has which is not limited to European/non-European. - American-based companies can not be for long time a trustworthy option for dutch citizens.

Table 4.3: Summary of the different views of respondents about topics mentioned in interview.

Chapter 5

Cloud Storage Security Strategy

In this Chapter, a new developed cloud storage security strategy is presented. In addition, how it is formulated, its important parameters and why it should be the starting point in a cloud adoption process is also explained.

5.1 Cloud storage security strategy

”Securing data in the cloud is not the same as securing data on-premises”, this is what repeatedly was mentioned during interviews with cyber security & cloud specialists. In this connected world, the fact should not be ignored that cloud storage as one of the cloud solutions, brings also potentials risks to businesses which requires efficient risks and security management that can minimize their impacts. As cloud adoption grows, organizations' strategy must also go hand-in-hand with a (cloud) security strategy. A cloud security strategy highlights how the enterprises should preserve the security of the cloud environment and the data contained in it. Procuring a cloud data storage is not the first step in this journey. Companies need solid strategies including security strategy so they can get the best technology for their organization's cloud ecosystem and to get the most out of the system they select.
It should be repeated that the focus of this study is 'cloud storage' and this type of cloud service is explained earlier in Chapter 2. It falls under IaaS service model. Considering the stated relevant security issues in the literature review and interviews with cyber security specialist and focusing on data sovereignty, the main objective of developing this cloud storage security strategy is drawn up to maximize the control over business assets (data) and protecting them by combining security solutions deployed across cloud infrastructures, applications and connections. In this way, it makes it possible to manage centrally the control and the visibility of the data. Such a comprehensive strategy must enable assessing, monitoring and control across three different levels within the cloud environment such as a) Platform, b) Applica-

tion and c) Network. This security strategy can also be interpreted as a plan that involves selecting and implementing best practices to protect a business data from internal and external threats.

As it was indicated in previous chapters (Chap.3), this cloud security strategy is formulated according to IBMS framework and covers various key parameters/elements that have impact on the security of cloud and business data in cloud environment. More important, all the mentioned security measures included in this strategy is extracted partially from the literature review and mostly from interview with experts. All the different critical influencing elements are categorised into: Organisation design/strategy, Technology, Process and Human. Then, all these relevant elements included in the strategy, are explained under these categories.

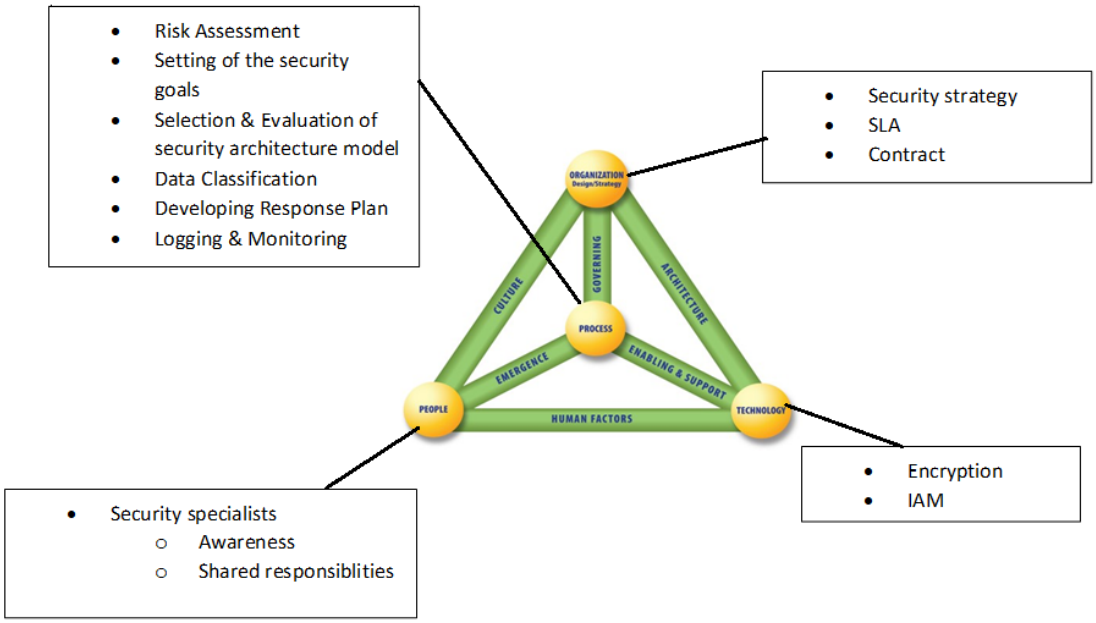


Figure 5.1: Overview of cloud security strategy [5]

In addition, when developing this security strategy, the ”Zero-Trust” security approach/mindset is followed. Meaning, no actor can be trusted until they are verified. This choice was made based on comparing the ”Zero-Trust” and ”Trust but Verify” principles. Thinking about the security, the ”Trust” can be also considered as an potential vulnerability. That is why ”Trust but verify” was not chosen.
Zero-Trust: In short, ”Nothing is trusted or privileged”.
The principles of ”Zero Trust” is as follow [53]:

- Verify explicitly: Based on all available data points, always authenticate and

authorize, including user identity, location, device health, service or workload, data classification, and anomalies.

- Use least privileged access: Limit user access with just-in-time and just-enough-access, risk-based adaptive polices.
- Assume breach: Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

5.1.1 Organisation design/strategy

In the world of rapidly changing technical environment, strategy still remains an essential part of defining clear organization wide goals and how to achieve them. As strategic planning is about setting long-term goals and establishing the directions and constraints, so information security and protection of data in cloud platform should also be an important element of organization's long term goals. This is because cloud is the long-term business solution in every sector. The integration of security strategy with the organisation strategy facilitate more secure and ensured future for a company. Important elements or parameters in this category are explored as follow:

Contract:

The cloud storage contract is beneficial for both the consumer and the CSP. While it can be highly technical and digitalized, the ”contract” will ultimately establish the partnership between the parties and considering some significant factors, should help mitigate any potential problems. Here this strategy emphasizes on the following critical pointers to be considered when negotiating a contract with a cloud provider:

- Certifications;
- Data location;
- Infrastructure security;
- Clearly statement of data egress terms and conditions;
- Security and audits;
- Data Processing (Ownership of data, Disposition of data, Data breaches, Legal/government requests for access to data);
- Back-up and recovery;
- Exit-Strategy.

Service Level Agreement:

In cloud context, a Service Level Agreement (SLA), functions as a blueprint of the service/solution the CSPs guarantee to provide and can protect the business's assets and reputation, which is of the most importance to every organization. It is expected to mediate consumers' expectations with respect to cloud service provision. In order to understand about services, priorities, responsibilities, guarantees, and warranties, in this strategy SLA is considered as a critical part of the contract and agreements between both sides (client and CSP) during cloud migration. Because in cloud computing, SLAs are efficient to control the use of cloud solution. As consumers might not completely trust the measurements provided solely by a CSP, which might require agreed-upon third-party mediators to measure the SLA's critical service parameters and report violations.

5.1.2 Process

In order to start with the migration procedure and following this cloud security strategy from the ground up, the following questions are the most significant that security team should consider in the first step:

1. What are the organization's business goals?
2. What data does the company need to manage to support these goals?
3. What type of data the company has?
4. What data sources does the company use?
5. What data sources does the company plan on using in the future?
6. How will the company meet regulatory compliance requirements for its data?
7. Who needs to access this data?
8. What cybersecurity measures are needed to protect this data?
9. What disaster recovery options are available?
10. What data privacy measures does the company need?
11. How transparent is the company with its data management?

Having a clear overview about the current situation and the future goals helps to set the first steps appropriately. Since the user's data has to be released to the cloud and thus leaves the protection-sphere of the data owner, then the following process should be started as first:

Risk assessment

According to the company profile, the risk level can be specified by the following steps:

- Context establishment & risk assessment purpose: In order to customise the risk management process to meet any company's needs and enable effective risk assessment and appropriate risk treatment, context establishment should be considered as first step. This step involves:
  - Defining the purpose and scope of risk assessment activities such as the relevant objectives, the decisions that need to be made, relevant stakeholders and the extent of their influence on and required resources ;
  - Defining the internal and external context of the company such as organisational values and culture, governance arrangements, policies and procedures and decision-making processes ;
  - Defining the risk criteria to be used to evaluate the significance of risks and to support decision-making processes such as consequence and likelihood definitions, method for determining the level of risk, criteria for deciding when a risk requires treatment, the impact of risk time frames (urgency) and existing risk controls and how combinations of risks will be taken into account [54].
- Risk Evaluation Criteria: Identify key security threats in the cloud. Security risks of cloud computing may include compliance violations, identity theft, malware infections, data breaches, diminished customer trust and potential revenue loss.
- Evaluate Compliance Requirements: Legal opinion should be sought to ensure that regulatory requirements are addressed for specific organizational needs related to HIPAA, PCI-DSS and other security regulations.
- Impact Criteria: An assessment technique that is important in improving risk scoring is developing of company-specific impact criteria. Impact criteria apply to the whole organisation and it is not dedicated to specific information or technology. It reflects the areas that are most relevant to the business or mission objectives. Categories that can be impacted are including at minimum: financial, productivity, business interruption or system availability and etc.
- Risk Acceptance Criteria: Risk acceptance criteria help the decision-makers to judge whether the risk level concerning the business process is acceptable or not - especially when the risk has a potential impacts.

Many factors can influence the view of what should be considered to be an acceptable risk. Some key factors are:

- Benefits gained from taking the risk;
- Degree of control over the risk;
- Risk aversion – one catastrophe is worse then many small accidents;
- Time until effects are experienced;
- Time since risk has been "realized" (time since accidents have occurred).

Setting of the required security goals

A solid and secure infrastructure is the foundation to any successful company. In order to migrate to cloud and build a successful secure infrastructure, identifying the need to balance the two primary objectives such as functionality and security is essential. When adopting the cloud storage, in term of security ensuring the CIA Triad: Confidentiality, Integrity, Availability is vital.

Selection & Evaluation of the Security Architecture Model

Before even considering moving the organization data to the cloud storage, there are a set of common concerns and challenges to be answered by the providers to assure the client organization that using the provider's cloud service is a good choice. Here, one of the main challenges is the risks, where the most important risks are about security. This means, they should place a bigger focus on security and select an appropriate security model. A security model specifically defines essential aspects of security and their relationship with all other systems and services. In general, no company can secure its sensitive information or data in cloud without having effective and efficient security models. The security of cloud services is always the focus of numerous potential cloud customers and a big barrier for its widespread applications. Actually, the main aim of a security model is to provide the required level of understanding for a successful and effectual migration and implementation of key protection requirements in cloud. In order to evaluate the cloud storage security model, it should be considered that well-designed security architecture should be based on the following key principles [55]:

- **Identification:** Knowing the users, assets, business environment, policies, vulnerabilities and threats and risk management strategies that exist within the cloud environment.
- **Trust boundaries:** Between the different services and components deployed on the cloud.

- **Security Controls:** Describes the parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.
- **Security by Design:** Describes the security configurations, control responsibilities and security baseline automations.
- **Compliance:** Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.
- **Perimeter Security:** It helps to protect and secures traffic in and out of company's cloud-based resources, including connection points between corporate network and public internet.
- **Segmentation:** Segments the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of 'least privilege'.
- **Automation:** Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.
- **Implement a Strong Password Security Policy:** A strong password security policy is best practice regardless of the service being used in a company and being accessed by users. Implementing the strongest policy is a significant element in preventing unauthorized access.
- **Flexible Design:** Helps to ensure architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.
  Visibility and Control: A key factor in cloud security is the ability an organization can have to see and control its data. When moving the business assets to the cloud, organizations lose a certain level of visibility into network operations. This is because the responsibility of managing some of the systems and policies shifts to the CSP. A good service provider will offer its client a solution that provides visibility of business data and who is accessing it, regardless of where it is and where company is located. That means, organizations must be able to monitor their network infrastructure without the use of network-based monitoring and logging. The CSP should offer activity monitoring that the client can discover changes to configuration and security across his/her ecosystem.

Compliance

Data privacy is also becoming a growing concern which increase the degree of Strictness of the compliance regulations and industry standards such as GDPR,

HIPAA, and PCI DSS. In order to ensure ongoing compliance, ”overseeing” who can access data and what exactly they can do with that access is the key factor. In general, cloud systems typically allow for large-scale user access, so if the proper security measures (ie. access controls) aren't in place, it can be difficult to monitor access across the network.

Data classification

Data classification is the fundamental part of securing organization's information. Knowing what data a organisation has and who can access it. The study revealed that very few organisations classify their data. This can also be considered as another risk, because knowing the sensitivity level of data helps to protect data with the right security measure. Including this process in strategy, helps to identify and assign pre-determined levels of sensitivity to different types of information. Then based on this classification, data can be transferred and stored in cloud storage under an appropriate security measure.

Developing response plan

A very effective cloud security strategy includes a plan of action which can be used at some points for example in the case of an incident. That means a documented plan with defined roles and responsibilities should be present in organisation. This plan should be tested, reviewed and updated regularly.

Logging and Monitoring:

Ensuring all relevant security events are captured, prioritized and delivered to security teams. It can be interpreted as a constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations and awareness of threats.

Security Awareness

The level of awareness in the organisation affects the general security of that organization. As cloud services are used in most businesses, so cloud security awareness has become imperative to prevent user risks and data breaches. Because users are the first line of defense in secure cloud environments, then unaware employee about her/his role in security is a big risk. Security awareness helps users including both employees and stakeholders understand the role they play in helping to combat information security breaches. Investing in effective security awareness training,

the employees understand proper cyber hygiene, the security risks associated with their actions and to identify cyber attacks they may encounter via email and the web. Moreover, the participants during the interview also claimed the insufficient involvement of the security specialist during cloud adoption. Further, they argued the lack of security awareness in the higher level of the organisations is the main reason. The decision makers are unaware of the cyber domain and all its relevant risks, this makes them to rely on their own capacity and don't refer to the right people with the relevant knowledge. In order to address this challenge, the involvement expertise and periodic security awareness is one of the important aspects that this strategy focus on it.

5.1.3 Human

In the procedure of cloud migration, human resources, in the form of various teams in a company are involved which among others, the security team must focus on reducing business risk from attacks and work to get confidentiality, integrity, and availability assurances built into all information systems and data.

Expertise

For many organizations, the shortage of (cloud) security specialist in the workplace is a big challenge, this was also confirmed strongly by some participants (P6, P7, P9, P13, p14 and P16). However, this issue was generally one of the topics that all the interview participants agreed on it to some degree. Involving the right people with the relevant expertise in the migration procedure even can prevent many risks that may happen. For example, lack of the expertise and specialist during the procedure leads to wrong configuration, assigning inappropriate security measures and etc. which creates some security gaps in the organisation security infrastructure. Leading the migration procedure is a challenging task that needs relevant knowledge. Many classic security strategies have been focused solely on preventing attacks, an approach that is insufficient for modern threats. The security teams, having the needed knowledge and expertise should ensure their strategy considers the current cyber risks & threats includes rapid attack detection, response and recovery mechanisms to increase resilience. This cloud security strategy considers the involvement of security specialists as one of the core factors.

Shared Responsibilities

While storing business data in cloud storage and share them with third party, then the security of those data is a shared task between client and the cloud provider.

The experience of interview participants showed that most of the time, organisation perceive that CSPs are the only responsible for managing all the tasks. Actually they think by outsourcing data storage, they transfer all the challenges and difficulties on the shoulders of service provider. However, with adopting cloud services, the shared responsibility come into play. Defining roles and responsibilities of both sides (customer and service provider) becomes more important in a cloud computing setting and should be addressed in the strategy. This is due to that multiple organisations are responsible for implementing and managing different parts so the security responsibilities should be also divided across these multiple organisations. In particular, the cloud provider is responsible for the security of the cloud infrastructure, while the customer is responsible for security of the data in the cloud. As the cloud security strategy helps to protect organization data, it's important to make it clear where the provider stops and where the client's responsibility begins. For instance, as mentioned earlier, the cloud provider is responsible for making sure customer's infrastructure built within its platform is inherently secure and reliable. While customizable cloud capabilities like application management, network configuration and encryption are the customer's responsibility.

5.1.4 Technology

Technology is explained as the last category in this strategy. After considering the factors in the previous categories and managing the initial steps, this part focus on the technology and technical aspects.
An effective cloud security strategy requires the use of right tools that make it easier to automate and streamline moving data from the existing storage system to the cloud storage in a secure way. The right security tools are necessary during the migration process. There are ways to transit data securely, such as using network security controls and encrypted network protocols and etc. So selection of the right tools and technology that improve the security of data is of significance.

Data encryption: By using of cloud storage, we are sending data to and from the cloud provider's platform and in the case of cloud storage, storing business data within third party's infrastructure. Considering the security measures, there are two significant aspects about security controls in cloud: 1) the presence of the security control and 2) the effectiveness or robustness of that control. In other words, it is not enough that a security control is present—but that control also needs to be effective. Here, about encryption as a security measure, one can describe it as a strong security measure. According to the literature review and also interview respondents (P2,P14 and P12), encryption is considered as another layer of cloud security to protect business data assets, by encoding them when at rest and in transit. But what

is the degree of trust(or assurance) that can be expected from encryption? A cloud may implement encrypted communications between the cloud and an external user — It is important to evaluate the effectiveness of this encrypted communications, to verify that the control is properly designed, implemented and verified. Some of the participants who were specialized in cloud security, mentioned encryption as the best security measure that increase the data security. Specially double/multi encryption (Double-Encryption: encryption of the already encrypted message more than one time). Because by double encryption the encrypted data is encrypted again which this increase the level of the security and makes it more complex. In fact, if the complexity of the encryption method increases, the security level would be increased as well. Considering the data sovereignty issue, proper encryption method can address this issue. Of course, selection of the enough secure encryption algorithm and method, managing the encryption keys is another important and complex task which by having the relevant knowledge in workplace can be figured out. So, business owners should ensure that their data at rest and in transit between internal and external cloud connection points is unreadable which consequently minimizes breach impact.

Identity and Access Management: Implementing a strong identity foundation which is based on the principles of least privilege and separation of duties is of important. IAM was also recommended by one of the security specialist (P13) during the interview to be considered as a main security measure for data protection. It is wise to implement a centralized identity and access management system which aim to eliminate reliance on long-term static credentials. It can be considered as a key capability to ensure data sovereignty [5], providing data owners with full control over their data and their digital identities. This requires the definition of data usage constraints: defining who is allowed to do what in which context with the data shared by the data owner.

Multi-Factor Authentication: Another security measure which was emphasized by the interview respondents is multi-factor authentication (MFA). This is a user account access protection method that combines multiple identity verification methods, such as passwords, biometrics, and authentication tokens, to provide more security than any one of these methods alone would. This security measure is considered as another important factor that this strategy emphasizes on it.

5.2 Conclusion

Currently organizations in almost all sectors rely on CSPs with more and more critical applications and data in the cloud. Due to the nature of cloud-based systems,

they are facing various security threats including the nefarious use of cloud services and the lack of cloud security architecture and strategy. Moreover, another big mistake that is most often seen during cloud (storage) implementation is transmitting too much of data to the cloud at once. Business owners are often too hasty in moving their data with different sensitivity level to the cloud, which could mean trouble if their business does not quickly adopt to the new environment. Just like adopting any new system, the transmitting team needs to understand the basics of it before they can fully operate it. Therefore, it is wise that a company before move any organisational data to cloud, it follow a cloud security strategy designed to test out the new storage security factors/methods. Data that is not business-critical is a good resource for this, as it will not be too big of a deal if that data ends up lost. By slowly testing out the security of cloud storage environment, the company will familiarize itself with the security measures of cloud and how stored data on the cloud are protected before it moves anything important. Once the security team involved in migration procedure has the hang of the storage environment, they can then shift to migrating critical data, applications and other important assets to the cloud.

Chapter 6

Discussion & Conclusions

Finally this chapter consists of four sections. First section describes the results which this study presents and then Second Section discusses those reported results. Section 3 provides the implementation of the cloud storage security strategy. In the following, Section 4 concludes the study and highlights the main findings which provide answer to the main research question. The limitation and future work of this study is also described under this section.

6.1 Results

The results of the research can be split up into two sections regarding the research question(s). First the current perception of cloud storage security risks with a focus on data sovereignty. During the first phase, a literature review was conducted which delivered preliminary background information in preparation for the expert interviews.

Comparing the results of the literature review and interview answers, both revealed almost the same security risks. According to the data collected during the literature review and interviews, the 'data sovereignty' was perceived as big challenge. Even for those respondents who first were not familiar with this term, but after that they were provided some explanations, they found 'data sovereignty' indeed a big issue. Through this study, it was also revealed that one of the biggest challenges in successful and secure cloud migration is the security of transmitted data (at rest) in cloud platform. To protect business assets - data, in transit and also at rest against potential risks and maintain the control over the data, first a baseline that ensure the data security has to be established before the migration procedure start. It is obvious that cloud environments introduce new data risks, such as data sovereignty and pose a challenge, so the security teams need to be aware of which security measure is needed to be assigned to keep the control of data owner over

the data. This is further complicated when security teams have limited knowledge about CSPs' architecture, either due to the CSPs not providing this information or due to the security teams are not aware if this information exists. Therefor, there should be a security strategy specific for cloud storage to solve all these issues. And because this study aimed to provide such a solution that can cover the mentioned risks, we developed and proposed a security strategy for cloud storage that can address the current existed challenges.
However during the last few years, some researches has been done on cloud security and privacy issue, but those researches initially were focused on known security risks. It should not be ignored that as cloud adoption became more relevant, research into cloud security strategies is also required more.

6.2 Discussion

The main goal of this study was to investigate the cloud storage security risks and challenges, impacts of data sovereignty and then based on those risks formulate a solution and then introduce it to address them. The first step in being able to reach the goal was reviewing the available literature.
Previous studies highlighted several potential challenges including data sovereignty. Those studies also confirmed the significance of having control over data as the data owner when the data is stored in cloud platforms. The results presented in chapter 4 shows an interesting picture of the current state of cloud migration and how the security factor is perceived in practice. As we have seen, currently organisations do not pay enough attention on security factor and even they do not have a strategy as baseline to manage their data migration proper secure. It is important to further investigate how to maximize the data sovereignty because it allows the organisations as data owner to have their (sensitive) data in their own control however they are hosted somewhere else outside their infrastructure. In the following of the literature review, gained insights on practical trend of migrating to cloud storage, interviewing security experts was the second step. As the result of the research conducted in this thesis, we found that currently the data sovereignty is a big challenge that organisations face it, more important that they accept it as a acceptable risk. In addition, this research also presents in general most common potential risks of cloud storage and how it is perceived by business owners and security specialists who have influence on and are involved in cloud migration. Based on the data collected from the interview and literature, current trend of the cloud adoption by organisation includes several potential risks that can be mitigated easily. The security specialists mentioned almost the same perspective regarding the cloud security. All of them

stressed the importance of data control in cloud platform and they believed that having a cloud security strategy should be considered as a basic measure on which organisations can further choose the mature security measures for protecting their data in third party infrastructure. Eventually, the main findings of this study showed that the lack of knowledge, not enough training and absence of well-defined security strategy according to organisation risk profile are big issues. Interview respondents were enthusiastic about a well-defined cloud security strategy, as all participants brought this up during the interviews and all of them indicated that pre-defined cloud security strategy was something they valued themselves. This supports the positive effects of the presence and involvement of a security strategy that helps security specialist who are involved in the migration process with ensuring the protection of business data. Because in a 'Cloud Security Strategy', extra attention is paid for the data protection and security aspect.

Finally, as mentioned above, an effort to solve the current issues with data control and security, a security strategy for cloud was formulated. Because one key thing this study discussed was the data sovereignty issue, according to this issue, one important remark on developed cloud security strategy is that it can address this challenge by some security measure such as double encryption and its special emphasise on efficient IAM. For example, when an organisation do not trust the encryption method of CSP but also use its own encryption method as a extra security layer (so-called double encryption) or manage the key management, then this organisation can maximize the data sovereignty and protection against external and internal threats such as malicious insiders.

6.2.1 Advantages of novel cloud security strategy

Some of the biggest benefits of having a cloud security strategy in place are:

- It ensures the confidentiality, integrity and availability of data.
- Competitive differentiator: It can be seen a competitive differentiator when a company is selecting cloud services (cloud storage) and CSP.
- Reduced risks: An ad-hoc cloud deployment leaves you vulnerable to the risk of disasters or downtime due to infrastructure or security issues. A cloud security strategy helps you diversify essential services over different environments. For example, you can run mission-critical apps with customer data on a private cloud while using a public cloud provider for routine, functional applications or storing archives.

- Data security: Using this cloud storage security strategy protects the entire data lifecycle – from creation to destruction. Critical data should be protected with encryption, strong passwords and multi-factor authentication.
- Regulatory compliance: Data security and privacy are top concerns for regulated industries as well as consumers. The cloud storage security strategy manages and maintains enhanced security around infrastructure to meet compliance and to protect business data.

When applied correctly, this strategy increases an organization's ability to minimize and limit the damage caused by a threat actors.

6.2.2 Disadvantage of novel cloud security strategy

- Financial cost: This strategy covers different aspects that impacts the overall organisation's security. For example this study revealed the lack of security specialist involved in the cloud migration as a big issue. To follow this strategy and involving/hiring security specialist has negative financial consequences.
- Time consuming: Security specialists spend a great deal of time preparing, researching then communicating the migration procedure status with for example Management Board, which may impede day-to-day operations and negatively impact the business. As this should be done with full attention then it would take more time and would sometimes have delay than normal - what is happening right now in organisations.
- Requires skilled human resource: Although security strategy for cloud helps reduce the security risks even in meeting long-term objectives, following this strategy itself sometime can provides opportunities for missteps. Using this strategy requires full attention, active participation and accountability of not only the security specialist but also the business owners/ final decision makers.
- Risk acceptation: Decision makers might find it too easy to accept vulnerabilities (discovered during the risk assessment) if mitigating them takes necessary resources from accomplishing a business objective.
- Limited resources: There are some other technical limitations in the term of technical security measure. For example double encryption which was mentioned one of the strongest security measures, is not easily applicable for some organisations. Organisations have their own IT-infrastructures or using managed services (offered by third-party), in both cases most of the time their standard services are not easy to connect to local security measures (encryption tools).

An important difference between this security strategy developed in this study and previous ones (mentioned in chapter 2) is that this strategy is specific for data protection and security which maximizes the data sovereignty. This can be observed through the different components which are included in this strategy with the goal of protecting the data and increase the control of the data owner over the data in cloud. For example this security strategy covers process, organisation strategy, technology and finally the human resource inside an organisation. Moreover, following this strategy, organisations should check CSPs on security and be critical of the services they purchase.

Altogether, this paper contributed in filling the research gap currently present in cloud security and the lack of well-defined strategy for security. However this new field needs more research but for current situation, it can be fully applicable in practice.

6.3 Implementation of this cloud storage security strategy

However, it is not much complex to develop a security strategy to protect the business' data but actually putting that strategy into motion is not an easy task. While merely having a strategy specified to data protection helps business owners be better prepared for the future, if that strategy is going to provide the maximum possible benefit, it needs to be implemented correctly. In this section we try to show how this security strategy can be implemented in a company.

We suppose the company-X aims to keeps its business data not anymore on-premise and wants to transfer them into cloud storage. With that in mind, the following steps clarify implementation of this security strategy in that company:

1. Data classification: An important element of an effective security strategy is the information classification. So identifying the types of available business data and classifying them into different classes is the first step. When the company knows its data then can decide which data can be sent to cloud and under which security measure and of course which CSPs are appropriate options to have in the next steps. For example: Public data, Confidential data, Internal data, Secret data and etc. which each of them needs different security measure.

2. Assemble security team and start assigning responsibilities: Sufficient human resources are of significant. In order to use this strategy properly, in this step the company-X needs also identify the available capacity (human power) to

assign the task and responsibilities. For example, is there security specialist that can follow this strategy and implement the data transmission procedure? If no, the relevant role needs to be filled with right person with the required knowledge - for example by hiring the experts.

3. Conducting a security risk assessment: According to the company-X risk profile, conducting a security assessment is of vital. Because the kind of risks can the company-X expects, which risks have high impacts and which risks are acceptable are important factors to be considered before the selection of a CSP.

4. Setting of required security goals: In this step, the security goals of the company-X should be established and verified if they are applicable.

5. Selection & evaluation of the security architecture model: This step identifies various areas that can assist in selection of the CSP. Reviewing the cloud architecture, security policies, privacy Term and Conditions, past and recent logged incidents, breaches and review performance of IAM system and other important security documentation. Then based of the outcome of that security evaluation the selection should be made. Following this, the agreement on SLA, the estimated time and cost between company-X and CSP can be finalized and then contract can be signed.

6. Data migration: Finally in this step, the data can be transmitted into the cloud storage under the agreed security measures. One of the security measures which in this step is important, is the transmission channel. It should be ensured that the (sensitive)data is transferred through a secure channel.

7. Security Awareness: The company-X needs to pay special attention on the security awareness of its employees. Because employees need to access these data stored in the cloud in their daily work activities. After the migration, employees should be trained about the proper and secure access of data and what are the risks that they need to be careful with their behaviours.

8. Evaluating your security strategy: In security filed, the periodic evaluation of the assigned security measure is very essential. This is a continues process that should be repeated minimum yearly. With the emergence of new cyber attacks and threats, new security measure are required.

6.4 Conclusions

The rise in cloud computing utilities has brought increased need for better data security. By their very nature, competitive cloud services (including cloud storage) are faced with the need to provide cost-effective services and features sets that enable ease of adoption. But equally important is the need for a appropriate cloud security strategy to be in place, to manage the data migration and protect the business data hosted in cloud. As data security and control of data is a big challenge, with this in mind, this study attempted to address this issue through the following main research question :

RQ: How can we design a secure cloud storage strategy to maximize the data sovereignty?

In order to provide an appropriate answer to this main research question, first the following preliminary questions were formulated and answered in Chapter 2 to give some more background information about this topic:

- What is cloud computing?
- What is data sovereignty?
- What are the different cloud storage strategies that are discussed in literature? and do they facilitate data sovereignty
- What is the data and how data classifications influences the security controls needed to preserve the confidentiality of data in cloud?

All above mentioned preliminary questions were answered in the first phase of the study. During the first phase, we started by reviewing existing work in this area by a Systematic Literature Review (SLR), conducted on Scopus about the cloud storage risks - in particular data sovereignty impacts. The answers to these questions are presented in the second Chapter of this paper which includes an introduction to cloud, followed by a detailed description of cloud different models and services, data sovereignty as a potential challenge and a summary of the available cloud strategies. It is obvious that cloud services are vital for organisation's development and help them the most in reaching their goals, but they also threaten the security of the business data which are stored or processed in those platforms. Here, the literature review highlighted the potential risks of storing data in third party platform, namely in cloud storage. According to the literature review, one of the main challenges that organisations currently face, is the lack of enough control over their data. As soon as data are placed in cloud platform, the CSPs has also control over an organisation's data, although this is also a potential risk. As the focus of this study was 'data sovereignty', this was explained with its impacts. In order to solve issues like the

data control in cloud platform, we could not find an available well-defined strategy to be followed which fully cover the security aspect of the data regarding cloud storage.

Following the first phase, the second phase of this study included interview to gather facts, opinions, perceptions and practices of security experts. The interview with experts presented valuable information on practical method of migrating and storing data in cloud. After analysing the interview answers, based on the output of the literature review and interview answers, we could design a cloud security strategy and described in this paper as an example of security strategy to guide security specialist to manage the cloud migration in a secure way with a focus on maximizing data sovereignty. Moreover, it is formulated in a way that based on this strategy, other organisation can also formulate their security strategy according to their organisation's goals and needs. Because having an efficient security strategy for cloud storage helps organisations to maximize their control over the data in cloud environment, this security strategy is designed such that covers different aspects of an organisation from organisational design/culture to human resource and technology. In fact, it presents the fundamental factors to be considered during migration of data to clouds that impacts data sovereignty. It starts with data classification and then according to the value of data, the evaluation and selection of a proper cloud provider is formulated as a structured process that this strategy aimed and consequently leads to increase the data control.

Finally, this proposed cloud storage security strategy tries to address not only data sovereignty, but also all those issues highlighted in literature and discussed during the interviews.

6.4.1 Limitation & Future Work

A big limitation encountered in this research was the lack of enough available resource (available (online) scientific researches). As this is a new topic, there has been done very few research. If we could have more information about the impact of this issue (data sovereignty) then we could collect now, we would increase the efficiency of this solution more.

Furthermore, finding the experts with the knowledge and experience in this field and of course those who were interested to attend the research interview was another challenge for us during this project. After finding the needed number of participants, due to the workload of the end of year, the time needed to conduct all interviews was much more than it was expected and estimated. We had contacted much more number of the experts who were specialized in cloud security but unfortunately due to high workload (end of year) they had and also their priorities they

had no time for conducting this interview. If we could have their opinions about the security of data in cloud, we could also consider their recommendations and empower our security strategy.

Lastly, there was no well-defined cloud security strategy to be able to compare with this novel security strategy. It would have been better to compare with an other strategy that is specified for cloud security, but finding that strategy for cloud security within the span of the research proved difficult.

Overall, the research went well. The thesis' core work lied in discussing the cloud storage risks with focus on data sovereignty and a solution to address those risks. There are many possibilities for future research in this field. The common next step is to compare this developed cloud security strategy with a well-defined strategy for cloud security. The current developed security strategy was based the potential risks highlighted in literature and experts interview. This can be further used as baseline and include any other security measure to address more security challenges as well.

Bibliography

[1] H. M.-E. Hussain. M-R, " Securing Cloud Data using RSA Algorithm , https://www.researchgate.net/figure/Cloud-computing-service-delivery-and-deployment-model_fig1_329796973," accessed: 2022-06-01.

[2] A. in Cloud Computing, " An Introduction to Cloud Service Models , https://geekflare.com/cloud-service-models/," accessed: 2021-10-09.

[3] D. Utomo, Suzanna, and M. Wijaya, "Tailoring togaf architectural development method to cloud adoption strategy," *5th International Conference on Information Management and Technology*, pp. 159 – 164, 2020.

[4] A. Khajeh-Hosseini, D. Greenwood, J. Smith, and I. Sommerville, "The cloud adoption toolkit: Supporting cloud adoption decisions in the enterprise," *Software Practice and Experience*, 2012.

[5] CIO-Wiki, "Buiness Model for Information Security (BMIS) , https://cio-wiki.org/wiki/File:BMIS.jpg," accessed: 2022-02-28.

[6] T. Luxner, "Cloud computing trends: 2021 state of the cloud report, https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/,."

[7] M. Mosch, H. Schweizer, S. Gross, and A. Schill, "Automated federation of distributed resources into user-controlled cloud environments," *IEEE/ACM 5th International Conference on Utility and Cloud Computing*, no. 64249672012, pp. 321 – 326, Nov. 2012.

[8] N. Kushwaha, P. Roguski, and B. W. Watson, "Up in the air: Ensuring government data sovereignty in the cloud," *12th International Conference on Cyber Conflict,CYCON*, no. 9131718, pp. 43 – 61, May 2020.

[9] N. Kushwaha and B. W. Watson, "Crown in the clouds: A canadian data sovereignty crisis," *15th International Conference on Cyber Warfare and Security, ICCWS*, pp. 286 – 295, 2020.

[10] N. Vurukonda and B. T. Rao, “A study on data storage security issues in cloud computing,” *2nd International Conference on Intelligent Computing, Communication Convergence*, vol. 92, pp. 128–135, Feb. 2016.

[11] S. Khan and K. Hamlen, “Anonymouscloud: A data ownership privacy provider framework in cloud computing,” *11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 170 – 176, 2012.

[12] N. Kaaniche and M. Laurent, “Data security and privacy preservation in cloud storage environments based on cryptographic mechanism computers,” *Computer Communications*, pp. 120 – 141, Oct. 2017.

[13] S. Ullah and D. e. F. D. Zuefeng, “Ultimate control and security over data localization in the cloud,” *International Journal of Security and its Applications*, pp. 15 – 26, 2013.

[14] S. Trabelsi and J. Sendor, “Sticky policies for data control in the cloud,” *10th Annual International Conference on Privacy, Security and Trust*, pp. 75 – 80, 2012.

[15] F. Kandah and A. Powell, “Ultimate control and security over data localization in the cloud,” *International Conference on Computing, Networking and Communications*, pp. 123 – 127, Feb. 2015.

[16] R. El-Gazzar, E. Hustad, and D. Olsen, “Understanding cloud computing adoption issues: A delphi study approach,” *Journal of Sysytem and Software*, pp. 64 – 84, 2016.

[17] N. Anggraini, Binariswanto, and N. Legowo, “Cloud computing adoption strategic planning using rocca and togaf 9.2: A study in government agency,” *5th Information Systems International Conference*, pp. 1316 – 1324, 2016.

[18] M. Al-Ruithe, E. Benkhlife, Y. Jaraweh, and C. Ghedira, “Addressing data governance in cloud storage: Survey, techniques and trends,” *Journal of Internet Technology*, pp. 1763 – 1775, 2018.

[19] A. De Paula and C. G. De Figueiredo, “Cloud computing adoption, cost-benefit relationship and strategies for selecting providers: A systematic review,” *11th International Conference on Evaluation of Novel Software Approaches to Software Engineering*, pp. 27 – 39, 2016.

[20] N. Kyriakou and E. N. Loukis, “Do strategy, processes, personnel and technology affect firm’s propensity to adopt cloud computing?: An empirical inves-

tigation," *Journal of Enterprise Information Management*, pp. 517 – 534, May 2019.

[21] C. Guo, Y. Li, and Z. Wu, "Sla-do: A sla-based data distribution strategy on multiple cloud storage systems," *22nd IEEE International Conference on Parallel and Distributed Systems*, pp. 602 – 609, Dec. 2016.

[22] R. El-Gazzar and F. Wahid, "Strategies for cloud computing adoption: Insights from the norwegian public sector," *12th European, Mediterranean and Middle Eastern Conference on Information Systems*, 2015.

[23] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, "Multilevel classification of security concerns in cloud computing," *Applied Computing and Informatics*, pp. 57 – 65, Jan. 2017.

[24] S. Shukla, S. Yadav, and B. Bohra, "Security challenges in cloud," *1st International Conference on Green Computing and Internet of Things*, pp. 1448 – 1451, Jan. 2016.

[25] N. F. Eozia, E. Ariwa, D. C. Asogwa, O. Awonusi, and S. O. Anigbogu, "A review of threats and vulnerabilities to cloud computing existence," *7th International Conference on Innovative Computing Technology*, pp. 197 – 204, Aug. 2017.

[26] B. Hari Karishna, S. Kiran, G. Murali, and R. Pradeep Kumar Reddy, "Security issues in service model of cloud computing environment," *4th International Conference on Recent Trends in Computer Science and Engineering*, pp. 246 – 251, Apr. 2016.

[27] J. Grover, Shikha, and M. SHarma, "Cloud computing and its security issues - a review," *5th International Conference on Computing Communication and Networking Technologies*, pp. 246 – 251, 2014.

[28] NIST-Orgnisation, "Final version of nist cloud computing definition published, https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published,."

[29] L. Nishad, R. Pandey, Akriti, S. Beniwal, J. Paliwal, and S. Kumar, "Security, privacy issues and challenges in cloud computing: A survey," *2nd International Conference on Information and Communication Technology for Competitive Strategies*, 2017.

[30] A. Gajbhiya and K. Shrivasta, "Cloud computing: Need, enabling technology, architecture, advantages and challenges," *5th International Conference*

on Confluence 2014 - The Next Generation Information Technology Summit, pp. 1–7, 2014.

[31] P. Modisane and O. Jokonya, "Evaluating the benefits of cloud computing in small, medium and micro-sized enterprises (smmes)," *2020 International Conference on ENTERprise Information Systems - International Conference on Project MANagement and International Conference on Health and Social Care Information Systems and Technologies*, pp. 784 – 792, Oct. 2020.

[32] J. Gibson, D. Eveleigh, R. Rondeau, and Q. Tan, "Benefits and challenges of three cloud computing service models," *2012 4th International Conference on Computational Aspects of Social Network*, pp. 198 – 205, Nov. 2012.

[33] S. Kachele, C. Spann, F. Hauck, and J. Domaschka, "Beyond iaas and paas: An extended cloud taxonomy for computation, storage and networking," *6th International Conference on Utility and Cloud Computing*, pp. 75 – 82, Dec. 2013.

[34] A. Albugmi, M. Alassafi, and R. Walters, "Data security in cloud computing," *5th International Conference on Future Generation Communication Technologie*, pp. 55 – 59, 2016.

[35] T. Galibus, V. V. Krasnoproshin, R. de Oliveira Albuquerque, and E. Pignaton, *Elements of Cloud Storage Security: Concepts, Designs and Optimized Practices*. Springer Link, 2016.

[36] S. M. Shariati, Abouzarjomehri, and M. H. Ahmadzadegan, "Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection," *2nd International Conference on Knowledge-Based Engineering and Innovation*, pp. 1078 – 1082, 2016.

[37] C. Silva, J. Silva, R. Rodrigues, G. Campos, L. Nascimento, and V. Garcia, "Security threats in cloud computing models: Domains and proposals," *IEEE 6th International Conference on Cloud Computing, CLOUD 2013*, pp. 383 – 389, 2013.

[38] M. Baezner and P. Robin, "Trend analysis: Cyber sovereignty and data sovereignty," May 2018.

[39] Z. Peterson, M. Gondree, and R. Beverly, "A position paper on data sovereignty: The importance of geolocating data in the cloud," *3rd USENIX Workshop on Hot Topics in Cloud Computing*, 2011.

[40] K. Singi, S. G. Choudhury, V. Kaulgud, R. J. C. Bose, S. Podder, and A. P. Burden, “Data sovereignty governance framework,” pp. 303 – 306, 2018.

[41] C. Esposito, A. Castiglione, and K.-K. R. Choo, “Encryption-based solution for data sovereignty in federated clouds,” *Trade Journal*, vol. 3, pp. 12–17, Feb. 2016.

[42] V. Paul and R. Mathew, *Data Storage Security Issues in Cloud Computing*. Springer Link, 2020.

[43] M. J. Morton, “Data Sovereignty: The Challenge of the Data Decade, https://www.delltechnologies.com/en-us/perspectives/data-sovereignty-the-challenge-of-the-data-decade/,” accessed: 2021-07-15.

[44] S. Khalil, “Adopting the cloud: how it affects firm strategy,” *Journal of Business STrategy*, pp. 28 – 35, 2019.

[45] N. Ahmad, Q. N. Naveed, and N. Hoda, “Strategy and procedures for migration to the cloud computing,” *5th IEEE International Conference on Engineering Technologies and Applied Sciences*, Nov. 2018.

[46] S. Orban, “6 Strategies for Migrating Applications to the Cloud, https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/,” accessed: 2021-08-11.

[47] S. Zardari and R. Bahsoon, “Cloud adoption: A goal-oriented requirements engineering approach,” *Proceedings - International Conference on Software Engineering*, Jan. 2011.

[48] AWS, “Data Classification - Secure Cloud Adoption, https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification-overview.html,” accessed: 2021-12-10.

[49] B. Kitchenham, “Procedures for performing systematic reviews,” *Keele, UK, Keele Univ.*, vol. 33, 08 2004.

[50] W. Adams, “Conducting semi-structured interviews,” 08 2015.

[51] T. Hayat Khan, “Step by step approach for qualitative data analysis,” *INTERNATIONAL JOURNAL OF BUILT ENVIRONMENT AND SUSTAINABILITY*, 2018.

[52] H. Hamidovice, “Bmis—an introduction to the system environment,” *Journal of Business Strategy*, Aug. 2011.

[53] Microsoft, “ Embrace proactive security with Zero-Trust , https://www.microsoft.com/en-gb/security/business/zero-trust,” accessed: 2022-04-16.

[54] N. Cranenburgh, “ Establishing the Context , https://rebok.engineersaustralia.org.au/wiki.html/establishing-the-context-r45/,” accessed: 2022-02-06.

[55] G. Security, “ Cloud Security Architecture , https://www.guidepointsecurity.com/education-center/cloud-security-architecture/,” accessed: 2022-02-09.

Appendix A

Interviews

A.1 Interview guideline: English

A.1.1 Introduction

1. What is your name and your position?
2. What did you study (study background)?
3. In which sector is this organisation active?
4. Could you please describe your company activities?
5. How long have you been working in this role?
6. Could you please describe your current job?

   Main questions
   Part I: General personal perspective about cloud storage security

7. Do you also use cloud for your personal usage? What kind of cloud service?
8. Could you please describe your opinion about the security of cloud storage service ?
9. What are your (specific) biggest cloud security concerns in cloud storage?
10. Are you familiar with ‘data-sovereignty’?
11. How do you define your important factors when adopting a cloud service?
12. Compared to traditional, on-premise IT environments, is the security of the data lower of higher or the same in the cloud storage?
13. How do you define your important factors when adopting a cloud service?

14. Do you trust the current CSPs in the market? Why yes/not?
15. Which cloud provider do you prefer to use for personal information now? Google / Microsoft / Amazon or..? Why?

Part II: General organisation's perspective about cloud storage security

16. Have you ever involved or experienced cloud migration?
17. Which cloud migration strategy (own strategy or offered by CSP) did/do your company follow during your cloud migration?
18. What types of corporate information do your company stores in the cloud?
19. Who makes the final decision regarding cloud migration?
20. What is the role and influence of security specialists in cloud migration (before migration, during and after)?
21. Did your organization experience a cloud related security incident in the last 12 months?

    If yes, what type of incident was it?
22. How confident are you in your organization's cloud security posture? Why?
23. How do your company protect the data and control the security of its data in the cloud?
24. What criteria do you consider most important when evaluating a cloud security solution?
25. What are the main barriers for your company to migrate to cloud-based security solutions?
26. Which security controls would most increase your confidence in adopting cloud storage?
27. Have you ever heard about GAIA-X?
28. Do you think your organisation is willing to move to GAIA-X?

End questions

29. Your suggestion/advice for improving the security of data in the cloud?
30. Is there something you would like to add? Maybe something I have not asked? A question, something you like to contribute?

Appendix B

Interview invitation information & Consent Form

B.1 Interview invitation information

Invitation to participate in an interview-based research study relating to governance of cloud storage.

You are being invited to participate in an interview-based research study led by Toofan Shafee, master student at University of Twente.

The study is about the governance of cloud computing and storing information in a secure way in cloud environments. In general, I am seeking your comments and perspectives on the security of cloud services - in particular cloud storage. One of the significant goals of this research is to find out how companies make decisions about cloud adoption, based on which criteria the choice is being made about a cloud provider and then according to the result of this survey, a secure strategy will be designed. Another important aim of conducting this research is to increase my understanding of ''cloud security, knowing how cloud security is perceived and experienced by both those in the field (cyber security specialists) and other decision makers in (Dutch) organisations" for the partial fulfillment of the Master of Computer Sciences – Cyber Security specialization degree. Therefore, I would like to extend an invitation to you to participate in this research as you are in an ideal position to give me valuable first hand information from your own perspective.

The interview will last approximately 60 minutes and it will be conducted online.

Please note that your responses, identifying information, and other names mentioned would be kept confidential and anonymous from the transcripts that will be made of the interview. Only the major lines of thought that emerge from the interviews will be used to describe important ideas that come out of the interviews.

Contact information:

Email Address: toofanshafee@student.utwente.nl

Title of research:	Governance of cloud storage
Superision of study:	This study is conducted as part of a master thesis supervised by the Twente University in Enschede, Netherlands.
Name of the researcher:	Toofan Shafee
Porpose of the study:	Investigation of cloud storage security from the cyber security specialists perspective, then analyse and address them through possible solutions.

B.2 Interview consent form

Please read the following information carefully. Feel free to ask question at any time if something is unclear.

Thank you very much in advance for taking the time. The interview will be taking a maximum of 60 minutes.

This consent form is necessary to ensure you that you understand the propose of the study and the condition of you participation, Therefore please read the following information with upmost care.

Please state your understanding and notice by checking the boxes in front of the corresponding information. Please sign this document subsequently to grant your approval.

- I understand that I am voluntarily participating in this research project. am aware that I can ask questions at any time and they will be answered during the process and in the future.
- I understand that I am able to withdraw my participation at any time without stating any reason.
- I agree that the interview will be recorded and a transcript will be produced.
- I am aware that the transcript of the interview will be analysed by the researcher Toofan Shafee.
- I agree that the transcript will be send to me to give me the opportunity to correct any factual error. And that I will state my email address for solely that propose.

- I am aware that this consent form will be kept separately to my responds so that no connection could be made to my identity.