JÖNKÖPING UNIVERSITY
School of Engineering

Vendor lock-in and its impact on cloud computing migration

Main Subject area: *Informatics*
Author: *Tesfaldet Weldemicheal*
Supervisor: Sonny Johansson
JÖNKÖPING 2023-07

This final thesis has been carried out at the School of Engineering at Jönköping University on vendor lock-in and its impact on cloud computing migration: a business point of view in Swedish companies. The author is responsible for the presented opinions, conclusions, and results.

Examiner:	Anders Adlemo
Supervisor:	Sonny Johansson
Scope:	15 hp (first-cycle education)
Date:	2023-07-24

Abstract

The concept cloud computing describes a business model in which multiple service providers pool their resources to serve customers online. The ability to pool and assign resources as needed, to deliver services based on accurate usage metrics, to rapidly scale up or down, to deliver services on demand, and to give customers access from any location are just a few of the many benefits of cloud computing. Many organizations and people are interested in cloud computing, but they are also apprehensive of it because of concerns about data security, data availability, and other issues.

In this thesis, the topic of vendor lock-in in cloud computing is investigated, as is the role that proprietary technology, contract terms, and network effects play in maintaining this issue in Swedish organizations. The research investigates the various ways in which these characteristics restrict businesses' ability to be flexible and independent by creating barriers that prevent them from switching cloud providers. The thesis addresses these concerns by presenting three potential solutions to the problem of vendor lock-in. These solutions include the utilization of open-source technology, the implementation of a multi-cloud, and an exit strategy. This thesis intends to assist organizations in controlling the risks that relate to cloud computing and vendor lock-in by giving guidance on the subject and providing solutions to the issues that have been identified.

keywords: *cloud computing, contract terms, network effects, proprietary technologies, vendor lock-in.*

Table of content

1 Introduction

The lower cost of deploying and maintaining applications and components is a central feature of the cloud computing system (Satzger, o.a., 2013). The use of cloud computing can improve teamwork and data sharing, as well as lower investment costs, maintain business continuity, and speed up elasticity. In recent years, the cloud computing model has gained significant acceptance (AlTwaijiry, 2021). The success of this business model is partly down to the fact that clients can take advantage of its services whenever they want, at their own pace, and pay as they go. With its low prices and high adaptability, the cloud is an attractive migration option. Despite its clear benefits, many businesses are hesitant to move to the cloud for fear of losing control of their data, being locked into a proprietary system, or facing legal complication (Alshammari, et al., 2017).

The technology of the cloud makes it possible for businesses to very quickly increase or decrease the size of their computer resources (Arce, 2022). This idea is drawing the interest of both public and private businesses, as well as small to medium-sized organizations, which view the cloud computing model as an advantageous business strategy to maintain their position in the market and fulfill the requirements of their companies. On the other hand, small and medium-sized businesses are improving their capacity to meet demands for computing resources while avoiding the consequential investment in over-provisioned infrastructure, maintenance, and other related areas (Arce, 2022).

According to AlTwaijiry (2021), cloud computing is still in its development and, as a result, suffers from a lack of standardization. In practice, what ends up occurring is that most new and existing cloud providers each propose their very own solution in addition to their own proprietary interfaces for users to use to gain access to the resources and services they offer. This variability presents a significant challenge since it places roadblocks in the way of the widespread adoption of cloud computing. The lock-in of vendors is the most significant obstacle, as it cannot be avoided at this moment (Harauzek, 2022).

Cloud computing provides a proactive business plan for companies of all sizes to help them stay competitive and fulfill their own unique needs (Finta, 2022). Even though this appears to be a lucrative opportunity for both public and private businesses, several obstacles have not yet been satisfactorily addressed. Security and vendor lock-in were identified as major roadblocks to cloud adoption in the UK market (Opara-Martins et al. 2016). As a major barrier to enterprise cloud adoption, vendor lock-in has been identified by European organizations including the European Union Agency for Cybersecurity (ENISA), and the European Commission (EC) (Noble & Mitchell, 2016).

1.1 Problem statement

As explained in the introduction, cloud computing improves collaboration, data sharing, investment costs, business continuity, fast elasticity, and access (Arce, 2022). Numerous businesses are adopting cloud computing due to its benefits (Alkhalil et al. 2017). Despite the many benefits, sharing data responsibility and relying on service providers' tools, and protocols are still challenges (Arce, 2022).

Many businesses are being encouraged to move their operations to the cloud because of all the benefits associated with doing so; nevertheless, to ensure that they are making the most appropriate choice, these businesses must be aware of the potential hazards involved (Finta, 2022). Additionally, the process of evaluating vendors to select them is an essential component for successful cloud migration that significantly reduces the chance of being locked in (Opara-Martins et al. 2016). If a company is not happy with the services, quality, or security offered by its cloud provider, has a desire to reduce costs, or for any other reason, they could elect to switch service providers (Alkhalil et al. 2017). However, changing cloud service providers can be a complicated process that requires cautious planning and execution. The business must ensure that their data is backed up and migrated to the new provider without data loss or service interruptions. Additionally, they would have to ensure that their applications and systems are compatible with the infrastructure of the new provider and that the new provider satisfies their security and compliance requirements. Before transferring cloud providers, the business should evaluate their options thoroughly, compare costs and features, and negotiate service level agreements (SLAs) with the new provider to ensure that their needs are met.

The transition from one service provider to another may be challenging or expensive for the company; in addition to these potential drawbacks, there is also the possibility that the business will lose data or be unable to migrate it (Opara-Martins et al. 2016). That kind of dilemma, often known as a vendor lock-in, happens during the process of switching from one vendor to another, which the company runs the risk of getting itself into.

Vendor lock-in is a common concern among businesses considering cloud migration, as it can limit their flexibility and ability to switch to another cloud provider in the future. When a company becomes reliant on the services or technologies of a single vendor, switching to a different vendor becomes difficult or expensive (Harauzek, 2022).

Vendor lock-in can have a significant impact on the ability to switch to a different cloud provider from a business standpoint (Harauzek, 2022). Swedish businesses that have heavily invested in a specific vendor's services or technologies may find switching to a different provider difficult or costly, as they may need to re-architect their systems or retrain their staff. Also, service level agreements or pricing structures can make it hard

for businesses to negotiate better terms with another provider (Øverby & Audestad, 2021).

Moving to a new cloud provider comes with the possibility of considerable expenses and difficulties (Finta, 2022). To make use of the services and technologies offered by a new provider, businesses may need to re-architect their existing systems and applications as well as invest in new hardware and software. As an added complication, firms may need to migrate substantial volumes of data, which can take considerable time and resources (Øverby & Audestad, 2021). A company can lessen the effects of vendor lock-in by taking measures to guarantee it will always have full access to its data and applications and will not be tied to any one vendor's pricing model (Finta, 2022). Moreover, organizations can take measures to prepare themselves for a potential switch to a different cloud service provider. Multiple factors, including proprietary technology, network effects, and contractual obligations, can lead to a cloud service provider's monopolization in each market (Opara-Martins et al. 2016)

When it comes to cloud computing, one of the primary ways that vendor lock-in can take place is using proprietary technology (Opara-Martins et al. 2016). Customers may have a tough time switching to a different cloud provider due to proprietary application programming interface (API), data formats, which may not be compatible with the services and technology offered by other cloud providers. Customers may find it more difficult to move their data and applications, which may result in an increase in the expenses associated with switching to a different provider (Opara-Martins et al. 2016). Additionally, because of proprietary nature of the technology used, clients may find it difficult to change their data or service to other vendors.

According to Øverby & Audestad (2021), customers and vendors can become entangled in a self-reinforcing cycle because of network effects. When a service or product is used by more people, the value of that service or product increases. Network effects can occur in cloud computing when customers and vendors become increasingly dependent on one another, making switching to a different provider difficult for either side. For example, a customer may have built many apps on a specific cloud provider's platform, which is new to the market or has few customers, making switching difficult without incurring significant costs or losing functionality. According to Øverby & Audestad (2021), cloud service providers with larger networks of customers are often able to offer better service quality and more competitive pricing. This creates a barrier to entry for smaller cloud service providers, as it can be difficult for them to attract enough customers to compete effectively. As a result, the provider creates a deficiency for the customer, which is a barrier to switching to the other vendor.

The terms of a contract might also play a part in locking in a vendor. Long-term obligations or penalties for early termination are examples of the kinds of clauses that could be present in the contracts offered by some cloud service providers (Ahronovitz, 2015). These clauses make it more difficult to switch to another cloud service provider

(Opara-Martins et al. 2016). Furthermore, some service providers may restrict their customers' ability to use the provider's services or technologies with other vendors by including restrictions in their contracts that prohibit such usage. This restricts the customers' flexibility and ability to switch service providers (Arce, 2022).

Before committing to the services of a cloud provider, businesses should perform a careful analysis of the proprietary technology, network effects, and contract terms associated with that provider to reduce the likelihood of being locked into a single vendor (Opara-Martins et al. 2016). This can include determining whether a provider's services and technologies are compatible with those offered by other providers, as well as determining whether the contractual terms are flexible. In addition, companies ought to give some thought to the implementation of multi-cloud strategies, which can increase their adaptability and their capacity to switch to a different provider if this becomes necessary (Opara-Martins et al. 2016).

According to Øverby & Audestad (2021), network effects, contract terms, and proprietary technology are still important in creating vendor lock-in and can make it hard for a company to switch to a different vendor. The study also noted that network effects can create a strong incentive for customers to stay with their current provider, even if they are dissatisfied with the service. According to a study by Beslic, o.a. (2013), proprietary technology factors are among the most critical contributors to vendor lock-in in cloud computing. This study found that proprietary technology is a critical factor in vendor lock-in in cloud computing. According to the study by Opara-Martins et al. (2017), contract terms are among the top factors that make it difficult for customers to switch cloud providers. Therefore, more studies are required to understand the issue. Because, as was stated earlier, these three characteristics are among the most crucial factors that contribute to vendor lock-in in cloud computing, and the researcher believes that the scope of the study should not be too broad and that boundaries should be made to keep the study area narrow, the researcher wants to do research on just these three.

Previous studies have shown that cloud service providers who offer clear and transparent contract terms are often more successful than those who do not and with larger networks of customers are often able to offer better service quality and more competitive pricing. By understanding these concepts and their consequences, clients can reduce the danger of vendor lock-in. However, no previous research on cloud computing vendor lock-in in Sweden has examined the role of proprietary technology, network effects, and contract terms and how Swedish organizations handled proprietary technology, network effects, and contract terms. Because of this, more research is needed to learn more about the problem.

1.2 Purpose and research questions

The aim of the thesis is to investigate the potential issues of proprietary technology, network effects, and contract terms on cloud computing vendor lock-in in Swedish

organizations and how they have handled these issues. To achieve the purpose of the thesis, the author will answer two questions. The questions aim to find out how Swedish companies have dealt with those problems.

- *What role do proprietary technology, network effects, and contract terms play in cloud computing vendor lock-in in Swedish organizations?*
- *How have Swedish companies handled proprietary technology, network effects, and contract terms toward vendor lock-in in cloud computing?*

Answering these questions aims to help explain the potential issues of vendor lock-in in cloud computing and helps to reduce risk. Understanding how proprietary technology, network effects, and contract terms affect vendor lock-in, firms can make more informed choices regarding which vendors to collaborate with, how to leverage network effects to their advantage, and how to negotiate more favorable contracts. This can assist them in increasing flexibility or avoiding vendor lock-in.

1.3 Scope and limitations

The purpose of this study is to investigate how Swedish organizations deal with vendor lock-in. This study only focuses on the proprietary technology, network effects, and contract terms in cloud computing. One limitation is that the study does not examine federation, which is the process by which multiple cloud service providers work together to develop a solution for an organization. That makes enterprises exposed to cloud service provider transition (Kamel & Ashraf, 2015). Another limitation is the sample size. To be sure, more research is needed to produce more accurate or contradictory findings. Another limitation of this paper may be the number of participants. The more studies we conduct with larger groups of employees, the less likely there will be bias in our findings.

1.4 Disposition

This chapter is followed by the "Method and Implementation". The method and implementation section describe how the data was collected and analyzed and discusses the credibility of the study. The Literature Review section provides a deeper understanding of vendor lock-in and the problem areas that are associated with it. The Results part presents and analyzes the collected data, while the Discussion section offers a comprehensive analysis of the results. The findings of the study and the consequences of those findings are summed up in the final part, which is titled "Conclusion."

The conclusion of the study summarizes the findings and provides implications for further research and practice. Additionally, the research considers any ethical

considerations that may have been raised in the study. Finally, the conclusion provides recommendations for future research and action.

2 Method and implementation

This chapter details the approach taken in deciding how to conduct the research, gathering relevant data, and analyzing those findings.

2.1 Data collection

The vendor lock-in in cloud computing data used in this study was collected via semi-structured interviews as the primary research method (Säfsten & Gustavsson, 2020; DeJonckheere & Vaughn, 2019). This is because a semi-structured interview is a combination of an unstructured interview, in which respondents are given free rein to elaborate on their responses, and a structured interview, in which respondents are asked to choose from a list of specified themes that yield yes or no replies. The responders would have room to elaborate, but the focus would remain on the topic with the preset questions, making semi-structured the preferred method.

The data for this study was gathered using a qualitative approach. Qualitative research is a strategy that facilitates the collection of non-numerical data through open-ended procedures that provide a deep understanding of the issue (Jamshed, 2014). Qualitative research is a type of study that helps create knowledge about the issue at hand and provides insight into it. This study's qualitative approach enabled the author to investigate the potential issues of proprietary technology, network effects, and contract terms in relation to cloud computing vendor lock-in in Swedish organizations.

Individual information was gathered through qualitative participant interviews, and the people who are interviewed choose whether to participate (Alsaawi, 2014). This is because the qualitative study describes and comprehends the attitudes that participants have towards the issue. During the time that the data are being collected, the study may incorporate new questions. In qualitative research, the method of data gathering that is used the most frequently is the qualitative interviews. The author is able to gain a more profound understanding of the topic using open-ended questions, which provide respondents with the opportunity to elaborate on their opinions (Alsaawi, 2014).

Individual or group interviews might take place throughout the same period, depending on how many people are being questioned. Purposive sampling was used to select certain individuals for interviews with the purpose of achieving this goal (Rai & Thapa, 2015). Methods of purposive sampling include selecting potential participants based on their circumstances, which in this context are required levels of expertise and experience (Etikan et al. 2016). Because the participants were required to have past work experience with or an understanding of cloud computing to supply the data that could be beneficial for answering the research questions, this technique was chosen. Consequently, the research questions are answered more effectively (Rai & Thapa, 2015). The semi-structured interviews are recorded (audio), and the responses are transcribed to collect information. The author intends to conduct interviews with employees from IT organizations to investigate their perceptions of the problem. The

identities of the employees who were questioned were kept secret so that this study would not reveal personal flaws or the security of the company. The age and gender of the participants were not considered relevant because they had no effect on the quality of the data. Participants could ask questions and have the option to skip a question if they didn't know the answer or didn't want to express their opinion on the topic for any other reason. Interviews were conducted via Zoom and Teams, and the conversations were recorded for further data analysis. The author allowed the participants to read the transcripts. There were a total of six participants. The average length of the interviews was 45 minutes. In addition, the participants' work titles and areas of expertise are mentioned.

2.1.1 Interview Selection

Etikan et al. (2016) and DeJonckheere & Vaughn (2019), emphasize the significance of having appropriate respondents to accomplish the goals of a study. In addition, they claim that the most reliable respondents are those who can be reached, who are open to being interviewed, and who are familiar with the issue that is the subject of the interview and have experience with it.

According to DeJonckheere & Vaughn (2019), purposive sampling, a type of non-probability sampling, involves the deliberate selection of a sample by the researcher according to specific criteria or objectives. Rather than relying on random selection, this technique allows the researcher to carefully choose individuals or cases that align with the intended purpose of the study. This type of sampling is commonly used in qualitative research when the aim is to select individuals who possess knowledge, skills, or experiences relevant to the research question.

In the context of the statement the paper provided, the researchers used purposive sampling to select respondents who have knowledge and experience of the subject under investigation (Etikan et al. 2016). This means that the researchers deliberately chose individuals who had specific expertise or insights that were relevant to the research question. By doing so, the researchers gather rich, detailed data that would be useful for answering the research questions. Considering this context, respondents were chosen based on the fulfillment of the criteria below.

- Work at or for a company and have experience about vendor lock-in and the problem areas that are associated with it.

Table 1. The participants background.

Participant	Interviewer position	Sector
P1	System manager	Private
P2	Cloud consultant	Private
P3	Cloud consultant	Private
P4	IT-consultant	Private
P5	Cloud engineer	Private
P6	Network engineer	Private

2.1.2 Interview Guides

According to Säfsten & Gustavsson (2020), semi-structured interviews include a brief list of guiding questions and follow-up questions based on the respondent's replies. This study's interview guide included static questions and follow-up questions that varied depending on the respondents' replies. It also allowed for unplanned follow-up questions if it is interesting in the subject. The author would like to start by thanking the respondents for their willingness to participate in the research that the author is conducting. Thank them for their time and valuable insights. Describe the purpose of this research, ask permission to record, and tell the participant their answers are kept private and anonymous as explained in the data collection form. The interview guide includes the questions in Appendix 1. The interview begins with an introduction and ends with a conclusion, see in Appendix 1.

2.1.3 Pilot interview

According to Kim (2011), a pilot interview is a small-scale test of a method done before the main interview to make sure that the methods or ideas will work in real life. A pilot interview is chosen so that the interview guide and the plethora of topics that were to be used in the interviews can be put to the test.

According to Kim (2011) conducting a pilot interview is an essential step in any research project. A pilot interview provides the researcher with the opportunity to test the research tools and methods, such as interview questions and the recruitment process. It also helps the researcher to identify any issues or barriers related to recruiting potential participants and using oneself as a researcher in a culturally appropriate way. By conducting a pilot interview, the interviewers are better able to maintain an open mind to the experiences of the participants and change the interview questions properly. This helps to ensure that the inquiry remains focused on the participants' lived

experiences and their unique perspectives (Kim, 2011). Pilot interview is chosen to increase understanding of how the guide operates, with the assistance of the initial interviews. Appropriate improvements may be made to the questions that are being asked to ensure that the inquiry remains focused on the participants' lived experiences and their unique perspectives, to identify potential issues and barriers, and to adapt interview questions and deep listening, reflection, and an open mind to the participants' experiences.

The pilot interview was carried out with one of the participants who were part of the research project. The author comes up with the questions, and the respondent offers editorial suggestions like rearranging the order. This respondent was chosen for the pilot interview because the author of the study had previous knowledge of the respondent and was aware of his level of competence in the topic at hand.

2.2 Data analysis

The qualitative research approach is subjective and deals with human feelings, attitudes, opinions, and thoughts, using inductive reasoning to develop a preliminary understanding (Hayes et al. 2010). Patterns or common themes in qualitative data can be identified via inductive reasoning. The author begins with the transcription, categorizes the code, and uses it to discover underlying themes and patterns in the information.

This method was chosen because it helps to reduce the complexity of the material generated during qualitative data collecting and for arriving at interpretations of situations or processes (Hayes et al. 2010. Because of this inductive reasoning is essential to gain a better understanding and insight into qualitative interviews. Throughout the data analysis, the author inductively interprets the meaning of the data, from specifics to broad themes (Jamshed, 2014; Hayes et al. 2010).

According to Ganapathy (2016), to arrive at explanations of situations or processes, you need to methodically simplify the information that you have acquired through qualitative data gathering. This will allow you to achieve your goal of arriving at an explanation. Although the generation of complexity at the outset of qualitative research is of the utmost importance, it is yet necessary to simplify the data to arrive at interpretations that may be applied more broadly. This helps in searching, integrating patterns in the data, and coding for patterns.

Coding is the process of assigning meaningful labels, usually words, to each data segment (Ganapathy, 2016). While transcription is the process of converting the spoken words into written text, coding is the process of identifying and categorizing the key themes and patterns in the data (Ganapathy, 2016). In qualitative research, a code is typically a single word or phrase used to symbolically attach a synthesis, significance, and emotive attribute to a subset of textual or visual data. The author conducts a thorough review of the interview transcripts during the coding phase in order to extract

universal themes. Thereafter, the author finds out the code, phases it and identifies and categorizes the key themes and patterns in the data.
Beginning with the categorization of codes, in which right from the beginning of the interviews, the responses of the participants break down into smaller pieces and tagged with codes. The interviews are carried out by the author, and the structure of the data analysis can be seen in table 2.

Table 2. Coding categories extracted from the interviews.

Code categories	**2nd Order coding**	**Themes**
create difficulty and costly to switch	role of network effect	network effect
create barriers to entry		
Evaluate and prepare an exit strategy	how to handle	
impact of long term contract	role of contract term	contract term
consider short term	how to handle it	
create exit plan		
hard to integrate with others proprietary technology	role of proprietary technology	proprietary technology
adopt multi-cloud	how to handle it	

Code categories include data sets that are larger and more detailed, that includes a significant number of the same codes are used multiple times throughout. This is both natural and purposeful. It is natural because human culture is characterized by primarily repetitive patterns of action and consistencies, and it is deliberate because one of the primary goals of the coder is to locate such repetitive patterns of action and consistencies in human affairs as they are documented in the data (Ganapathy, 2016).
According to Ganapathy (2016), responses may contain irrelevant details because respondents' perspectives and contexts of relevance are different from the purpose of the paper. Because of the sheer volume of information generated during the data gathering process, in qualitative data analysis often the identification and localization of the relevant raw data.

Once the data has been transcribed and coded, it is analyzed to identify common themes and patterns. This analysis was done using qualitative data entered manually into a spreadsheet. After analyzing the data, conclusions and recommendations are drawn

based on the insights gained from the interviews. This approach allows to capture the perspectives and experiences of the interviewees in their own words, providing rich and detailed insights into the issues of proprietary technology, network effects, and contract terms toward vendor lock-in in cloud computing. These conclusions and recommendations can be used to inform future research and make informed decisions about the use of cloud computing services.

2.3 Validity and reliability

The goal of this research is to understand what role proprietary technology, network effects, and contract terms play in cloud computing vendor lock-in and how to deal with that problem. To do this right, it is important to make sure that the research and results are valid and trustworthy. When doing any kind of research, both reliability and validity are important parts of the process to make sure the research is good.

According to Harauzek (2022), the researcher is responsible for ensuring that the research is valid by ensuring that the data and results presented are reliable and up to scholastic standards. According to Ali & Yusof (2011), internal validity is how well a study shows a reason link between the diagnosis and the result that was seen. A logical process can be used to figure out if a study is valid on the inside. To guarantee this, research's methodology is solid, that the research questions are appropriate, and that the research's techniques of data collecting, and analysis yields the desired results.

According to Säfsten & Gustavsson (2020), external validity refers to the ability to make statements about the scope and transforms of the results and whether they are valid for more people and generalizable in other situations. This means external validity is dealt with by laying out the rules for who can be in and who cannot be in, describing the subjects in terms of relevant variables, and figuring out how generalizable the results are. To ensure that the author is using purposive sampling to select respondents who have knowledge and experience of the subject and Inductive reasoning is used to identify themes or patterns in qualitative data. According to Säfsten & Gustavsson (2020), the term "construct validity" refers to the degree to which an operationalization (operational definition) is able to capture the construct at hand. More specifically, it refers to the degree to which there is overlap between the operational definition (what is measured) and what is intended to be measured (the studied construct or theoretical phenomenon). To do this, the author ensures that the research questions are relevant and that the methods used to gather and analyze the data produce the desired results.

Semi-structured interviews used by the author to make sure that the research is valid. As a result of using a purposing sampling strategy, the people who took part in the interviews were people who had previous job experience and were well-versed in the problems that were being discussed because they were chosen based on their skills. Recordings of the interviews were taken, and then the data that gleaned from those recordings' transcripts. After being reheard, the transcribed data went through editing.

According to Ali & Yusof (2011) reliability is the guarantee that a different researcher looks into the same problem or working with the same data set would arrive at the same conclusion that the first researcher did. However, it is hard to come to the same conclusion. Because of that, it may be difficult to secure the reliability of the research. Additionally, it is possible for the number of people who participate in a study to influence the validity of the study; however, in general, the results are more reliable when the sample size is larger.

2.4 Considerations

Due to the in-depth nature of qualitative research, subject protection goes beyond what is required in other types of research (Arifin, 2018). Because of the importance of protecting the interviewees and adhering to ethical standards in research, potential interviewees were given information about the study's goals and methods before any interviews were conducted. People could choose to participate in the study on their own, and if they did, they were given information before the interviews were done. The information was explaining why they were chosen for the research, what the goal of the research is, and how the answers they give can help get a better understanding of the effects of vendor lock-in from proprietary technical, network effects, and contract terms points of view, as well as contribute the theoretical knowledge descriptively with a part that focuses on solutions that practitioners use to minimize the risks (Arifin & Mohd, 2018). It is critical to emphasize the ethical aspects of the research to increase its validity (Arifin & Mohd, 2018). The ethical considerations allow the author to ensure that the research does not cause physical or psychological harm to the respondents. Participants should not endanger themselves by feeling compelled to reveal sensitive information. As a result, the author takes these concerns into account and modifies the study so that it does not become overly complicated. The author ensures that privacy procedures are followed to protect the participant. The research is being carried out under strict privacy and confidentiality guidelines. Respondents should be aware that their identities will be withheld once the findings have been presented and published. To avoid misinterpretation of data collection, all interviews for those who participated in the study in any way are being recorded and then transcribed so that they can be correctly interpreted (Arifin & Mohd, 2018).

3 Theoretical framework

3.1 Cloud computing

According to Arce (2022) the benefits of cloud computing include an improvement in cooperation and data sharing as well as lower investment costs, improved business continuity, faster elasticity, and increased access. Because of the many benefits it offers, a growing number of companies are switching to cloud computing (Arce, 2022). Despite the many advantages, there are still challenges associated with sharing data accountability and relying on the tools, protocols, and standards provided by service providers (AlTwaijiry, 2021). However, in order to ensure that they are making the most appropriate choice, these organizations need to be aware of the potential risks that are involved.

Many businesses are being urged to shift their operations to the cloud because of all of the benefits that are connected with this (Finta, 2022). Also, the process of analyzing suppliers to select them is a key component for successfully migrating to the cloud. This component lowers the likelihood of being trapped in a single cloud provider (Finta, 2022). A firm may decide to switch service providers if it is not satisfied with the services, quality, or security that its cloud provider offers, if it has the desire to lower expenses, or for any other reason (Alkhalil et al. 2017). The most popular cloud computing solutions can be seen in table 3.

Table 3. the most common cloud computing solutions.

	Amazon Web Server	Microsoft Azure	Google Cloud Platform
Proprietary Technology	Amazon Elastic Compute Cloud (EC2)	Azure Virtual Machines service	Google Compute Engine Virtual Machine Service
	Amazon S3 Storage Service	Azure Blob Storage	Google Cloud Storage
	Amazon RDS (Relational Database Service)	Azure SQL Database	Google Cloud SQL
Contract Term	Saving plan for long-term commitments.	Saving plan for long-term commitments.	sustained use discounts for long-term commitments.
	savings plans that offer discounts for sustained usage.	Azure hybrid benefit that allows customers to use their existing Microsoft licenses to save on Azure costs	committed use discounts that offer even greater discounts for fixed-term commitments.
Network Effect	large and active community of users	large and growing community of users	growing community of users

3.2 Cloud computing vendor lock-in

According to Alkhalil, A., Sahandi, & John (2017), vendor lock-in is when a business becomes dependent on the services or technologies of a single vendor, this makes switching to a different vendor hard or expensive. Businesses may be locked into specific service level agreements or pricing structures, making it hard to negotiate better terms with a different provider (Alkhalil et al.2017; Arce, 2022).

According to Arce (2022), because of the widespread problem of vendor lock-in and the difficulties connected with it, businesses are moving at a glacial pace toward embracing the cloud model. Although present cloud solutions for both public and

private enterprises are designed to lock customers into a single vendor, there is only a limited ability for these solutions to interoperate with other cloud-based systems.
According to Opara-Martins et al. (2016), due to the absence of standards, vendor lock-in is a key obstacle to the widespread use of cloud computing. The vendor lock-in problem is now being addressed through technologically focused solutions and initiatives (Opara-Martins et al. 2014). There is a dearth of research analyzing and elaborating on the complexities of the vendor lock-in problem in the cloud setting. As a result, when utilizing a vendor's services, most consumers are completely unaware to the proprietary standards that severely limit application portability and interoperability (Harauzek, 2022).
According to Alshammari, o.a. (2017), businesses may need to invest in new hardware, software, and staff training, as well as re-architect their systems and applications. To mitigate the impact of vendor lock-in, businesses can take steps to ensure that they maintain control over their data. Vendor lock-in can occur when customers and vendors become increasingly dependent on one another. Some cloud providers may include terms in their contracts that make switching to a different provider difficult.

3.2.1 Proprietary technology

According to Opara-Martins et al. (2016), proprietary technology when it is owned and managed by a single entity, which is often the provider of the technology. For example, a customer that uses a proprietary database or middleware technology may find it difficult to move their applications to a different cloud provider that does not support that technology. Consumers may have a difficult time migrating to a different cloud provider due to the use of proprietary application programming interfaces (APIs), data sets that may not be compatible with the services and technology provided by alternative cloud providers. Clients may have a harder time moving their data and applications, which could result in an increase in the costs associated with switching to a different provider (Øverby & Audestad, 2021). This makes it more challenging for businesses to transfer to a different vendor. In cloud computing, the use of proprietary technology can result in vendor lock-in by making it difficult for businesses to switch to a different vendor. This is because businesses may not be able to use their existing technology and data with a different provider, which would prevent them from making the switch. Because of this, the use of proprietary technology in cloud computing might contribute to the phenomenon of vendor lock-in, which makes it more challenging for businesses to transition to a different provider.

3.2.2 Network effects

According to Øverby & Audestad (2021), network effects increase a product's value as users increase. This generates a self-reinforcing loop in which more consumers adopt a product or service, making it more valuable. When more people are using the same

cloud vendor's service, it's easier for them to communicate with one another. The value of the cloud provider's services can rise because of enhanced interoperability, which opens the door to new use cases. An increase in the volume of data created by a cloud vendor's customers paves the way for enhanced data analytics capabilities as customer numbers rise. Because of this the new entrants may have trouble competing with existing cloud companies due to this cycle because they may not be able to supply the same degree of value. If a customer chooses a new cloud provider, they may have a more difficult time switching cloud computing providers. This is due to the fact that new cloud providers are unable to compete with those already in the market. As a consequence of this, the service provider causes the consumer to face a weakness, which makes it more difficult for the customer to transition to another provider.

3.2.3 Contract terms

According to Ahronovitz (2015), contract terms are legally binding agreements that govern how cloud computing services can be used. These terms can influence vendor lock-in by specifying the conditions under which an organization can switch to a different service provider, in addition to the circumstances under which the vendor can access and use the company's data (Ahronovitz, 2015). Additionally, these terms can specify the conditions under which the company's data can be accessed and used by the vendor (Pellegrini et al. 2017). This is because clients are more likely to have faith in providers that are forthcoming about their terms and conditions and who are willing to provide robust guarantees regarding data privacy, security, and other aspects.
According to Opara-Martins et al. (2017), the contract may include terms and conditions that restrict an organization's ability to migrate to a different vendor or cloud environment. For instance, the contract may contain provisions that make it difficult or costly to move data or applications to another cloud provider or prevent the use of specific technologies or tools that may be required to facilitate the migration.

3.3 How to deal with vendor lock-in

According to Pellegrini et al. (2017), customers may be reluctant to accept cloud services if they are locked into relationships with providers that limit their options by using proprietary or restricted interfaces. Hence, consumers are unable to readily switch to different providers without incurring high switching expenses.

3.3.1 Multi-cloud

One option to prevent being locked into a single provider is to adopt a multi-cloud approach (Pellegrini et al. 2017). Assume a business wants to create and deploy a web application. They chose a multi-cloud strategy, utilizing two cloud providers, IBM Cloud and Microsoft Azure. Azure provides dependable infrastructure services such as virtual machines (VMs) and storage, as well as a dependable content delivery network

(CDN) for quick content delivery. They also offer good scalability options for dealing with traffic spikes.

IBM cloud, on the other hand, is known for its platform-as-a-service (PaaS) services. They offer managed databases, application containers, and a platform for serverless computing. Their PaaS products allow for quick development and deployment, which reduces the need for infrastructure administration. The company receives various advantages by integrating the strengths of both providers. Adopting a multi-cloud strategy can bring benefits in terms of flexibility, robustness, and leveraging the skills of several providers in this scenario. However, careful planning, management, and evaluation of the accompanying issues and trade-offs are required.

Adopting a multi-cloud strategy assists in keeping operations running smoothly even if a vendor needs to be replaced (Opara-Martins et al. 2017). While this method has some advantages, such as improved flexibility, redundancy, and the opportunity to exploit the assets of diverse cloud providers, it also has some drawbacks, such as the possibility of limited mobility and interoperability issues. Organizations might investigate cloud-agnostic designs and technologies that abstract away cloud-specific dependencies to reduce the dangers of vendor lock-in in a multi-cloud strategy. This can include adopting standardized APIs, adhering to open standards, utilizing containerization technologies such as Docker and Kubernetes, cloud-agnostic databases like PostgreSQL or Apache Cassandra, and multi-cloud management platforms such as RightScale, CloudBolt, or Scalr. Furthermore, continuous evaluation and planning for cloud provider diversity or migration methods can aid in mitigating the impact of vendor lock-in.

Snowflake (n.d.) describes itself as a cloud-based data warehousing platform that can be utilized on AWS, Azure, and Google Cloud Platform. It can enable interoperability between the two clouds. Snowflake can be hosted on AWS or Azure and provides a unified data warehouse platform accessible from both clouds. This enables enterprises to use services from both clouds concurrently and to effortlessly move data between the two clouds. Snowflake also integrates natively with AWS and Azure services such as Amazon S3, AWS Glue, Azure Data Factory, and Azure Data Lake. This enables enterprises to use these services from within Snowflake, allowing for greater interoperability between the two clouds.

3.3.2 Open-source software

According to Zhu & Zhou (2012), open-source software is an excellent option for avoiding vendor lock-in. In most cases, open-source software is built and kept up to date by a group of programmers who work together to make a program that anybody can use and alter in any way they see fit. This means that the software is not owned by any one corporation, making it simpler for consumers to choose between multiple options without being locked into one vendor's infrastructure.

According to Aldwyan, Y., & Sinnott (2019) open-source software is also more adaptable than proprietary software, making it easier to tailor to specific needs. For example, Couchbase, is an example of open-source software. According to Finta (2022), adopting cloud infrastructure and orchestration, such as OpenStack and Kubernetes, are some instances of open-source software. OpenStack is a free and open-source cloud computing platform. It enables enterprises to build and manage both private and public cloud infrastructures. It offers a variety of services, such as computation, storage, and networking, providing consumers with more control and less reliance on individual cloud vendors. Couchbase, on the other hand, is a NoSQL database built for the storage and management of vast amounts of unstructured and semi-structured data. It is designed for high performance and low latency, making it a popular solution for online and mobile applications that demand quick data access. Couchbase can be installed on-premises or in the cloud and supports a range of data models, including key-value, document, and graph.

According to Beslic, o.a. (2013), firms that use open-source database management systems like PostgreSQL, MySQL, and MongoDB can help reduce the risk of becoming locked into a particular vendor by embracing database management systems like these. Quint & Kratzke (2016) also suggested that containerization, such as Docker, is an open-source platform that makes it easier to create, deploy, and manage containers, which gives flexibility to adopt different providers or mitigate the risk of vendor lock-in. According to Finta (2022), considering using Ansible for Infrastructure as Code helps reduce the likelihood of being locked into a single vendor. Ansible is a free and open-source automation tool that supports both on-premises and cloud environments and enables users to define and manage infrastructure in the form of code.

3.3.3 Exit Strategy

According to Harauzek (2022), create an exit plan and figure out how you would move away from the vendor if you had to. It is essential to prepare an exit strategy and a plan for how to move away from a vendor if your relationship with the vendor deteriorates or the vendor's product or service no longer satisfies the requirements of your company. This may also include locating the information and software programs that are most important to the functioning of your company. For example, keep a copy of all critical data. It is essential to keep a copy of all critical data and applications in-house or with a trusted third-party provider just in case the current vendor cannot access or provide the data. Find other suppliers who sell products or services that are comparable to those already available (Opara-Martins et al. 2016). Do an analysis of their capabilities to discover whether they can fulfill the demands of your company. Create a strategy for moving away from the existing vendor and toward the new vendor while you search for a replacement. This plan ought to include deadlines, milestones, and activities that need to be carried out (Opara-Martins et al. 2016). Do trials of the products or services

offered by the alternative vendor before making the switch to ensure that they satisfy your organization's prerequisites (Harauzek, 2022).

According to Opara-Martins et al. (2017), if you have already signed a contract with a cloud provider, negotiating the terms of the contract may be more challenging. However, it may still be feasible to negotiate contract revisions or amendments, particularly if there are genuine reasons to do so (for example, changes in your business needs or unhappiness with the quality of service). When discussing adjustments to an existing contract, it is critical to approach the process constructively and collaboratively. It can be beneficial to carefully define the exact modifications you want to see in the contract as well as the rationale for these changes. It may also be beneficial to obtain the advice and support of a legal or contract expert during the negotiation process.

4 Results

This chapter discusses the results, which are broken up into two sections: the presentation of the data that was collected and an analysis of the data. No quotes were attributed to the individuals who participated in the study since the value of their privacy is so important. This is done to protect the respondents' privacy and maintain their anonymity.

4.1 Roles of proprietary technology, contract term and network effect

The research's initial query focuses on the opinions held by businesses regarding the significance of proprietary technology, network effects, and contracts in cloud computing vendor lock-in.

4.1.1 Roles of proprietary technology

During the interviews, the people being interviewed were asked what their organization thought about proprietary technology. Some of the answers to the question about how the companies felt about the role of proprietary technology in cloud computing vendor lock-in are listed below.

> *... I would say the tech stack that you're using can be a big factor. Like I mentioned earlier, if you're using.NET, for example, core or something like that, it will be very buggy to a degree for your trees and the cloud platform, so moving from Azure and this to AWS would be difficult to do, and therefore you're locked with Microsoft in this instance. Another thing would be the cost of moving your resources, and the cost is not just money; it also includes availability because some of your resources are mission-critical and need to be online 24/7.* **- Participant 5**

In this context, the participant claims that the tech stack, or the set of tools, data sets, and frameworks that are assembled and utilized during the development and operation of a software application or platform, can make it difficult to move from one cloud provider to another. In addition, the participant claims that moving your resources will not only cost you financially; it will also cost you in terms of availability. This is because some of your resources are mission-critical and must always be accessible online. During the process of moving, you will be required to make some changes in your code, for example, to point to the new location. It is possible that this will result in a decrease in the process or in the quality of your service. It is possible to accomplish this with or without the resources that you now possess, but a significant amount of labor will be required, which will result in additional expenses.

> *…we were starting to use "in-house" computing to manage IT infrastructure within our organization's own physical premises or data centers, and it became hard to create proprietary technology that was compatible with the other companies like that we had to move to cloud computing, so proprietary technology created difficulties for new customers.* **- Participant 2**

This demonstrates that the corporation was unable to utilize the current technology due to the presence of proprietary technology, which makes it challenging for the company to develop technology that is computable. On the other hand, the existing technology was incompatible with their proprietary technology, which meant that they were unable to continue using it. As a result, they were unable to continue working with the new technology.

> *…it is not motivating for new businesses, new markets, or innovation. All of them, for example, have different software development kits (SDKs), and the Azure SDK is incompatible with the AWS SDK or the GCP SDK, which is a major issue. However, if the new providers have a unique service or tool to offer the customer—something that the existing provider cannot offer to the customer in a more innovative way—they can succeed and compete with the existing big providers.* **- Participant 1**

In this scenario, the respondent asserts that proprietary technology can only be safeguarded if it is owned and administered by a single provider of the technology. Because of the use of proprietary application programming interfaces (APIs) and data formats, customers have a difficult time switching to a different cloud provider. For instance, the software developer kits offered by Amazon Web Services (AWS) are incompatible with those offered by Google Cloud Platform. Because of this, businesses had a more difficult time moving their data and applications, which results in an increase in the costs that are associated with switching to a different provider.
On the other hand, the respondent asserts that new proprietary technologies providers can achieve success and compete successfully with established large providers if they have a distinctive service or tool to offer their customers, which is something that the established provider cannot provide to their customers in a manner that is more innovative.

4.1.2 Roles of network effects

The following are some of the responses that were provided to the question about the views that are held by the businesses regarding the role that network effects play in cloud computing vendor lock-in.

> *...there may be a variety of factors at play, but one of them may be that the cloud provider is relatively new to the market and that only a small percentage of customers have adopted this technology, or, as I mentioned, we were searching only for big-name companies that could meet our needs.* **- Participant 1**

In this scenario, the participant claims that it is possible that a number of factors are at play, but one of them may be that the cloud provider is relatively new to the market and that only a tiny fraction of consumers have adopted this technology. Alternatively, as he indicated earlier, the company of P1 were searching exclusively for well-known organizations that could fulfill our requirements. This means a cloud service provider has few customers, all of whom do not receive improved service as a direct result of their collective size. Because the provider does not offer the customer better security-compatible technologies that are prohibitively expensive and do restrict the customer's ability to switch to another vendor, this is the most important reason.

> *...I agree with you to a degree, but at the same time as you will receive more attention, there will be less traffic on the servers, and so on. We had a comparison and three representatives from Google, Microsoft, and an AWS team to talk about the product, and because Google has entered the cloud services mastery with Microsoft and AWS, you can really feel like they are behind, like the product they're providing is not at the same level as Microsoft and AWS.* **- Participant 5**

P5 in this scenario states that the network effect is one of the elements that can make it difficult for businesses to move from one provider to another. This is one of the variables that can make it difficult for businesses to transfer from one provider to another. On the other hand, there will be less traffic on the servers and other such things while more attention will be devoted to you. In addition, the participant claims that they have a comparison, as well as three representatives from Google, Microsoft, and a team from AWS to talk about the product. This means the company has a real understanding of what is happening in the market and can easily select which provider can meet the customer's needs.

> *...if you have many customers, it means that you have a large amount of trust using the same cloud provider increases reliability of the service. As you said create a positive cycle where more people use a cloud provider's services, making them more valuable and attracting more users.* **- Participant 2**

According to P2, the network effect has a significant role to play in the phenomenon of vendor lock-in. If you have many clients, this indicates that they trust you and your business. Keeping the same cloud service provider results in an increase in the service's level of reliability. Create a virtuous loop in which more people utilize the cloud provider's services, hence increasing the value of those services and attracting additional customers.

4.1.3 Roles of contract terms

The following are some of the answers that were given to the question about the perspectives that the businesses have regarding the function of contract terms in cloud computing vendor lock-in.

> *…many large companies have this problem. I mean it is one of the many business issues you can get in the use case training. If I remember rightly, there was a previous use case, some bank had this problem.* **- Participant6**

The respondent claims that one of the many kinds of business problems that you can find out about during the use case training is contract term toward vendor lock-in in cloud computing. A significant number of companies are currently attempting to deal with these problems. In this instance, the terms of the contract make switching to another vendor difficult.

> *In terms of contractual agreements, I am aware that certain companies have encountered difficulties due to offering long-term discounts while failing to deliver satisfactory services. This has resulted in being bound by a contract, which is why we have shorter contracts that can be terminated if necessary. However, it may come at a slightly higher cost, as we pay monthly. Additionally misinterpreting and misunderstanding of the contract or signs and I mean the agreement SLA. In this case customer may not have enough knowledge about the rule and regulation so the understanding of the cloud agreement can be the factor that can lead to vendor lock-in.* **- Participant 3**

In this scenario, the service provider offers the customer a price reduction in exchange for signing a longer-term contract, which is detrimental to the success of the business. Because of the longer-term contract with the provider, the company is restricted from pursuing business with other consumers. They sign a contract with the provider even though the provider does not provide good service. A misunderstanding about the

contract is another factor that can lead to being locked in with a particular vendor. This means the customer has no idea what they are agreeing to when they sign the document.

> *P1, oh, yeah once you are committed to a particular cloud provider, it may be difficult for you to make changes to their account or switch to a different cloud provider. Whenever there is a shift in either the requirements of the company or the services or prices offered by the cloud provider, this can become problematic.* **– Participant 1**

In this case, after you have signed a contract with a specific cloud provider, it is challenging for you to make changes to your account or switch to a different cloud provider. It is possible for this situation to become problematic whenever there is a change in either the requirements of the company or the services or prices offered by the cloud provider. This may necessitate adapting to altered circumstances or undergoing a complex migration process to transmit data and applications to a new provider. To avoid future problems, it is essential to be aware of these potential obstacles and to consider supplier selection and understand the contract terms.

4.2 How do we deal vendor lock-in

The second question that has been investigated in this study is how different companies deal with the vendor lock-in that they either currently experience or have previously experienced. This study's findings are organized around a central theme that focuses on three different points: an exit strategy, open-source software, and multi-cloud. The responses provided by the respondents to those points are discussed under the heading that most appropriately fits them. The following are some of the responses given by respondents who either currently have or previously had experience with vendor lock-in regarding how to handle it.

4.2.1 Exit Strategy

The following are a few of the responses that were given to the question about the perspectives that the businesses have regarding the exit strategy or how to deal with cloud computing vendor lock-in.

> *Before signing any contracts with cloud providers, our company conducted a thorough analysis of their offerings and implement a caching radius to store the information in a cache. Our very own memory store radius is utilized.* **– Participant 4**

The respondent claims that they have a backup or that they implemented a caching radius to store data before signing contracts. This means the company had an exit plan and was already prepared to exit if it became necessary. In this scenario, it is essential

to prepare an exit strategy and a plan for how to move away from a vendor if your relationship with the vendor deteriorates or the vendor's product or service no longer meets the requirements of your company.

> *Negotiate clear exit sections in contracts with cloud providers. These clauses should specify the conditions and costs associated with migrating to a different provider or technology.* **– Participant 1**

The respondent is aware of the significance of the exit strategy and possesses sound intuition regarding how to proceed once it becomes clear that the provider is unable to fulfill the requirements that you are seeking. An exit strategy is a tactic that enables a company to sever its ties with one cloud provider and move on to a new vendor.

4.2.2 Open-source software

The following are a few of the comments that were given to the question that was asked about the viewpoints that the businesses have on the open-source software or how to cope with cloud computing vendor lock-in.

> *Obviously, the option would be the use of multi cloud, and the second option is use opensource. These two options can help you to go out of the box.* **– Participant 3**

The participant argues that open-source software needs to be taken into consideration as a second choice because it is a computer program that may be freely disseminated to other users.

> *In my opinion companies should consider using open standards (open-source tech such as those found in the CNCF foundation) and interoperable technologies (examples can be Snowflake and Couchbase).* **– Participant 1**

The participant contends that open source should be considered a viable option. Open standards are technological specifications or protocols that anybody can use without restriction. Because there is no single entity that has legal copyright over the code, users can experiment with different software without being restricted to a single service provider's platform.

4.2.3 Multi-cloud

The following are some of the responses to the question about businesses' perspectives on multi-cloud computing or how to deal with cloud computing vendor lock-in.

> *P2, Regarding GDPR, some cloud provider follows the rules of GDPR. So, for us and our customers, GDPR is important. In this case, our database must stay inside Sweden, and this is the law of the company. On the other side, Google Cloud Platform is not in Sweden; it is in Finland, Germany, or another country, so we select AWS for the database only.* **- Participant 2**

In this scenario, P2 argues that utilizing many cloud storage locations is one method to lessen the likelihood of being dependent on a single service provider. Even though the company adapted a multi-cloud solution because of legal aspects. They are adapting a multi-cloud solution to meet the needs of their company. Having access to multiple vendors improves your company's chances of meeting or exceeding its own stringent criteria and reduces your reliance on any one supplier. If your business is tied to a single cloud provider, you may want to look at cloud-agnostic architectures and technologies that eliminate your reliance on any one cloud (Pellegrini et al. 2017). This can be achieved through the use of tools that offer abstraction and interoperability across various cloud platforms, as well as the adoption of open standards and containerization technologies such as Docker and Kubernetes (Finta, 2022).

> *The good solution is to adopt multi-cloud, do all the tests, and if you are satisfied with what Azure is providing, then you can close your contract with AWS and fully function on AWS if you want. But it has always been recommended, right? If you can afford the cost, the skill set in your environment and multi-cloud deployment have always been things to consider. The recommendation these days is that it helps you not be locked into a single provider.* **– Participant 3**

P3 says that using multi-cloud lets you know what's good and bad about the provider, and if you're happy with what the provider gives you, you can cancel your contract with the other provider and do everything you need to do with the provider you chose. This is because multi-cloud enables you to understand what is good and bad about the provider. It has always been possible to deploy to many clouds if you have the skills and money to do so. The common piece of guidance these days is something like not being bound to a single supplier.

5 Discussion

In this chapter, the discussion centers on the findings and the associated analysis. The discussion establishes a link between the findings of the study and the problem, as well as the research findings that were provided in chapters 1 and 3, respectively. Following the discussion of the study's findings is a discussion of its methodology, which comes after the discussion of the study's findings.

5.1 Result discussion

In this study, the question that needed to be answered was what factors Swedish organizations to be locked with one cloud computing vendor and how to deal with that situation. This question was answered by looking at the data and answering it using inductive reasoning. It was through this method and the questions asked in the research that common themes emerged. The themes that were found were backed up by an analysis of the data and connected with previous research under associated subheadings.

5.1.1 Role of the factors

The first question of the research is as follows:

- *What role do proprietary technology, network effects, and contract terms play in cloud computing vendor lock-in in Swedish organizations?*

The data gathering and analysis revealed the significance of contract terms, proprietor technology, and network effects on Swedish organizations' vendor lock-in in cloud computing. Utilizing inductive reasoning in the data analysis and purposive sampling for data collection, the overall theme of what role do proprietary technology, network effects, and contract terms play in cloud computing vendor lock-in in Swedish organizations was used to develop the requirements.

P5 confirmed that the tech stack, or the set of tools, data sets, and frameworks that are assembled and utilized during the development and operation of a software application or platform, can make it difficult to move from one cloud provider to another. In addition, the participant claims that moving your resources will not only cost you financially; it will also cost you in terms of availability. This is because some of your resources are mission-critical and must always be accessible online. During the process of moving, you will be required to make some changes in your code, for example, to point to the new location. It is possible that this will result in a decrease in the process or in the quality of your service. It is possible to accomplish this with or without the resources that you now possess, but a significant amount of labor will be required, which will result in additional expenses. And this links to Opara-Martins et al. (2016) proprietary technology when it is owned and managed by a single entity, which is often the provider of the technology. Consumers may have a difficult time migrating to a

different cloud provider due to the use of proprietary application programming interfaces (APIs), data formats, and hardware that may not be compatible with the services and technology provided by alternative cloud providers.
Additionally, P2 confirmed that the network effect has a significant role to play in the phenomenon of vendor lock-in. If you have many clients, this indicates that they trust you and your business. Keeping the same cloud service provider results in an increase in the service's level of reliability. Create a virtuous loop in which more people utilize the cloud provider's services, thereby increasing the value of those services and attracting additional customers, and this can be related to the work of Øverby & Audestad (2021), when network effects increase a product's value as users increase. This generates a self-reinforcing loop in which more consumers adopt a product or service, making it more valuable. When more people are using the same cloud vendor's service, it's easier for them to communicate with one another. The value of the cloud provider's services can rise because of enhanced interoperability.
Also, P3 said that the terms of contracts play an important role in cloud computing vendor lock-in. The service provider offers a price reduction to the customer in exchange for signing a longer-term contract, which is harmful to the business's success. Because of a contract with the provider, the company is forbidden from pursuing business with other customers. And this can link to Ahronovitz (2015) where the contract terms are the legally binding agreements that govern how cloud computing services can be utilized. These terms can influence vendor lock-in by specifying the conditions under which an organization can switch to a different service provider, in addition to the circumstances under which the vendor can access and use the company's data.

5.1.2 How to handle them

The second question in the study is:

- *How have Swedish companies handled proprietary technology, network effects, and contract terms toward vendor lock-in in cloud computing?*

After the data collection and analysis, it was clear that the participants were aware that cloud providers can make switching difficult. The requirements were developed using inductive reasoning in data analysis and purposive sampling for data collection, with the overall theme of how to deal with proprietary technology, network effects, and contract terms in cloud computing vendor lock-in in Swedish organizations.
P2 argues that utilizing many cloud storage locations is one method to lessen the likelihood of being dependent on a single service provider. Even though the company adapted a multi-cloud solution because of legal aspects. They are adapting a multi-cloud solution to meet the needs of their company. Having access to multiple vendors

improves your company's chances of meeting or exceeding its own stringent criteria and reduces your reliance on any one supplier. If your business is tied to a single cloud provider, you may want to look at cloud-agnostic architectures and technologies that eliminate your reliance on any one cloud. This can be achieved through the use of tools that offer abstraction and interoperability across various cloud platforms, as well as the adoption of open standards and containerization technologies such as Docker and Kubernetes (Finta, 2022). And this relates to Opara-Martins et al. (2016) businesses should consider adopting multi-cloud methods, which can improve their adaptability and capacity to switch to a different provider if necessary.

P3 said that open-source software needs to be taken into consideration as a second choice because it is a computer program that may be freely disseminated to other users. And this relates to open-source software, which, according to Zhu & Zhou (2012), is an excellent option for avoiding vendor lock-in. In most cases, open-source software is created and maintained by a group of programmers who collaborate to create a program that anyone can use and modify in any way they see fit.

P4 claims that they have a backup or that they implemented a caching radius to store data before signing contracts. This means the company had an exit plan and was already prepared to exit if it became necessary. In this scenario, it is essential to prepare an exit strategy and a plan for how to move away from a vendor if your relationship with the vendor deteriorates or the vendor's product or service no longer meets the requirements of your company. And this can be linked to Harauzek (2022), creating an exit strategy, and determining how you would move away from the vendor if necessary. It is critical to plan an exit strategy for a vendor if your relationship with the vendor deteriorates or the vendor's product or service no longer meets your company's needs.

5.2 Method discussion

The research was carried out using a qualitative methodology, which turned out to be a good solution for addressing the objectives and concerns raised by the study However, research on vendor lock-in in cloud computing is not widely conducted in Swedish organizations. Another factor to consider is the author's previous interview experience. In contrast, the research utilized inductive reasoning and purposive sampling to select respondents who were familiar with the topic and had prior experience with it. This resulted in a more comprehensive examination, and inductive reasoning is a method for analyzing qualitative data to identify recurring topics or patterns. The qualitative method was selected because it was believed that using that approach would make it simpler to obtain knowledge that could be used to describe and explain the phenomena being studied (Säfsten & Gustavsson, 2020).

Semi-structured interviews were used to collect data for the study, which was then analyzed using inductive reasoning. The methods complement each other well and contribute to the study's goal and the answers to the questions. People give long,

unfocused answers on the semi-structured interview form, which is then broken down by theme. The semi-structured interview format was also beneficial because it allowed for both pre-planned and unplanned follow-up questions based on what the respondents said (DeJonckheere & Vaughn, 2019). An unstructured interview form could have been used for this study, giving respondents the freedom to speak candidly about the subject and their approach to the problem without being influenced by questions (Brinkmann, 2014). However, when choosing between the two interview forms, semi-structured emerged as the superior option, as an unstructured interview form could have harmed the study's validity by allowing discussion on topics other than the study's question. Structured interviews are another option; they may be preferable when it's crucial to have consistent and comparable responses. In qualitative research, semi-structured interviews are often preferred over structured interviews for several reasons. Interviewers have more flexibility in semi-structured interviews. Researchers can gain a more in-depth understanding of the participant's experiences, viewpoints, and narratives through the use of semi-structured interviews, and the participants are allowed to share their own experiences, ideas, and perspectives in a relaxed and open setting.

The purpose of the research was investigating the potential issues in proprietary technology, network effects, and contract terms on cloud computing vendor lock-in in Swedish organizations and how to handle it. This was accomplished by gathering and analyzing various pieces of empirical evidence. The sample size and the amount of expertise that the author has are the two primary factors that determine how reliable the study is. Even though it was found that six respondents were sufficient to answer the questions that were given by this study, it is feasible that a bigger sample size would have been required in order to acquire a fuller grasp of the topic. It was possible to ensure that people who were questioned had prior knowledge of the topic when utilizing a focused sample, which led to an increase in the study's validity. This was one of the positive effects of using purposive sampling to help with the selection of a targeted sample. In the given scenario, the author interacts with six individuals and receives responses that overlap or are similar. Three participants share a similar perspective on proprietary technology, while a fourth offers a divergent viewpoint. In addition, two participants indicated that they had neither knowledge nor an opinion on the topic. Regarding the network effect, four responses are similar, one response differs from the majority, and one respondent is unclear or unaware. In contrast, four participants hold the same opinion regarding the contract terms, while two are unsure or uninformed about this aspect and this can be seen in table 4. Regarding the exit plan, open-source software, and multi-cloud, all the participants were aware, but they were unaware of the disadvantages of the multi-cloud solution and the issue associated with it, such as portability and interoperability.

Table 4 the three factors and the participants knowledge of them.

	proprietary technology	network effect	contract terms
P1	customers have a hard time migrating to a new cloud provider due to the use of proprietary application programming interfaces (APIs) and data format.	we were searching only for big-name companies that could meet our needs.	once you are committed to a particular cloud provider, it may be difficult for you to make changes to their account or switch to a different cloud provider.
P2	proprietary technology creates difficulty moving from one provider to another.	if you have many customers, it means that you have a large amount of trust	The P2 position is not involved in the contract term
P3	that may be a contributor to vendor lock-in, however, I am not familiar with the underlying proprietary technology.	p3 says they sought out an established firm like AWS because of that company's widespread popularity, better customer support, cutting-edge features, and low prices.	P3 is aware that certain companies have encountered difficulties due to offering long-term discounts
P4	New providers may succeed and compete with established ones if they provide something the established ones do not: a service or tool that the customer cannot get somewhere else or in any other way	network effects can lead to vendor lock-in by creating a situation where a particular vendor becomes dominant in a market due to its large user base	misinterpreting and misunderstanding the contract or signs can make it difficult to move to another provider
P5	the participant claims that the tech stack, or the set of tools, data sets, and frameworks that are assembled and utilized during the development and operation of a software application or platform, can make it difficult to move from one cloud provider to another	I agree with you to a degree, but at the same time, you will receive more attention, there will be less traffic on the servers.	contract term does not include the P5 role
P6	Even though I am not aware of proprietary technology, I believe that it could be one of the causes of vendor lock-in.	P6 don’t believe that they have such a problem, and they use AWS.	it is one of the many business issues you can get in the use case training

6 Conclusions and further research

The findings of the study as well as some recommendations for additional research are presented in this chapter.

6.1 Conclusions

Many businesses are making the transition to cloud computing right now. The most common issue that a lot of businesses are having to deal with is being locked in with a single vendor. Most of the participates are aware of the risks associated with cloud computing's vendor lock-in, as well as the benefits of cloud computing. Concerning the circumstances that can lead to vendor lock-in and make it difficult to switch to a different cloud provider. The people who took part in the study are also aware of how to deal with the factor in cloud computing that has the potential to lead to vendor lock-in. The following are the conclusions that can be drawn from this study with the assistance of the data collection and analysis chapter as well as the discussion chapter that is linked to the two questions that were asked in this study. After the conclusions come the practical and scientific ramifications of the findings.

- *What role do proprietary technology, network effects, and contract terms play in cloud computing vendor lock-in in Swedish organizations?*

In cloud computing, vendor lock-in can be caused by several factors, including contract terms, proprietary technology, and the network effect. Customers have the option of selecting cloud providers that offer flexible contracts, open-source technologies, and interoperability with other providers to avoid being locked into a single vendor. Customers also have the option of investing in cloud services, which make it simple for them to switch between different cloud providers according to their specific requirements.

- *How have Swedish companies handled proprietary technology, network effects, and contract terms toward vendor lock-in in cloud computing?*

According to what is discussed in the finding, the client can choose from a variety of solutions to get out of this predicament, such as exit planning, multi-cloud computing, and open-source software. Utilizing exit planning, multi-cloud architecture, and open-source software are three ways in which cloud computing users can make it simpler for themselves to avoid being locked in by a single vendor. When formulating a plan to reduce the negative effects of being locked in with a particular vendor, businesses

should consider the specific demands and necessities of their operations, as well as weigh the benefits and drawbacks of several different possible approaches.

6.1.1 Practical implications

The recommendations that this study can provide to businesses that are interested in making the transition to cloud computing can be of great use to those businesses. The questions that were asked in the study are connected to these recommendations, and it can help businesses maintain relationships with vendors without becoming dependent on any one of them by utilizing these recommendations.

In a multi-cloud scenario, the range of practical implications and solutions for companies facing vendor lock-in can vary depending on the type of company and its circumstances. The distinct baselines and potential solutions for startup businesses relating to proprietary technologies, network effects, and contract terms: Startups have limited resources to deal with vendor lock-in issues, and the solution is to prioritize open standards and interoperability. This necessitates the prioritization of open-source technologies, standardized APIs, and platforms that enable portability across multiple cloud providers, such as Snowflake. Design applications and infrastructure to rely on proprietary features and services as little as possible. Employ containerization technologies such as Docker and orchestration tools such as Kubernetes for flexible deployment. Contracts with cloud service providers should provide flexibility and explicit exit strategies. Ensure that there are no long-term obligations or punitive terms that restrict the ability to transfer providers.

For small and medium-sized businesses, assets and current vendor dependencies should be considered. Consider vendor reliance, investigate alternate solutions, and prioritize contracts with flexible terms and exit plans. Concerning proprietary technologies, the organization should investigate open-source alternatives, develop in-house solutions, and place interoperability and data portability as top priorities. Concerning network effects, the business should foster collaborations with multiple vendors, diversify network connections, and partake in interoperability-promoting industry initiatives. Regarding contract terms, the company should include explicit exit plan for example consult with a legal or contract expert who can provide guidance and assistance throughout the negotiation process if it is after a contract. Consider data portability clauses, and protection of intellectual property in vendor contracts. Consider the impact of vendor lock-in on operations, costs, and future growth when developing an exit strategy. The organization should identify alternative vendors and conduct due diligence on their capabilities and compatibility, develop a phased transition plan with specific milestones, timelines, and resource allocation, communicate the transition plan to stakeholders; manage their expectations; and ensure minimal disruptions.

6.1.2 Scientific implications

The study contributes to the scientific field by providing an up-to-date picture of the factors that lead to vendor lock-in at Swedish companies as well as the ways in which the companies see fit to deal with them. This study helps show how the three factors affect businesses and how these factors have forced businesses to use only one vendor. However, there are other factors, such as knowledge gaps, that contribute to vendor lock-in that are not covered in this study. And the reason that the author wants to focus only on these three factors is that the scope of the study should not be too broad and that boundaries should be made to keep the study area narrow.

It is difficult to draw larger general conclusions regarding how to deal with this factor without considering the study to be a basis for further research in the subject due to the sample's small size. However, the study can be considered a basis for further research in the subject. This study is a contribution to pointing out the factors that can lead to vendor lock-in in Swedish organizations, as there are not many previous studies in this field that have been conducted in Swedish organizations. The study has the potential to draw attention to three factors, including network effect and proprietary technology, both of which have not been reflected in the previous research conducted on Swedish organizations. The study may also help to show that the user is a point that needs more research because there are differing opinions about how the user is affected, which is something that the study can help to show.

Regarding the findings and articles, some of the key elements that make it difficult for cloud clients to switch providers are proprietary technology, network effects, and contract terms. The difference is in how to manage them; some of the participants had no idea how to manage them, while others were familiar with open source and had an exit strategy after signing a contract. According to Opara-Martins et al. (2017), it is feasible that revisions or additions to the contract can still be negotiated, particularly if there are valid reasons to do so (such as a change in the requirements of your business or unhappiness with the quality of the service). If the process of negotiation will involve the creation of a contract, it is essential to confer with a legal or contract expert who is able to provide direction and assistance at every stage of the process.

On the other hand, the four people involved are aware of the multi-cloud option, but they are oblivious to the drawbacks associated with it, such as portability and interoperability. According to Opara-Martins et al. (2017), this method, while it does carry the risk of limited portability and interoperability concerns, does offer certain benefits, such as enhanced flexibility, redundancy, and the ability to utilize the capabilities of various cloud providers. These benefits include the opportunity to leverage the strengths of various cloud providers. Using cloud-agnostic designs and technologies that abstract away cloud-specific dependencies is one way for businesses to reduce the danger of becoming locked into a single cloud provider when implementing a multi-cloud strategy. This may involve making use of standardized

application programming interfaces (APIs), adhering to open standards, adopting containerization technologies such as Docker and Kubernetes, and making use of tools that enable abstraction and interoperability across a variety of cloud platforms. In addition, regular evaluation and planning for cloud provider diversity or migration methods can be helpful in reducing the risk of being locked into a particular vendor.

6.2 Further research

This research focuses on proprietary technology, contract terms, and network effects and how to handle them. There are several factors that can lead to vendor lock-in, and this study recommends further research on the lack of standardization for any additional research that may be conducted in the future that is not covered by this research. As a result of the lack of standardization in cloud computing, customers may find it difficult to easily move their data or applications from one provider to another. This can lead to vendor lock-in. This can give rise to concerns regarding the ownership of data, as well as privacy and safety. The study also doesn't investigate federation, which is a way for multiple cloud service providers to work together to create a solution for an organization. Federated cloud computing refers to this process. This leaves businesses vulnerable during the transition to cloud service providers (Kamel & Ashraf, 2015), and this study recommends further research.

7 Reference

Ahronovitz, M. (2015). Cloud Computing Use Cases: Introducing Service Level Agreements. *Use Cases Discussion Group, White Paper V4. 0*.

Aldwyan, Y., & Sinnott, O. R. (2019). Latency-aware failover strategies for containerized web applications in distributed clouds. *Future Generation Computer Systems*, 101, 1081-1095.

Ali, M., A., & Yusof, H. (2011). Quality in qualitative studies: The case of validity, reliability and generalizability. *Issues in Social and Environmental Accounting*, 5(1/2), 25-64.

Alkhalil, A., Sahandi, R., & John, D. (2017). An exploration of the determinants for decision to migrate existing resources to cloud computing using an integrated TOE-DOI model. *Journal of Cloud Computing*, 6,1-20.

Alsaawi, A. (2014). A critical review of qualitative interviews. *European journal of business and social science*, 3(4).

Alshammari, A., Alhaidari, S., Alharbi, A., & Zohdy, M. (2017). Security threats and challenges in cloud computing. *In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 46-51). IEEE.

AlTwaijiry, A. (2021). Cloud Computing Present Limitations and Future Trends. *ScienceOpen Preprints.*

Arce, D. (2022). Security-Induced Lock-In in the Cloud. *Business & Information Systems Engineering*, 64(4), 501-513.

Arifin, & Mohd, S. R. (2018). Ethical considerations in qualitative study. *International Journal of Care*, 1(2), 30-33.

Bergman, M., M., & Coxon, A. P. (2005). The quality in qualitative methods. *In Forum Qualitative Sozialforschung/Forum: Qualitative Social Research (Vol. 6, No. 2)*.

Beslic, A., Bendraou, R., Sopenal, J., & Rigolet, J. Y. (2013). Towards a solution avoiding Vendor Lock-in to enable Migration Between Cloud Platforms. (pp. 5-14). *In MDHPCL@ MoDELS*, (pp. 5-14).

Brinkmann, S. (2014). Unstructured and semi-structured interviewing. *The Oxford handbook of qualitative research*, 2, 277-299.

Burns, M. (2012). Cloud-based ERP: The risk of vendor lock-in. *Emerging Issues and Technologies for ERP Systems*, 77-80.

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. *Family medicine and community health*, 7(2).

Etikan, I., Musa, A, S., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, 5(1), 1-4.

Finta, G. (2022). Mitigating the effects of vendor lock-in in edge cloud environments with open-source technologies.

Ganapathy, M. (2016). Qualitative data analysis: Making it easy for nurse researcher. *International Journal of Nursing Education*, 8(2), 106-110.

Harauzek, D. (2022). Cloud Computing: Challenges of cloud computing from business users perspective-vendor lock-in.

Hayes, K., B., Heit, E., & Swendsen, H. (2010). Inductive reasoning. *Wiley interdisciplinary reviews: Cognitive science*, 1(2), 278-292.

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, 5(4), 87.

Kamel, F., & Ashraf, M. (2015). Vendor Lock-in in the transistion to a Cloud Computing platform.

Kim, Y. (2011). The pilot study in qualitative inquiry: Identifying issues and learning lessons for culturally competent research. *Qualitative Social Work*, 10(2), 190-206.

Noble, H., & Mitchell, G. (2016). What is grounded theory? *Evidence-based nursing*, 19(2), 34-35.

Opara-Martins, & J. (2014, November). Critical review of vendor lock-in and its impact on adoption of cloud computing. *In International Conference on Information Society (i-Society 2014)* (pp. 92-97). IEEE.

Opara-Martins, J. S. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud Computing*, 5, 1-18.

Opara-Martins, J. S. (2017). A holistic decision framework to avoid vendor lock-in for cloud saas migration. *Computer and Information Science*, 10(3).

Øverby, H., & Audestad, J. A. (2021). *Introduction to digital economics: Foundations, business models and case studies.* Springer Nature.

Pellegrini, R., Rottmann, P., & Strieder, G. (2017). Preventing vendor lock-ins via an interoperable multi-cloud deployment approach. *In 2017 12th International*

Conference for Internet Technology and Secured Transactions (ICITST) (pp. 382-387). IEEE.

Quint, P. C., & Kratzke, N. (2016). Overcome vendor lock-in by integrating already available container technologies towards transferability in cloud computing for smes. *Proceedings of CLOUD COMPUTING, 2016.*

Rai, N., & Thapa, B. (2015). A study on purposive sampling method in research. *Kathmandu: Kathmandu School of Law*, 5.

Säfsten, & Gustavsson, M. (2020). *Research methodology: for engineers and other problem-solvers.* Lund: Studentlitteratur AB.

Satzger, B., Hummer, W., Inzinger, Leitner, C., . . . Dustdar, S. (2013). Winds of change: From vendor lock-in to the meta cloud. *IEEE internet computing* (pp. 17(1), 69-73). IEEE.

snowflake. (n.d). *Connect to Snowflake Enterprise Data Warehouse from BI, analytics, and reporting tools through bi-directional data drivers*. Retrieved from cdata.com: https://www.cdata.com/drivers/snowflake/

Zhu, K. X., & Zhou, Z. Z. (2012). Research note—Lock-in strategy in software competition: Open-source software vs. proprietary software. *Information systems research*, 23(2), 536-545.

8 Appendix

8.1 Interview Guide

To begin with, I am grateful that you have agreed to participate in the study that I am conducting. The purpose of this study is to describe the role of different factors in terms of vendor lock-in within cloud services and how they have been managed. Your response will be kept private and anonymous. Do you mind if we record the conversation for further data analysis? Once the interview is transcribed, the recording will be discarded, and the author will allow you to read the transcript and make any changes you wish.

- Would you like to introduce yourself?
- What is your role in the company?
- What does vendor lock-in mean to you?
- How are you affected by contract terms on your cloud services?

  How has the company handled it?

  Oh …

  Something that has been identified in previous studies is called network effects.

  Oh….

  Network effects create a positive cycle where more people use a cloud provider's services, making them more valuable and attracting more users. Due to this cycle, new entrants may not be able to match the value of existing cloud providers, making them more valuable and attracting more users. Due to this cycle, new entrants may not be able to match the value of existing cloud providers. This can cause cloud service provider lock-in, making it more difficult for companies to transfer providers.

- How have network effects affected you?

  How have you handled it?

  Oh…

  Another thing that has been identified in previous studies is proprietary technology.

Oh….

Proprietary technology refers to technology owned and controlled by a single vendor. Without the provider's permission, this technology is not usable by other vendor due to intellectual property laws. Providers frequently use proprietary technology to distinguish their products and services, which makes it difficult for businesses to switch to another supplier.

- How have proprietary technologies affected you?

  How have you handled it?

- Have you identified additional aspects that affect vendor lock-in?

- Do you have any other thoughts or comments about vendor lock-in that you would like to share?

Finally, thank you, and your responses will help me better understand the factors that can lead to vendor lock-in and inform strategies to reduce the risk of vendor lock-in. We greatly appreciate your time and attention on this important matter.