WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Critical Evaluation and Comparison between Proprietary and Open-Source Cloud Systems

SEMINAR PAPER

Viktoria Pluy
Matriculation Number: 12001374

Lecture Number: 4135, Summer Semester 2023

Supervisor: Univ. Prof. Mag. Dr. Rony G. Flatscher

Submission Date: 14 June 2023

Abbreviations

AI Artificial Intelligence

API Application Programming Interface

AWS Amazon Web Services

CLOUD Act Clarifying Lawful Overseas Use of Data Act

CSA Cloud Security Alliance

CSP Cloud Service Provider

ENISA European Network and Information Security Agency

FBI Federal Bureau of Investigation

GDPR General Data Protection Regulation

GPL General Public Licence

IaaS Infrastructure as a Service

NASA National Aeronautics and Space Administration

NIST National Institute of Standards and Technology

PaaS Platform as a Service

R&D Research & Development

SaaS Software as a Service

XaaS Anything as a Service

Abstract

Cloud computing has revolutionized the market and the way how companies as well as individuals handle and store their data. This transformative technology shapes the cloud computing landscape with two approaches: proprietary and open-source cloud systems. However, users are often not able to choose between those two as they come with differences.

The aim of this seminar paper is to discover and highlight the differences of proprietary and open-source cloud systems. Based on that, a sound recommendation, whether proprietary or open-source is the preferred approach, should be given to the readers. This is done by a thorough comparison between both approaches based on different functionalities. Afterwards, a detailed critical evaluation will take place.

Emanated from the comparison and the critical evaluation, there will be a recommendation in favour for the utilization of open-source cloud systems. With the ability to review and modify the source code, a number of advantages arise. One of them being the high flexibility. The users have loads of freedom to customize, but also to create own security standards and innovate. In terms of interoperability open-source cloud systems have the opportunity to choose from various offers on the market which, as a result, prevents the vendor lock-in. Since there have been massive development processes in place to further drive innovative approaches for open-source cloud systems, a number of high-quality alternatives to proprietary cloud systems have been established. Additional quality for these systems is ensured by the online community that functions as a support system for users with urgent questions. Even cost advantages can be mentioned with open-source cloud systems as no maintenance or licencing fees need to be paid by the user.

Table of Contents

Abbreviations II

Abstract III

1 Introduction 1

2 Cloud Systems 2
2.1 Definition "Cloud System" 2
2.2 Legal Regulations 5
2.3 Proprietary and Open-Source Cloud 7

3 Comparison between Proprietary and Open-Source Cloud Systems 9
3.1 Interoperability 9
3.2 Cost 11
3.3 Security 13
3.4 Innovation 15
3.5 Usability 17
3.6 Support 19
3.7 Ethical Aspects 21
3.8 Cloud Providers in 2023 24

4 Critical Evaluation 26

5 Development Trends for the Future 28

6 Conclusion 30

7 Bibliography 31

8 Table of Figures 35

1 Introduction

"There is nothing more constant than change", states the famous philosopher Heraclitus. This quote has gained progressively more importance over the last decade since the information technology market experienced an upheaval. New technologies are introduced regularly, but not all stay relevant to the market. However, cloud computing has successfully revolutionized the IT market and changed the way how businesses operate. Additionally, advanced services for users have been created that offer them pioneering functionalities. Due to the increasing relevance of cloud computing, several companies have decided to invest in this opportunity and expand their product range or even specialize only in offering cloud computing services. This resulted in proprietary and later also in open-source cloud system offerings. Since both have advantages and disadvantages, it is often demanding for users to choose. Therefore, the aim of this seminar paper is to thoroughly compare and critically evaluate the differences of proprietary and open-source cloud systems to give a sound suggestion.

In order to come to a valid recommendation, the second chapter will focus on the definition of cloud systems and the different operating and service models. Furthermore, important legal regulations will be discussed. Afterwards the definitions of proprietary and open-source cloud systems will be introduced.

The third chapter will focus on the comparison of proprietary and open-source cloud systems based on different characteristics. Every attribute will be thoroughly explained and be brought into context with both cloud systems.

Chapter four then will contain a critical evaluation of the established differences in the previous chapter. Finally, a reasonable recommendation will be given if either proprietary or open-source cloud systems should be preferred.

A further outlook on future development trends will be given in chapter five. Several interconnected technologies will be mentioned and be brought into context.

2 Cloud Systems

The following chapter will provide an overview of cloud systems in general, including definitions and explanations. Furthermore, both proprietary and open-source cloud systems will be illustrated in more detail.

2.1 Definition "Cloud System"

Cloud computing refers to a new paradigm for the ubiquitous provision of computing infrastructure. Hereby the user has an on-demand access to several resources, like storage, servers and software applications either over the internet or over a private network. Typically, these resources are managed by a CSP (cloud-service provider) via a remote data center [IBM23].

The United States Government defines cloud computing as:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." [MT11]

That being said cloud computing has five unique characteristics and can be differentiated by four deployment models and three service models which will be discussed in the following.

Cloud Computing Characteristics

Based on the NIST (US National Institute of Standards and Technology) and the ENISA (European Network and Information Security Agency) [BSI23] cloud services are characterized by five traits:

1. **On-demand Self Service:** Resource provisioning is done without service-provider interaction.
2. **Broad Network Access**: The services are available through the web.
3. **Resource Pooling:** The provider works with a pool of resources that is made available to a large number of users (multitenancy).
4. **Rapid Elasticity:** The services can be provided quickly, easily accessible and often also automated.

5. **Measured Services:** Utilization of resources can be measured and shared with the users.

The CSA (Cloud Security Alliance) further includes a service-oriented architecture, the need for a multi-tenant cloud and a pay-per-use model as additional characteristics, next to on-demand self-service and elasticity.

Cloud Computing Deployment Models

Based on the NIST [BSI23] there are four distinct cloud system deployment models, which will now be further elaborated on.

1. **Public Cloud:** The public cloud describes a cloud system that is obtainable to users via the internet. Computing resources might be either available for free or come with a subscription fee. Within the public cloud system, the provider not only manages but also owns the data which the user is utilizing. Therefore, the provider has full responsibility for a functioning workload of the user's data. In a public cloud environment, the data center is not accessible by only one user. The infrastructure is a shared environment used for all public cloud customers. Currently leading public cloud providers are AWS (Amazon Web Services), Google Cloud and Oracle [IBM23].

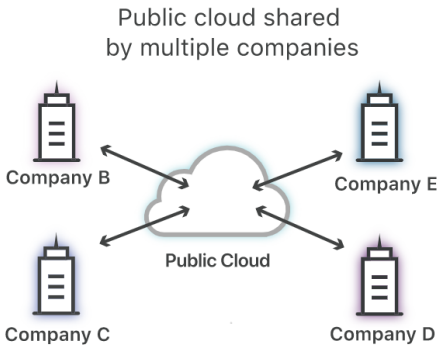

Figure 1: Public Cloud [Clo23]

2. **Private Cloud:** Contrary to the public cloud, a private cloud environment, also called internal cloud, has its resources only accessible to one single user. Normally, the private cloud runs directly in the user's data center, which combines the advantages of a cloud system with an on-premises infrastructure. However, it can also be run in an independent data center. This type of cloud system is typically used by

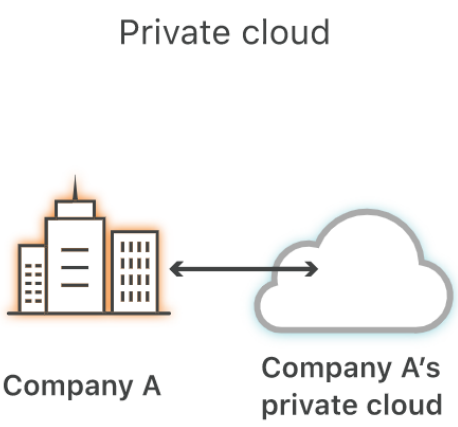

Figure 2: Private Cloud [Clo23]

companies and organizations that require a more secure and higher controlled environment over their computing resources [IBM23].

3. **Hybrid Cloud:** The third variety of cloud systems is a combination of a public and a private cloud. The aim is to provide an organization with the flexibility to use either one of them based on their current circumstances. Ideally, the hybrid cloud is an integrated infrastructure and connects both public and private cloud systems [IBM23].

4. **Community Cloud:** In a community cloud multiple organizations share different resources and services based on common interests on a single cloud infrastructure [BSI23].

Cloud Computing Service Models

When it comes to cloud computing, three individual cloud services are available and can be run: IaaS (Infrastructure as a Service), SaaS (Software as a Service) and PaaS (Platform as a Service).

- **Infrastructure as a Service:** IaaS provides computing resources in the shape of hardware and associated software as a service. This authorizes the users to provide different resources when needed rather than having a long-term commitment. This gives the user flexibility with pricing because they are able to choose between a contract and a pay-as-you-go basis. That being said IaaS is a form of hosting because the service provider owns the equipment and maintains it, but the users need to deploy their own software services manually [BJJ10].

- **Platform as a Service:** PaaS on the other hand supplies users not only with hardware but also with some type of application software. The hosts offer a deployment platform for applications as a service to the users over the web [BJJ10].

- **Software as a Service:** The idea of SaaS is to provide access to software applications over the cloud. The SaaS host offers the application via their data center to users over the internet. The user then pays on a consumption basis for the used applications. The tenants do not have to do additional development or programming, but they often have the opportunity or need to configure the software [BJJ10].

Over the last few years more and more service models have been established. This ranges from security as a service or business process as a service to storage as a service. These different types are often summarized under the term anything as a service (XaaS) [BSI23].

2.2 Legal Regulations

Due to the dynamic growth of cloud systems, different legal measures have been taken, one of which is the US CLOUD Act (Clarifying Lawful Overseas Use of Data Act).

CLOUD Act

In March 2018 the US federal legislature adopted the so-called CLOUD Act. This particular US law strives to describe rules for sharing users' data for the purpose of criminal proceedings by organizations providing cloud services. These organizations need to hand over the data even if the data is not processed and saved in the US but rather for example on servers in the European Union. However, the data still needs to be requested via an official governmental channel like a warrant or a subpoena [Roj20].

Originally the CLOUD Act was introduced because the US FBI (Federal Bureau of Investigation) had difficulties with acquiring user data via warrants. The law that regulates warrants was drafted before cloud computing was a wider used technology. These issues from the FBI were highlighted by the popular Microsoft Ireland case which then also built the foundation of the US CLOUD Act. In this particular case the US government argued that they have the right to access Microsoft's data as they were a part of a US drug trafficking investigation. However, Microsoft contradicts to these demands because in their opinion the state does not have the authority to access any data that is not stored on US soil. After

bringing the case to the US Supreme Court the governors decided to enable the CLOUD Act and therefore allow the US law enforcement to access the data from Microsoft Ireland [Das18].

Since cloud computing offers cross-border services, one key feature of the CLOUD Act are the bilateral agreements between the US and other federal governments. One recently made bilateral agreement is between the US and the UK. The Data Access Agreement, which is the name for the mutual agreement between the US and the UK, is based on the CLOUD Act and will allow the US to gain better and faster access to data stored in the UK for crime investigations. Similar agreements have been made with Australia and Canada [Roj20].

Even if big players in the technology field like Google or AWS have announced their support for the CLOUD Act, several complaints have been filed by other groups. One issue being constantly brought up was the conflict with the European GDPR (General Data Protection Regulation). The CLOUD Act enables the US government to subpoena users' data not only from the US but also from abroad without the users' consent whereas the GDPR has regulations for the exact opposite. The GDPR sets a framework for all companies that operate with data of European citizens and states that explicit consent needs to be obtained from the user upfront before collecting their personal data [Roj20].

As of June 2023, an agreement between the European Union and the US has not been made which leaves this issue unresolved for now. However, with an US-EU bilateral consensus this problem can be resolved. Especially with the European Union being such an important player and having a leading role in the modern privacy protection of cyberspace, it may be worth pursuing to offer them a proactive role in shaping further legal regulations that are not partly incompatible with other governmental policies [Roj20].

2.3 Proprietary and Open-Source Cloud

Based on the dynamic growth of cloud computing there has been a significant historical change. In addition to the availability of a proprietary cloud, there has been an increasing demand for an open-source cloud over the past three decades. All four cloud categories, meaning public cloud, private cloud, hybrid cloud and community cloud systems have the opportunity to be either proprietary or open-source. In the following chapter a short overview of both types will be given.

Proprietary Cloud

A proprietary cloud system includes a computing infrastructure that is maintained by one vendor or organization. When working with a proprietary cloud, the user is not permitted to modify the source code. This leads to a certain dependency on the vendor because the user is tied to the organization with regards to different tools and components. Additionally, a proprietary cloud always comes with subscription and/or licencing fees [OST16]. Yet mentioned and further characteristics will be discussed in chapter three.

Well-known vendors for proprietary cloud systems are for example IBM Cloud, Oracle Cloud and Google Cloud.

Open-Source Cloud

The open-source cloud has gained more and more popularity among organizations particularly in the last few years. Compared to a proprietary cloud, an open-source cloud refers to a computing architecture where the source code is publicly available. Based on that everybody can access, revise and distribute the source code. The development process of open-source is more or less a collaborative process, where several contributors work together. Open-source clouds often offer more flexibility, customization, and cost-saving alternatives to the users [ZPS14].

Based on Mr. Bretthauers research [Bre01] especially open-source has evolved over the last 30 years from a completely unknown territory to one of the most or even the most popular computing infrastructure of the 21st century.

- **1960/1970:** For the first time in history, developers agreed to share their source codes leading to the first open-source operating system called Unix.

- **1980:** In the early 1980s severe changes were made to Unix leading to the GNU GPL (General Public Licence) project led by Richard Stallman. The published GPL enabled users to distribute their source code and modify software while also protecting their legal rights.

- **1990:** Approximately five years after the launch of the GNU, a Linux operating system was released with GNU tools and for the first time a viable alternative to proprietary software was established. Due to the popularity and increasing technologies of the internet at that time, a widespread adoption of open-source was achieved.

- **2000:** Finally, popular companies like Google or IBM started to invest into open-source alternatives which lead to further development for these types of projects.

Currently many different software licences co-exist in the IT-World. Figure Three will give a brief overview on the most popular ones.

Capabilities (Without Application Licensing Restriction)	GPL (Linux)	Dual-GPL (MySQL)	LGPL/MPL (OpenOffice, Firefox)	Apache/BSD (Apache, FreeBST)
1) Download	✓	✓	✓	✓
2) Evaluate	✓	✓	✓	✓
3) Deploy	✓	✓	✓	✓
4) Redistribute	⊘ [1]	✓ [3]	✓	✓
5) Modify	⊘ [2]	⊘ [2]	⊘ [2]	✓ [4]

Figure 3: Open-Source Software Licences [AOC11]

Until now different developments of open-source systems are achieved on a regular basis making open-source an essential part of every technology ecosystem.

However, companies and organizations often underestimate the features and capabilities of open-source, resulting in a higher adoption rate of proprietary cloud systems. A thorough comparison between those two will be done in the subsequent chapter followed by a critical evaluation in chapter four.

3 Comparison between Proprietary and Open-Source Cloud Systems

The following chapter will illustrate the differences between both proprietary and open-source cloud systems with regards to various characteristics.

3.1 Interoperability

Interoperability plays a key role in the paradigm of cloud computing and enables the evolution of collaborative services. That being said, interoperability refers to the ability that different systems can co-exist and connect with other applications that are either already available or might be developed in the future. When looking at cloud systems, interoperability is a highly important characteristic because one organization might use different cloud systems that all need to be integrated smoothly and managed effectively [AOC11].

Open-Source Cloud System

Firstly, when looking at interoperability, there needs to be a distinction between open-source and open standards since these are two different concepts. Open standards refer to publicly available specifications that are developed by an open-community and enhance interoperability leading to amplified data exchange. Open-source on the other hand refers to the publicly available source code. Following this definition, it is clear that open standards allude more to specifications whereas open-source touches on implementation. Even if they are two distinct concepts, they are often used together to ensure interoperability [AOC11].

According to Almeida et. al [AOC11], three important advantages referring to interoperability can be highlighted when using an open-source cloud system. Due to the accessibility of the source code and the rights to modify it, developers have an easier job to implement different systems, connect them and therefore build modular, efficient systems. In addition to that, the developer community often tackles upcoming generic obstacles together which leads to an insignificant number of unresolvable interoperability problems.

Furthermore, due to the transparency of the source code, organizations have the ability to verify that the software operates as it should which leads to higher trust in operability.

By leveraging open-source and open standards different cloud platforms have the ability to exchange data more easily. This results in a quicker movement of data between different cloud applications without the need of significant customization.

Proprietary Cloud System

When taking a closer look at proprietary cloud systems, interoperability cannot be achieved so easily as it can be with open-source due to the uniquely used proprietary protocols and interfaces from various organizations. This often forces a vendor lock-in, where users do not have the freedom to choose from different vendors or services. If they decide to switch the cloud provider, it may come with major re-adjusting to the system. For that purpose, some proprietary cloud vendors, for example AWS, offer tools and API's (Application Programming Interface) to enable integration with other systems that are not from the AWS product portfolio to accelerate data exchange [DB14].

In addition to the offered tools from proprietary cloud vendors like AWS, there are offerings from third-party providers. They also provide tools for organizations to see through the differences of various proprietary cloud systems and enable a seamless communication [Mün13].

In summary, there are a few differences to consider between open-source and proprietary cloud systems in terms of interoperability.

- Open-source cloud systems ensure easier integration of different systems due to the available and modifiable source code, which makes it effortless to implement and connect them. The continuous ability of open-source cloud systems to verify ongoing operations builds further trust in interoperability.

- Achieving interoperability between proprietary cloud systems can be more challenging than with open-source cloud systems. However, with the right usage of API's and other tools, like third-party offerings, a successful and seamless communication between systems can be established.

3.2 Cost

Obviously, there are serious distinctions between open-source and proprietary cloud systems in terms of cost. Therefore, it is essential for organizations to evaluate their budget before choosing between those two. In general, the main contributors to costs are licencing, deployment, and customization expenses.

Licensing

One of the most prominent distinctions between proprietary and open-source cloud systems are the licencing fees, which also represent a fundamental aspect of cost. Nevertheless, it is important to note that every software application needs a software licence to run. Due to the fact that proprietary clouds are normally commercial, an organization needs to pay for the licensing fees. The expenses for a proprietary cloud can differ extremely based on the wanted services, number of users, levels of support and more. These licencing fees often also cover any maintenance and support tasks such as applying security patches and providing regular updates [SBJ15].

In contrast, an open-source cloud is not commercial and therefore only offers licences that indicate that the service is free of charge. Such licences could be the Apache Licence or a GPL (General Public Licence) which is also the most common. These licences allow the user to use the service without charge as well as modifying and distributing it. However, opting for an open-source cloud with a non-commercial licence means organizations will be responsible for carrying out maintenance work themselves. On the one hand that means that you have more flexibility and control over the maintenance but on the other hand it signifies that more expertise and skills of internal workers are needed [SBJ15].

Deployment

When it comes to deploying proprietary and open-source cloud systems, there is an inconsequential distinction associated with costs can be made. Proprietary cloud systems often come with high deployment costs such as hardware, implementation services, staff training and of course the acquisition of the cloud system itself [Bai08].

Open-source cloud systems also require certain hardware infrastructure and therefore also come with deployment costs. Especially in the last few years open-source vendors started to charge for additional add-ons, as well as further administration [SBJ15].

Customization

When acquiring a proprietary cloud system there are several options for customization which of course come at an additional cost. This does not only cover configuration but also includes changes that need to be done in order to have successful operations within the acquiring organization [SBJ15].

An open-source cloud system also allows for customization. There are normally no additional charges as the process of customization is done with community support through discussions on blogs or websites. Therefore, no costs arise for needed customization. However, a strong skillset and expertise of workers within the organization is needed to implement the changes [SBJ15].

A short summary of the cost differences of proprietary and open-source cloud systems will be given now.

- Proprietary cloud systems come with large deployment costs that cover the cloud acquisition and further elements like hardware infrastructure. Additionally, licensing fees arise that also cover maintenance and support for the organization. When there is need for customization, supplementary costs will emerge.

- Open-source cloud systems also require deployment costs that cover for example hardware infrastructure. However, open-source cloud systems are not based on commercial licences which means that these are free, and no licensing fees will be charged for utilization. Since there are no licensing fees, there is no covered maintenance and support for the organization. Nevertheless, due to the online community forums advice can be sought immediately. However, internal resources need to be qualified enough to handle maintenance and support activities as well as customization.

3.3 Security

Security plays an essential role in every system and/or application. This especially applies to proprietary and open-source cloud systems since the stored data is distributed over the internet. When comparing proprietary and open-source cloud systems, the security aspect is influenced by a variety of factors. Before starting the comparison between proprietary and open-source cloud systems with regards to security, it is essential to know that both proprietary and open-source cloud systems have the ability to be labelled as secure. With proper measures both types can achieve a high level of security. Together with an in-depth assessment of the specific needs an organization has and an overview of the company's risk tolerance, the right type of cloud system can be chosen. Along with essential security measures like multi-factor authentication, firewalls and more, a sufficient level of security can be established with both proprietary and open-source cloud systems. In this comparison there will not be an evaluation of adequate measures that need to be followed to ensure security, but rather a listing of differences how the security process looks like within the two types of cloud systems.

Proprietary Cloud System

A proprietary cloud system is often seen as more secure since it is developed in a controlled environment by trained employees. Furthermore, the cloud system is also controlled by only one vendor which can lead to quicker response to any security breaches. However, it is important to emphasize that due to the fact that only one vendor is responsible for a secure environment, there needs to be high trust between the cloud system acquirer and the vendor. The users must rely on the seller to integrate upcoming patches, updates, and certifications on time to safeguard them from any breaches [FRR+18].

Additionally, cloud vendors are surrounded by experts that deal with cloud security on a daily basis. Dedicated teams are responsible for keeping all necessary security measures up-to-date and address any potential vulnerabilities. These professionals are also in charge of modifying the source code when needed. With their security expertise a more intensive auditing can be achieved, leading to fewer data breaches for the user. However, the missing transparency of the source code limits the availability for independent security experts to review the code and therefore identify potential vulnerabilities that may exist for the user [FRR+18].

Open-Source Cloud System

One important aspect to consider regarding security of open-source cloud systems is that they are not always developed in a controlled environment. Large open-source companies might to do that but often the development is done by individuals from all over the world which makes security more of a shared responsibility. In addition to the transparency of the source code, the collaborative nature of the open-source community has major benefits for the security auditing. Since all of the individuals are able to review the source code, potential vulnerabilities can be identified more easily. Subsequently, they can work together on a proper solution and fix the source code afterwards. The collaborative nature of this process often leads to faster identification and resolution of vulnerabilities [SBJ15].

But not only the open-source community has the ability to review the source code. Security experts can also review the code and make sure that the security measures align with best practices. This allows users a broader range of engagement from different people, including both experts and the community itself. Consequently, this will eventually lead to a faster response time with higher quality advice. All individuals can come together, work on the identified vulnerability, develop a solution and lastly distribute patches or solution approaches [SBJ15].

According to a recent study mentioned in the paper of Singh et. al. [SBJ15], it was found that security vulnerabilities can be fixed twice as quickly within the open-source community compared to commercial software.

Required patches and updates need to be integrated by the user itself. This requires a strong skillset and expertise. Additionally, the user needs to have a clear understanding when updates and patches need to be implemented to secure the cloud system properly [SBJ15].

During the comparison it became evident that there are different approaches to ensure security within proprietary and open-source cloud systems.

- Proprietary cloud systems are developed within a controlled environment by trained employees. These experts are able to modify the source code by themselves where they can achieve a high-quality auditing of the system which may lead to less security breaches for the user. Given the lack of transparency in the source code, users can only count on the expertise of the vendor and their center of excellence. This reliance creates a necessity for high vendor trust.

- Security aspects of open-source cloud systems are solved through a collaborative process where both individuals of the open-source community and independent security experts are involved. Due to this broad engagement upcoming security issues may be solved quickly and efficiently due to a faster response-time and more pieces of advice. However, the integration of the identified alterations as well as updates and patches need to be done by the user itself which requires high engagement and a lot of expertise.

3.4 Innovation

In our fast-paced world the creation and integration of innovation is essential. Especially the new paradigm of cloud computing needs to be innovated repeatedly to fulfill the needs of the market. Both proprietary and open-source cloud vendors have realized the importance of innovation for their products due to the increased usage of their services. The contribution of proprietary and open-source cloud systems to innovation happens in different ways.

Proprietary Cloud System

While some might say that the unavailability of the source code may be a difficulty for innovation, it is not. Several experts from within the vendor's organization and different independent specialists are working on making the cloud system better and more efficient. In order to do that an organization will invest resources into the R&D (Research & Development) process. With additional investment and the expertise knowledge of consultants, researchers and other employees, innovation for proprietary cloud systems will be facilitated [SBJ15].

Besides the center of excellence of the vendors organization there are several existing online client groups that foster further innovation. This is done by contributing with thoughts, concepts, or best-practice solutions. An example for that could be leaving reviews which will animate the vendor to foster innovation and adjust the cloud system to the needs of the customer [SBJ15].

According to Singh et. al. [SBJ15] the significant focus on R&D from the vendors organization also comes from the companies need to not become irrelevant. It will always be a priority for the vendor to include innovation from the market and specific customer needs in a timely manner to offer a high-quality product with competitive advantages to boost sales. The users will profit from this revenue-oriented way of thinking by always having a first-rate cloud system with the newest creative alterations included.

Open-Source Cloud System

The research of Singh [SBJ15] marks a few characteristics of innovation for open-source cloud system. Firstly, an open-source cloud system enables innovation for the user with the ability to view the source code and modify it, to tailor it to their specific needs without any restrictions. This transparency offers huge freedom to the user.

When an innovation breakthrough is achieved, it can be immediately shared with the online user community. However, that is not a necessity. Therefore, innovation might not always be known by all community members which could lead to a competitive advantage only for the innovator itself. Even if the innovation is shared over an online forum, it might only be seen by engaged users.

However, these existing online forums through its collaborative creation process can be a center of innovation. When all members actively participate, engage with the context, and share their expertise, the creation of new ideas can be unlocked at a rapid pace. Due to the immense number of online user groups, vendors of open-source cloud system generally are not in favour of large-scale R&D.

As we can see both proprietary and open-source cloud systems are a subject to innovation. With the increasing utilization and importance of cloud computing

further innovation will be achieved, both through R&D expenses from proprietary cloud vendors and through the collaborative process of the open-source community.

The above-mentioned facts will now be summarized shortly.

- Proprietary cloud vendors invest into R&D to contribute to the creation of new ideas. Together with experts from within the organization and independent specialists, innovation can be achieved. Especially for commercial cloud vendors the creation of unique ideas is key to stay relevant in the market and their customers and therefore to increase their sales.

- Open-source cloud vendors rely hugely on the collaborative process of their online-community for the creation of innovation. Through this joint interacting, breakthrough innovation can be achieved. However, this may not always be perceived by every user either due to the non-sharing of innovative ideas or the unwillingness to participate actively on community platforms.

3.5 Usability

Due to the huge supply range of cloud systems on the market, it is essential for vendors to ensure that their products have excellent usability. Usability describes the capability to interact with a product and use it efficiently and effectively. For companies it is crucial to emphasise usability, otherwise the customers will fulfill their need with someone else [Nie12].

Proprietary Cloud System

When looking at proprietary cloud systems, usability usually is very high positioned. This is based on two premises. Firstly, usability often marks a competitive advantage over other existing vendors. Secondly, when no sufficient usability is established within the product, the users are more likely to abandon the product and fulfill their needs elsewhere. Therefore, commercial cloud vendors are more likely to do regular usability testing. This results from the fact that the tailored demands from their customers need to be met [PK13].

To further support users with an efficient and effective interaction with the cloud system, vendors often distribute support manuals. This instant referral allows the

customers to quicker understand the system, improve the learning and therefore empowers immediate usage of the proprietary cloud system [SBJ15].

Besides distributing manuals vendors frequently offer different supporting materials which include for example seminars or training courses. With these methods further employment of the cloud system should be guaranteed [SBJ15].

Open-Source Cloud System

Especially in the last years different open-source cloud systems have been condemned for their missing usability. This was based on the fact that open-source systems have not conducted usability testing prior to their release which led to insufficient ease of use for the customers. However, things have changed, and the importance of a user-friendly and intuitive interface has been acknowledged [SBJ15].

At present the usability of open-source cloud systems is tested by the online community which leads to new and satisfactory solutions that are not prone to any developer bias. One core element of usability engineering within open-source cloud systems is the fact that the developers are also users. That means they have deeper knowledge of the exact needs. Additionally, users have the opportunity to seek advice and share experiences which triggers further improvement for cloud systems. Moreover, the regular engagement of users on the platforms and their discussions on usability leads to an iterative cycle of improvement [PK13].

Due to the collaborative process of idea creation over online-forums or blogs, an immediate documentation of action happens even if they are not legally required to do so. Furthermore, open-source cloud vendors often offer multiple manuals and guidelines so users can fully leverage all the offered features of the cloud system. If questions occur that cannot be answered with manuals, the online community can deliver answers [PK13].

In addition, open-source cloud systems have the opportunity to integrate other frameworks and tools from different vendors due to the utilization of API’s. This further enhances usability for the user as it provides them with greater flexibility to integrate additional features to fulfil their unique requirements [NTY01].

We have seen that both proprietary and open-source cloud systems have the ability to offer high-level usability. The above-mentioned points on how this can be achieved will now be briefly summarized.

- Commercial cloud vendors value usability a lot. Therefore, regular usability testing is conducted by experts to ensure the delivery of high-quality and easy to use cloud systems. Together with distributed manuals and offered training courses, the vendors try to further empower utilization of their systems.

- The open-source community also has acknowledged the importance of usability for their cloud systems resulting in collaborative usability testing over their online forums. Even if they are not legally required to offer support materials, they also provide manuals and exact documentation. Additionally, usability of open-source cloud system can be enhanced by integrating other independent frameworks and tools.

3.6 Support

Offering efficient and effective support is always a must for companies that work with information technology. Especially with cloud systems that work over the internet and often contain sensitive data, successful support needs to be provided to customers to help them with any upcoming issues. The offering of support can look different between proprietary and open-source cloud systems.

Proprietary Cloud System

Support is probably the greatest competitive advantage of commercial cloud systems. As mentioned in chapter 3.2., proprietary cloud systems come with licencing fees. When paying for these fees the users are entitled to ongoing support from the cloud vendor. This is especially important for customers without technical mastery. If users encounter difficulties with the cloud system and the provided manuals are not sufficient enough, the proprietary cloud vendor offers official, immediate support. Support channels could be via a live chat, a hotline or personal contact persons [SBJ15].

The employees from the commercial cloud vendor are trained for giving appropriate and prompt assistance. The support workers often need to undergo extensive training to handle complex issues as efficiently as possible. This

immediate support from qualified employees reduces downtime and ensures the trouble-free continuing of the customers processes [SBJ15]. The deep knowledge of the employed workers is one of the main reasons why proprietary cloud systems have been chosen over open-source in the past, as it can reduce risk for the client [PK13].

Another point to consider is that after revealing the issue to the support team, immediate action can happen, since the system is controlled and maintained by the vendor.

Open-Source Cloud System

Open-source cloud systems rely heavily on their online community to tackle upcoming issues. Due to the fact that several individuals from all over the world are a part of the open-source community, a very fast response time to problems can be achieved. However, there needs to be actual knowledge of the occurring issue otherwise the given feedback might not be sufficient enough [PK13].

When turning to the online community with a system issue, one will receive comments and advice from all active participating individuals. This collaborative interaction can lead to finding effective solutions very quickly as experts from different domains interact with each other. However, since the users then need to implement the given feedback themselves, it is essential to have the skills and expertise to understand the points given and resolve it afterwards within the system [PK13].

As we have seen, there are profound differences in the support from proprietary and open-source cloud systems. Ultimately, the decision between those two depends on the specific requirements of a company. To make the distinction of those two in relation to support more obvious, a concise summary will be given.

- Proprietary cloud systems are characterized by immediate support within certain response times given by trained professionals from the vendors organization. This instant and effective support reduces risk for the customer and ensures smooth operations along the way. After issuing the problem to the vendor immediate damage-control can be done.

- Open-source cloud systems rely on the collaborative interaction of their online community when offering support to upcoming issues. Due to exchange of individuals from all over the world, different solution approaches can be identified. However, this is all dependent on an exact description of the user's issue. When an appropriate solution has been found, the user itself needs to implement it which requires lots of expertise in this field.

3.7 Ethical Aspects

When talking about ethics in cloud computing there is a range of information to consider to ensure a responsible way of use. Usually, ethical considerations can be distinguished in three groups, which are data, provider, and user. The category data refers to data privacy, ownership, and security. Data ownership becomes a more and more important aspect in cloud computing, since an increasing number of people outsource their sensitive data to cloud services. Especially since cloud computing services operate across-borders, different legal regulations may apply that do not always align with national laws (see chapter 2.2). Data security and data privacy are also forthcoming ethical aspects that need to be considered. Data security must secure the data from unauthorized access whereas data privacy relates to the integrity, availability and confidentiality of data that needs to properly comply with legal regulations. The providers need to concentrate on sustainable and green cloud computing. With reference to users, aspects of individual empowerment are vital which refers to the ability to co-develop the product. [MR21].

Proprietary Cloud System

When looking at first category, which is labelled as data, a proprietary cloud system has a huge impact on privacy, ownership, and security.

Firstly, even if proprietary cloud systems are normally controlled and managed by one single vendor, usually the vendor does not claim ownership over the data. However, the user often grants rights to the vendor to use, store and manage their data. Data ownership can vary between different user contracts since they are dependent on the agreed terms and conditions [Chi16].

Surely all proprietary cloud vendors need to safeguard their user's data as good as possible, otherwise they will not be able to acquire new customers. However, there is no general statement on how safe someone's data is with a proprietary cloud vendor. Since the introduction of the CLOUD Act (see chapter 2.2) some aspects of data privacy might be harder to achieve. Especially since there is some friction with the European GDPR. Nonetheless, different proprietary cloud vendors have commented and released statements that any data they store will be safe and that they are committed to ensure data privacy.

Figure 4: Data Privacy & CLOUD Act – AWS [AWS23a]

When looking away from the data aspect and to the provider's side, a green offering of proprietary cloud services is important. On the one side, proprietary cloud systems require significant energy resources due to the wide hyperscale data centers. On the other hand, experts say that the usage of cloud might be the greenest technology due to the centralized characteristics. However, proprietary cloud vendors have recognized the importance of global warming and its impact. Therefore, strategies have been established that help to reduce the carbon footprint and support the usage of renewable energy for their data centers [MR21].

The individual empowerment of users also plays a significant role within ethical aspects of cloud computing and refers to the ability to co-develop and/or co-create a product [MR21]. Proprietary cloud vendors offer the possibility for customization. Additionally, they will ask for the user's feedback to optimize their services. This leads to a certain range of individual empowerment for the user. However, the customer itself cannot develop anything. Due to the vendor-lock in, users often

lack the ability to merge different cloud systems to best suit their needs. These facts limit the individual empowerment of users within a proprietary cloud system.

Open-Source Cloud System

Within an open-source cloud system users maintain ownership over their data they upload to the cloud since there is no vendor who manages or controls the environment. When taking a closer look at data privacy it becomes clear that resolving this matter lies within the responsibility of the user. Due to the availability of the source code, they have the possibility to review it for any disadvantageous loopholes. If they are not satisfied with the level of privacy, they are able change the code [Ger21].

Due to the fact that open-source cloud systems need data centers to offer their services, they also need a lot of energy resources. However, more and more renewable energy assets are used to run these data centers [MR21].

When looking at individual empowerment, open-source systems offer lots of advantages. Since the users are able to review the source code, they have the possibility to make any change they want. Furthermore, they can merge different tools and services of various open-source cloud vendors which fosters further customization to fulfil their needs.

As we have seen both commercial and open-source software cloud systems can ensure an ethical and responsible way of use. The given information will now be briefly summarized.

- Users that utilize a proprietary cloud system normally maintain ownership of their data. However, that is dependent on the terms that are agreed on in the contract between the vendor and the user. Data privacy and security might now be harder to achieve now due to the US CLOUD Act but still vendors assure all their customers to safeguard their data appropriately. Another ethical aspect that needs to be dealt with is the green offering of services. Even though proprietary cloud systems need lots of energy resources for their data centers, they can reduce the carbon footprint with centralization. The last element of ethics is individual empowerment which is established for users with the possibility for customization.

- When utilizing an open-source cloud system, the users maintain ownership over their data. Users have the opportunity to ensure data privacy by reviewing the source code and potentially making necessary changes to meet their privacy requirements. Since data centers are needed for the provisioning of open-source services, high carbon usage is required. Starting from 2023, there will be a shift towards the usage of renewable energy resources to reduce the carbon footprint. Lastly, individual empowerment for the user is achieved through the ability to view the source code and make any alterations that are needed.

3.8 Cloud Providers in 2023

As of June 2023, there are several vendors that offer commercial and open-source cloud system. Due to the evolving and increasingly important market, there is a growing number of vendors and there will certainly be new players in the future.

Proprietary Cloud System

In the following, the three organizations with the most impact on the market will be presented.

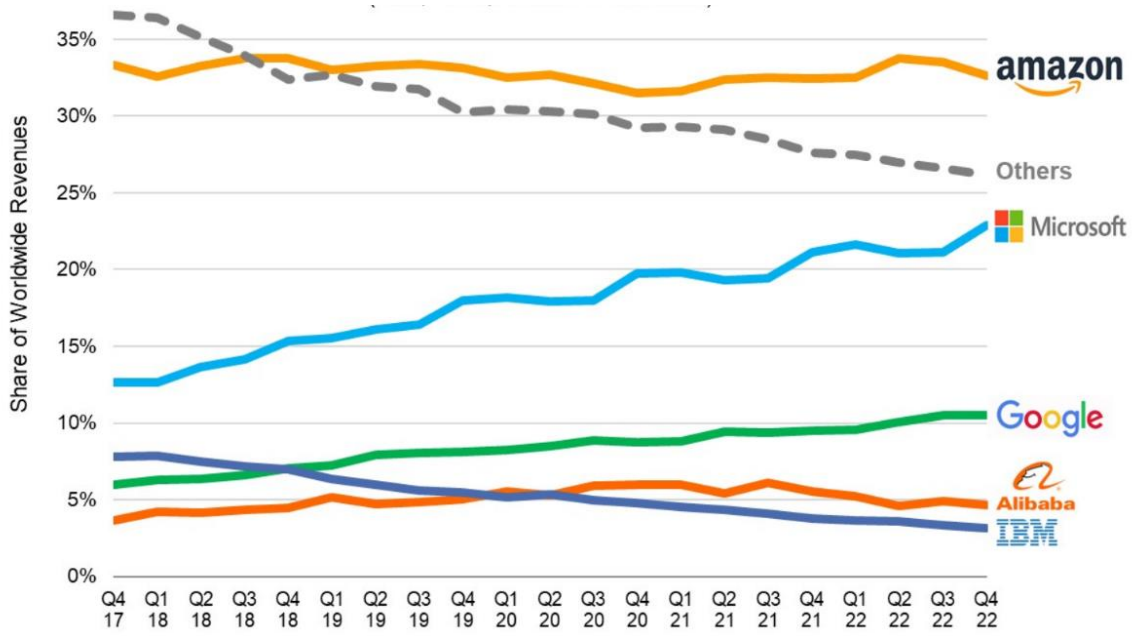

Figure 5: Cloud Vendors Market Share 2017-2022 [Syn23]

- **Amazon Web Services (AWS):** With a market share of around 33% of the overall cloud market at the end of 2022, AWS is the leading cloud service

provider globally. With pre-built cloud solutions for 19 industries and numerous services based on different technology categories, AWS made a profit of approximately 21 billion US dollars in 2022 [AWS23b].

- **Microsoft Azure:** Microsoft Azure was able to reach a market share of 23% in Q4 in 2022. With a similar product range from AWS, Microsoft Azure additionally offers a wide range of cloud services that can be well integrated with other Microsoft products on the market [Mic23].

- **Google Cloud Platform (GCP):** Despite maintaining a steady market share of 11%, Google stands out among its competitors by offering similar services alongside exceptional expertise in artificial intelligence and analytics.

Other players in the market that make up the rest of the market share are cloud vendors like Alibaba, IBM, Salesforce and many more.

Open-Source Cloud System

With the rising interest of open-source cloud solutions, many vendors have emerged on the market and successfully provided their services. Again, the three key players of open-source cloud systems will be introduced.

- **OpenStack:** The solution from OpenStack provides services for computing, storage and many other functionalities and is widely adopted by users from the open-source market. The OpenStack platform was developed by NASA (National Aeronautics and Space Administration) and is supported by many companies, mainly from the US. The code, used by NASA and Rackspace Cloud, is licenced under the Apache2 licence [SAE12].

- **Kubernetes:** Kubernetes, originally developed by Google, is known for its containerization capabilities. However, it also can be used for managing cloud infrastructure [Goo23].

- **CloudStack:** Apache CloudStack offers IaaS for private, public and hybrid cloud environments. With CloudStack, computing, storage and network resources can be managed. Apart from its own API’s, Apache Cloud Stack also supports the API’s from AWS [KJM+14].

4 Critical Evaluation

In the following chapter the advantages and disadvantages of proprietary and open-source cloud systems will be discussed. Subsequently, an informed recommendation will be given.

Proprietary Cloud System

As we have seen in the comparison, proprietary cloud systems feature lots of capabilities that are tailored to the users' needs. Nevertheless, the identified disadvantages also need to be considered.

The biggest asset for the user when operating with proprietary cloud systems is the service and the support from the vendor. He will make sure that the newest updates will be installed, patches will be done frequently, and bugs and other issues will be fixed by professional employees without any individual work. This tailored support, that is offered by the vendor, can reduce risk for the user and makes handling business more smoothly.

However, this leads to an enormous dependency on the vendor where the whole data management is influenced by the handling of the vendor. As a user, one is not able to view the source code and therefore cannot make any alterations regarding customization, security or other aspects of the cloud system. Additionally, customers experience the vendor-lock in. That means that someone is not able to change systems or integrate other services from independent vendors without having to deal with high switching costs or other constraints.

Ultimately, the users need to pay regular licencing fees in order to use the provided cloud system. The fees may be accompanied by charges for any additional feature that is needed by the user. This concludes that using a proprietary cloud system can be fairly expensive.

Open-Source Cloud System

Compared to proprietary cloud systems, the user is able to view the source code. This comes with many advantages. Firstly, the vendor-lock in can be prevented. When utilizing open-source cloud system services any vendor can be used. This

also improves interoperability tremendously not only within open-source cloud systems but also between proprietary and open-source cloud systems.

Due to the fact that the source code is open, any individual can fix any upcoming issues within relatively little time. This is based on the fact that the source code is examined by multiple people leading to a very high probability that issues can be detected. The inspection is done by the open-source community who mainly communicates over online blogs. Owing to the fact that everybody is able to view the code and there is an existing online community with thousands of members, immediate support can be given. Additionally, the support is free of charge.

However, using open-source cloud systems can also have its downsides. For example, when talking about support, there is no fixed promise that correct and immediate support can be given. Additionally, every fix needs to be implemented by the user itself. This results in higher complexity and requires strong technical expertise especially in the programming field.

On the balance, therefore, using open-source cloud systems offers more advantages than the utilization of proprietary cloud systems. There is much more flexibility for the user, not only for customization but also for ensuring security, innovation and interoperability. Furthermore, the costs are significantly lower since no licencing fees need to be paid to the vendor. Due to the existing open-source online community, support can be given as efficiently as with proprietary cloud systems, leading to effective solutions for the user. Another fact that needs to be considered is that there are several existing open-source alternatives to proprietary cloud systems that can be utilized by users. This leads to a high degree of freedom when choosing vendors and impedes the vendor lock-in.

5 Development Trends for the Future

Undoubtedly, there will be a continuation of rapid growth with cloud computing services. Therefore, both proprietary and open-source cloud systems are subject to further development in the future.

Artificial Intelligence

According to Forbes [Mar21] cloud computing will further accelerate the usage of artificial intelligence (AI) and vice versa. The advantage of integrating AI in cloud systems is that they have the ability to evolve over time and therefore provide advanced data processing. Furthermore, the impressive capability of AI analytics within cloud systems will result in growing cloud-based AI services from June 2023 onward. That being said, cloud vendors will include AI in their services and will play a key role in delivering these services while also setting up the infrastructure to use it. With pre-built AI services, the vendors will make sure that users can have access to AI functionalities. The experience with Chat GPT shows that cloud services have found and will find a way in the future to integrate AI technologies to add additional value. Machine learning (ML) also plays an essential part since every technology that routes data traffic from data centers to our devices is built on it.

Serverless Computing

A new trend within cloud computing is serverless computing that may completely change our perception of hosting services. Of course, it is not really serverless, but another layer of abstraction is added between the platform and the user resulting in no involvement with configuration or other technicalities [Mar21]. By utilizing serverless computing the overall costs of deployment can be dramatically reduced since resources are only charged when the certain code is executed [Ana23].

Multi- and Hybrid Cloud

The future of cloud will not be only public or private cloud. Users are rather seeking to find the right balance between flexibility, security and other aspects. Therefore, multi- and hybrid cloud environments will become the norm. Proprietary cloud vendors have recognized this market need. Consequently, they are developing tools that facilitate the integration of different cloud platforms. Additionally, open-

source cloud vendors are driving initiatives to further support interoperability between existing cloud providers. Especially OpenStack is striving to provide an environment with vendor neutrality.

Green and Sustainable Cloud Computing

The growing environmental concerns also came to the attention of tech giants. Especially when looking at the produced carbon emissions of cloud computing, there will be an increased focus on green cloud computing practices. Cloud vendors will further invest in renewable energy sources to make their date centers more energy efficient [Mar21].

Increased Regulation

Due to the fact that cloud computing is becoming ubiquitous, additional legal regulations will arise. Especially with the disharmony between the CLOUD Act and the European GDPR (see chapter 2.2) it is likely that further regulations are needed to protect the user's rights and integrity [Ana23].

6 Conclusion

With the rising interest of cloud computing and the offering of both proprietary and open-source cloud systems on the market, users have difficulties to find out which of them is a better fit.

By concluding a thorough comparison of different characteristics followed by a critical evaluation, it has been established that the usage of open-source cloud systems comes with more advantages for the user than the utilization of proprietary cloud systems. The comparison revealed that due the ability to view the source code, users have a much higher flexibility with open-source cloud systems. This applies to customization, security, innovation and also interoperability. Interoperability can be further enhanced due to the fact that there are numerous vendors on the market and all their cloud services can be combined by the user.

At this point it is also worth mentioning that the continuous development of open-source cloud systems until 2023 resulted in high-quality alternatives to proprietary cloud systems. Another aspect that underlines the quality and the effectiveness of open-source cloud systems is the existing online community. A 24/7 exchange over several internet blogs and websites enables users to reach out for support and other relevant questions. This support system helps users to make the best of their utilized cloud system with the help of fellow colleagues without any additional charges. Finally, another benefit of the utilization of open-source cloud systems is the fact that the costs are significantly lower compared to proprietary cloud systems. Besides individual costs for hardware infrastructure, no licencing fees need to be paid to the vendor.

Nevertheless, it should be emphasized that the choice between a proprietary and an open-source cloud system ultimately depends on the users unique requirements. Depending on the specific needs of the user, a proprietary cloud system may offer more advantages. However, users should note that the utilization of an open-source cloud system, which offers high value due to high flexibility and prevented vendor lock-in, is always an approving choice.

7 Bibliography

[Ana23] B. Anand. Cloud Computing Future: 12 Trends & Predicitions About Cloud. KnowledgeHut. https://www.knowledgehut.com/blog/cloud-computing/cloud-computing-future. Retrieved 30 May 2023.

[AOC11] F. Almeida, J. Oliveira, J. Cruz. Open Standards and Open Source: Enabling Interoperability. International Journal of Software Engineering & Applications. 2(1): 1-11.

[AWS23a] Anonym. Clarifying Lawful Overseas Use of Data (CLOUD) Act. AWS. https://aws.amazon.com/compliance/cloud-act/. Retrieved on 12 May 2023.

[AWS23b] Anonym. Start Building on AWS Today. AWS. https://aws.amazon.com/. Retrieved on 13 May 2023.

[Bai08] S. A. Baird. The Heterogeneous World of Proprietary and Open-Source Software. Electronic Commerce Research and Applications. (7)1: 232-238.

[BJJ10] S. Bhardwaj, L. Jain, S. Jain. Cloud Computing: A Study of Infrastructure as a Service (IaaS). International Journal of Engineering and Information Technology. 2(1): 60-63.

[Bre01] D. Bretthauer. Open Source Software: A History. University of Connecticut. 2001.

[BSI23] Anonym. Cloud Computing Grundlagen. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html. Retrieved on 13 April 2023.

[Chi16] R. Chima. Cloud Security – Who Owns The Data? Blueberry Consultants. https://www.bbconsult.co.uk/blog/cloud-security-who-owns-the-data/. Retrieved on 12 May 2023.

[Clo23] Anonym. Was ist eine Public/Private Cloud? Cloudflare. https://www.cloudflare.com/de-de/learning/cloud/what-is-a-public-cloud/. Retrieved on 7 April 2023.

[Das18] J. Daskal. Microsoft Ireland, the CLOUD Act, and International Lawamaking 2.0. Stanford Law Review. (71). 2018.

[DB14] J. Daryapurkar, K. Badge. Cloud Computing: Issues and Challenges. International Journal on Recent and Innovation Trends in Computing and Communication. 2(4): 770-773.

[FRR+18] M. Fagundez, C. Romero, P. Ricardo, X. Juanola. A literature review about the difference in security for open source and proprietary source software - And its influence in Open Science. Universitat Pompeu Fabra. 2018.

[Ger21] T. Gerlinger. Open Source statt US Cloud Act. IT-Zoom. https://www.it-zoom.de/it-mittelstand/e/open-source-statt-us-cloud-act-27533/. Retrieved in 12 May 2023.

[Goo23] Anonym. Was ist Kubernetes? Google Cloud. https://cloud.google.com/learn/what-is-kubernetes? . Retrieved on 13 May 2023.

[IBM23] Anonym. What is cloud computing?. IBM. https://www.ibm.com/topics/cloud-computing. Retrieved on 6 April 2023.

[KJM+14] R. Kumar, K. Jain, H. Maharwal, N. Jain, A. Dadhich. Apache Cloud Stack: Open Source Infrastructure as a Service Cloud Computing Platform. 1(2): 111-116.

[MAR21] B. Marr. The 5 Biggest Cloud Computing Trends in 2022. Forbes. https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/. Retrieved on 28 May 2023.

[MIC21] Anonym. Im Daten-Dschungel: Wie Microsoft mit dem CLOUD Act umgeht. Microsoft. https://news.microsoft.com/de-de/im-

daten-dschungel-wie-microsoft-mit-dem-cloud-act-umgeht/. Retrieved 20 April 2023.

[Mic23] Anonym. Microsoft Azure. https://azure.microsoft.com/de-de/. Retrieved on 13 May 2023.

[MR21] B. Murphy, M. Rocchi. Ethics in Cloud Computing. In Data Privacy and Trust in Cloud Computing. Palgrave Macmillan. 105-128. 2021.

[MT11] P. Mell, T. Grance. The NIST Definition of Cloud Computing. Information Technology Laboratory. https://csrc.nist.gov/publications/detail/sp/800-145/final. Retrieved on 17 April 2023.

[Mün13] J. Münch. Cloud Based Software Engineering: Proceedings of the Seminar No. 58312107. University of Helsinki. 2013.

[Nie12] J. Nielsen. Usability 101: Introduction to Usability. Nielsen Norman Group. https://www.nngroup.com/articles/usability-101-introduction-to-usability. Retrieved 09.05.2023.

[NTY01] D. Nichols, K. Thomson, S. Yeates. Usability and open-source software development. University of Waikato. 2001.

[OST16] J. Opara-Martins, R. Sahandi, F. Tian. Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. Journal of Cloud Computing: Advances, Systems and Applications. 5(4): 1-18.

[PK13] N. Pankaja, M. PK. Proprietary Software versus Open Source Software for Education. University of Mysore. 2013.

[Roj20] M. Rojszczak. CLOUD act agreements from an EU perspective. Computer Law & Security Review. (38): 1-6.

[SAE12] O. Sefraoui, M. Aissaoui, M. Eleuldj. OpenStack: Toward an Open-Source Solution for Cloud Computing. International Journal of Computer Applications. (55): 38-42.

[SBJ15] A. Singh, R.K. Bansal, N. Jha. Open Source Software vs Proprietary Software. International Journal of Computer Applications. 114(18): 26-31.

[Syn23] Anonym. Cloud Spending Growth Rate Slows But Q4 Still Up By $10 Billion from 2021; Microsoft Gains Market Share. https://www.srgresearch.com/articles/cloud-spending-growth-rate-slows-but-q4-still-up-by-10-billion-from-2021-microsoft-gains-market-share. Retrieved on 13 May 2023.

[ZPS14] I. Zarko, K. Pripuzic, M. Serrano. Interoperability and Open-Source Solutions for the Internet of Things. Springer. Split/Croatia. 2014.

8 Table of Figures

Figure 1: Public Cloud [Clo23] 3
Figure 2: Private Cloud [Clo23] 3
Figure 3: Open-Source Software Licences [AOC11] 8
Figure 4: Data Privacy & CLOUD Act – AWS [AWS23a] 22
Figure 5: Cloud Vendors Market Share 2017-2022 [Syn23] 24