

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,500

Open access books available

176,000

International authors and editors

190M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)



Chapter

# Perspective Chapter: Cloud Lock-in Parameters – Service Adoption and Migration

*Justice Opara-Martins*

## Abstract

ICT has been lauded as being revolutionised by cloud computing, which relieves businesses of having to make significant capital investments in ICT while allowing them to connect to incredibly potent computing capabilities over the network. Organisations adopt cloud computing as a way to solve business problems, not technical problems. As such, organisations across Europe are eagerly embracing cloud computing in their operating environments. Understanding cloud lock-in parameters is essential for supporting inter-cloud cooperation and seamless information and data exchange. Achieving vendor-neutral cloud services is a fundamental requirement and a necessary strategy to be fulfilled in order to enable portability. This chapter highlights technical advancements that contribute to the interoperable migration of services in the heterogeneous cloud environment. A set of guidelines and good practices were also collected and discussed, thus providing strategies on how lock-in can be mitigated. Moreover, this chapter provides some recommendations for moving forward with cloud computing adoption. To make sure the migration and integration between on-premise and cloud happen with minimal disruption to business and results in maximum sustainable cost benefit, the chapter's contribution is also designed to provide new knowledge and greater depth to support organisations around the world to make informed decisions.

**Keywords:** vendor lock-in, security, ICT, cloud computing, parallel computing, IaC, Kubernetes, micro-services, terraform, Kotlin

## 1. Introduction

Cloud computing is a ubiquitous model for enabling network users' on-demand access to a shared pool of configurable computing resources that can be rapidly provisioned and released to the client without direct service provider interaction [1]. A cloud service provider is a party that makes cloud services available. Cloud computing technology is a new solution giving users the option to access software and information and communication technology (ICT) resources with the desired flexibility and modularity and at very competitive prices. In 2010, 80% of the US economy was driven by the service industry. But while there is more flexibility available in the cloud, there is a risk you can become dependent on the products and services from particular providers.

Cloud computing benefits the service industry the most and advances business computing with a new paradigm. As pointed out by Brynjolfsson et al. [2], the real strength of cloud computing is that it is a catalyst for more innovation. To assist corporations to adopt cloud computing services, Sahandi et al. [3] affirm that much research on cloud computing has concentrated on two broad areas: (i) business agility and (ii) catalysts for more innovation. The focus of this writing is to study both high-performance computing (HPC) for scientific computing and high-throughput computing (HTC) systems for business computing. Although many of the concepts do not appear to be new, the real innovation of cloud computing lies in the way it provides computing services to customers [3]. Further, this research examines clusters, massively parallel processors (MPP), grids, peer-to-peer (P2P) networks and internet clouds. These systems are distinguished by their platform architectures, operating system (OS) platforms, processing algorithms, communication protocols, security demands and service models applied. The study emphasises scalability, performance, availability, security, energy-efficiency, workload outsourcing, data centre protection, etc. The surge of interest when installing virtual machines (VMs) has widened the scope of system applications and upgraded computer performance and efficiency in recent years. An internet cloud of resources can be either a centralised or a distributed computing system. Cloud computing architecture relies on virtualisation techniques that create multiple virtual environments [3]. Parallel, distributed or both types of computing are used in the cloud. Clouds can be constructed using real or virtualised resources over sizeable, distributed or centralised data centres. A sort of utility computing or service computing, according to some authors [4, 5], is cloud computing. Cloud computing is used to equip virtual machines as central storage and processors to avoid ICT equipment costs in organisations or homes.

For example, using a cloud provider to manage your storage lifecycle might lead to lock-in, and it will reduce the work required to manage your service. Accepting some lock-in brings advantages that seem counter-intuitive, but one should balance this benefit of cloud lock-in against potential risks, so one can get the best value and reduce the burden of future legacy technology. By designing them as virtual resources over automated hardware, databases, user interfaces and application environments, clouds hope to power the next generation of data centres. In this way, the ambition to create better data centres through automated provisioning gives rise to clouds. ICT infrastructure is now shifting from locally managed software-enabled platforms and physical hardware to outsourced virtual infrastructure managed by cloud service providers [6]. But risks concerning security, privacy, financial aspects and the wider organisation are vital and require serious consideration before a cloud migration. In order to efficiently come to the correct decision about cloud migration with respect to business needs (as per lock-in avoidance), an organisation should be able to objectively consider the aggregated risks of cloud adoption. According to Khajeh-Hosseini et al. [7], it is emphasised that there is a need for guidelines and decision support tools for enterprises that are considering migrating their ICT systems to the cloud. The necessity of a comprehensive migration framework to support organisations through the migration decision cannot be overemphasised [8]. The process of cloud migration is therefore a complex undertaking, depending on many factors that contribute both for and against a decision to migrate.

Cloud technology has resulted in a variety of implementations and solutions where each vendor defines their own interfaces and approaches for similar products and services, which has resulted in heterogeneity application platform infrastructure (APIs) and libraries. These APIs complicate integration efforts for companies of all sizes and locations as they struggle to understand and then manage these unique

application interfaces in an interoperable way, and integrate applications from cloud to cloud and cloud to on-premise systems [9]. The concept of cloud computing has evolved from cluster, grid and utility computing. Cluster and grid computing leverage the use of many computers in parallel to solve problems of any size. In order to offer a wide variety of services to end users, cloud computing makes use of dynamic resources. A big data centre or server farm serves as the infrastructure in the cloud computing high-throughput computing (HTC) paradigm. Through a linked device, users can share access to resources at any time and from any location thanks to the cloud model. According to Foster et al. [10], cloud computing leverages multitasking to achieve higher throughput by serving heterogeneous applications, large or small, simultaneously. From another perspective, the cloud computing environment assigns due importance to good governance and the integrity of systems and data. While research confirms the widespread adoption and usage of cloud computing services across enterprises, arguably it should be said primarily of cloud computing as a business phenomenon rather than a technological one [11]. Moreover, a corporation can benefit from cloud computing in two different ways: directly through lower expenses and indirectly by being able to concentrate more emphasis on key business tasks. Cloud computing is a promising endeavour with the potential to offer financial benefits to an organisation [12].

The rest of this chapter is structured as follows. Section 2 reviews the state of the art in the domain of cloud computing lock-in solutions. Through this review, a set of guidelines are extracted that a vendor-neutral cloud service should follow in order to mitigate lock-in risks. Section 3 introduces parameters and discusses its core dimensions. Section 4 confirms the set of guidelines to follow for a successful intra-cloud migration with low switching costs (customizability). Section 5 summarises good practices and guidelines for building a standardised infrastructure, portable data structures and interoperable platforms. Finally, Section 6 concludes this chapter by discussing the research findings and future work.

## **2. Related work**

In the study by Opara-Martins [8], the author has shown that the complexity of vendor lock-in that exists in the cloud environment, with the complexity of service offerings, makes it imperative for businesses to use a clear and well-understood decision process to procure, migrate and/or discontinue cloud services. Some of the existing cloud solutions for public and private companies are vendor locked-in by design, and their existence is subject to limited interoperate with other cloud systems [13]. There are several works that highlight vendor lock-in as a concern for cloud adoption and migration. The goal of this research is to gain a comprehensive understanding of the type of solution and motivation driving widespread adoption of cloud computing across institutions, enterprises and government parastatals. The approach of cloud computing is practical due to the combination of security features and online services. Cloud computing continues to be one of the most vital and fast-growing models of ICT. Researchers and practitioners have been actively reporting solutions and motivation with this new technology. The use of a specific cloud service during an application design may affect its maintenance and forthcoming migration requirements. The effort required to migrate an application from one cloud environment to another varies depending on the particular cloud service that it consumes. Any organisation that is considering the adoption of cloud services must start by identifying the



type of cloud service components it intends to take advantage of before starting plans for integration with existing enterprise networks. Therefore, enterprises' capability to ease switchability between cloud providers without any lock-in effect is important for its decision-making regarding service model adoption [14].

Prior to adopting cloud computing services, organisations must fully understand the impact they will have on existing business processes. The cloud service agreement is a documented agreement between the cloud service provider and cloud service customer that governs the covered services, while the cloud service level agreement is a part of the cloud service agreement that includes cloud service level objectives (i.e. commitment a cloud service provider makes for specific, quantitative characteristics of a cloud service. Where the value follows the interval scale or ratio scale) and cloud service qualitative objectives for the covered cloud service(s). Cloud service qualitative objective is the commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the interval scale or ordinal scale. Therefore, a service level agreement (SLA) is a critical part of any service-oriented vendor contract. An SLA serves as an intermediary between the cloud service provider and a client organisation, while a cloud service broker is a service between cloud service customers and cloud service providers, in which the cloud service broker arbitrates, delivers and manages the cloud services from cloud service providers to cloud service customers. The SLA management is involved during the establishment of a cloud service agreement and manages cloud SLA by monitoring cloud services for cloud service level objective to verify the service level, by detecting failures to meet the terms of the cloud SLA through monitoring and by providing agreed remedies for failures to meet the terms of the cloud SLA. Cloud computing has the potential to transform a large part of the ICT industry, making software even more attractive as a service and shaping the way ICT hardware is designed and purchased. Cloud services exist under a shared security environment and both cloud service providers and users contribute to the overall security [15]. Thus, a less secure cloud service provider can lock-in users by providing the means for creating value within the security umbrella. Cloud computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and services availability and demonstrate compliance.

A cloud computing system typically consists of the following components: data, applications, platforms and infrastructure. Data are the machine-processable representation of information stored in computer storage. Applications are computer programs that carry out tasks associated with solving business issues. Platforms are computer programs that enable applications and carry out generic, non-business-related tasks. Physical resources for processing, storage and communication make up the infrastructure. A data model that specifies the data's structure and includes meta-data that the application can use to interpret elements of the data is the application data. Therefore, unless an application is standalone, the effort is needed to integrate it into a system. The degree of interoperability of an application can be measured as its cost of integration. Hence, understanding the theoretical framework described in this study is an important first step in understanding the remainder of the cloud lock-in parameters. Overall, a detailed understanding of these areas is required in the research field in order to make the correct decisions concerning cloud migration.

The research approach used in this study is mixed methods. Opara-Martins [8] carried out a study on cloud vendor lock-in from 2012 to 2016. In the survey, technical experts from a wide range of organisations were asked about their use of cloud

computing. The 114 business respondents, who represent organisations of various sizes in numerous industry verticals, include technical executives, managers and practitioners. Respondents are firms from a wide range of cloud-related industries, including both providers and consumers of cloud lock-in solutions. The survey also shows that as computing resources move from on-premise to the cloud environment, aspects like a contract (also referred to as commercial) lock-in are exacerbated to further complicate decision-making for/against cloud adoption. Specifically, in this work [16], the author(s) discussed a number of technical and organisational factors that should be taken into account in order to assist businesses in enhancing their security posture, identifying and mitigating privacy-specific controls, and maintaining the flexibility to easily switch cloud providers (i.e., avoid lock-in), we will talk about a number of technical and organisational factors worth taking into consideration. This will increase ICT agility and business continuity. Their answers provide a comprehensive perspective on the state of the cloud today. The next section takes an unusual approach to further this study, whereas the subsections discuss the background and motivation for this study.

## 2.1 Background

Vendor lock-in is a topic of intense discussion in the ICT industry, and the general business community is now paying more attention to it. On the one hand, those who support open-source technology highlight the avoidance of vendor lock-in as a fundamental benefit. On the other hand, there are cloud service providers and suppliers of proprietary software who claim that vendor lock-in is nothing to worry about. Vendor lock-in has, according to some, always existed, and they are right. You will essentially be 'locked in' to the data centre operator, the hardware provider and, in the end, your engineer who operates and maintains it, even if you employ an engineer to create a specific solution internally. Any modification to such components will raise risks, extend project duration and raise costs. You might call this a lock-in. A growing problem is locating existing tools or adopting new ones that can lessen the effects of vendor lock-in. According to Satzger et al. [17], there are three types of solutions that have been suggested to mitigate vendor lock-in for the cloud, namely: (i) standards [18]; (ii) abstraction layers and adapters [19] and (iii) reducing accidental complexity, by adopting semantics and model-based solutions [20]. Based on these assertions, the chapter's contribution is also intended to provide new knowledge and greater depth to support organisations around the world in making informed decisions, ensuring that the migration and integration between on-premise and cloud happen with minimal disruption to business and results in maximum sustainable cost benefit.

## 2.2 Motivation

Fear of vendor lock-in is one of the main motivators for a multi-cloud strategy. When a consumer is 'locked in' to a single vendor for goods and services, it signifies that transferring to another vendor would be prohibitively expensive or disruptive to operations. Going all-in with a single vendor may enable you to streamline processes, increase your agility and maybe improve quality as single-vendor solutions are frequently better integrated. So, even while vendor lock-in has advantages in a perfect world, there is a serious potential for exorbitant expenditures. There are other issues as well, the technology you adore may be placed on hold or eliminated entirely when you are locked in since you are totally dependent on your vendor to drive innovation. This is particularly risky in our current 'as a service' world, when providers can decide

to discontinue their product at any time, leaving you with few options and no time to transfer. Although utilising a single cloud provider plainly results in some dependence, you can migrate your data to any environment of your choice and only pay for the services you use. Therefore, your applications should be created or moved to be as flexible and loosely connected as possible to reduce the danger of vendor lock-in. The application components that communicate with cloud application components should be loosely coupled to them. Adopt a multi-cloud strategy as well. Consider putting the majority of your workloads in one cloud and the rest in another if your business requires the use of many vendors and the ensuing complexity is worth it. This will guarantee that you get some experience without suffering any negative effects. Additionally, if possible, employ automation to streamline processes and ensure consistency as later discussed in this chapter.

### **3. Systematic initial review**

The author has carried out a systematic initial review (SIR) of the existing literature regarding cloud lock-in, not only in order to summarise the existing solutions and motivations concerning this area of specialty but also to identify and analyse the current state and the most important areas for cloud computing. The aim of the SIR is to identify and relate gaps in knowledge as it pertains to cloud lock-in with possible solutions for the advancement of this knowledge domain.

Understanding what lock-in parameters are in cloud computing will help organisations to make the shift towards the cloud since it leverages many technologies and it also inherits their heterogeneous features. As described in this chapter, storage, applications, data, virtualisation and networks are the largest lock-in areas in cloud computing. Providers, end users and developers should consider the lock-in areas to take good advantage of the cloud. It is also essential to analyse compatibility issues such as database schema semantics and data types of the database so that there are no inconsistencies between the database layer before and after cloud migration.

Requirements for open, interoperable standards for cloud management interfaces and protocols, data and data formats will develop as more businesses create cloud adoption strategies and execution plans. As a result, cloud service providers will be under pressure to base their offerings on open, interoperable standards in order to be given serious consideration by businesses. Cloud computing promises to make switching to a different provider quick and easy, but that is only possible if users are careful to avoid provider lock-in. The reason because standards influence choice and choice influences the market, standard-based cloud services are essential for the development and dissemination of this paradigm. Third-party suppliers will be allowed to create and provide value-added management capabilities in the form of separate cloud management solutions in the presence of standards-based cloud offers. Vendors who already have ICT management tools available on the market would leverage such products to manage cloud solutions and hybrid cloud deployment. Due to the heterogeneity of the runtime environments, there are extra compatibility concerns when creating hybrid clouds based on legacy hardware and virtual public infrastructure. The X86 machine mode is supported by hypervisors, which can be a technical hurdle to a seamless transfer from private to public contexts.

In cloud lock-in conditions, a big installed base of a client is kept within the virtual infrastructure of one vendor, who does not reveal the intervals of their system, preventing the customer from shifting their installed base to another provider without

incurring a significant fee. The cloud service customer is a party that is in the business relationship for the purpose of using cloud services. Since most cloud offerings are proprietary, customers adopting the according services or adapting their respective applications to those environments are explicitly bound to the respective provider and other necessary parameters to support the migration. The amount of work a user is willing to put into transferring their skills to another environment, which typically involves reprogramming the corresponding programs limits their ability to move between providers. This makes the user dependent on both the provider's success and failure, as leaning too much on a single source might have major negative effects on service use [21]. In this respect, dependency, lock-in, privacy and security have been identified as a hurdle to cloud computing in companies and have been discussed in subsequent sections. The next subsection details the pragmatic approach used in this study.

### 3.1 Philosophical approach

Adopting cloud computing is a complex decision involving many factors [12]. Although cloud-based offers are proliferating on the web and there is competition among cloud computing services, the rules and standards governing cloud computing are insufficient to provide customers with conditions of use ensuring that they will not experience lock-in situations or dependency with regard to the cloud computing providers. In fact, a client or another provider cannot always use the data formats and application interfaces used by a cloud computing service. Similarly, users want to be able to recover their data whenever they wish, without distortion or loss. Also, when it comes to recovering disputed data, the laws in the region where the data are physically located may present difficulties (act). All of these factors highlight the need for rules and standards that enable the interoperability and reversibility of the cloud computing ecosystem. The long-term development of cloud computing depends on this. Here again, it is evident that circumstances change, however, and as they become complex the simplifications can fail. However, this does not automatically imply that all new economic models brought about by cloud computing, whether for cloud service providers or for cloud service users, systematically guarantee significant financial gains. Due to the complexity of the cloud computing model, as it has been presently proposed, various outcomes of the corresponding economic analyses regarding the costs and benefits associated with adopting a cloud computing model have been found. This chapter is based on the *CYNEFIN* (pronounced ku-nev-in) framework, which allows executives to see things from new viewpoints, assimilate complex concepts, and address real-world problems and opportunities. The framework divides the problems that leaders face into five contexts based on how cause and effect relationships differ: four of these simple, complicated, complex and chaotic-demand that leaders analyse circumstances and take necessary action. When it is difficult to determine which of the other four contexts is dominating, the fifth context disorder applies [22].

Executives can avoid problems that arise when their preferred management style causes them to make poor decisions by using the *CYNEFIN* framework to help them to identify the context in which they are operating. The author's focus in this chapter is on the fifth context since the disorder is not uncommon in the cloud computing business world and this writing concentrates particularly on that context. Moreover, leaders who understand that the world is often irrational and unpredictable will find the *CYNEFIN* framework particularly useful and disorder makes it difficult to



recognise when one is in it. Effective leaders learn to shift their decision-making to match changing business environments.

Cloud environments provide a powerful and flexible computing option for many researchers. Now is the time for organisations and institutions to reassess, and in many cases, readjust their approaches to take full advantage of the agility, speed, scalability and availability of the cloud at a time when such capabilities are more important than ever. So when you look at cloud computing through an ethicist's eye, an economist's eye or with a policy dimension the impact of the decisions, we take now will have economic and societal impacts for generations to come [23]. In the following section, author will demystify the cloud paradigm with substantial evidence and undeniable facts.

#### **4. What is in the 'Cloud'**

The survey report conducted by Sahandi et al. [3] revealed that 25.1% of participants were not sure about the term cloud computing; therefore, this section fills in this gap by providing substantial evidence on what the 'cloud' literally means. This is important because the increase of cloud computing understanding is expected to accelerate cloud adoption by enterprises. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. Cloud computing, more specifically, refers to the use of a set of services, applications, information and infrastructure made up of pools of compute, network, information and storage resources that can be quickly orchestrated, provisioned, implemented and decommissioned, as well as scaled up or down, enabling on-demand utility-like (as in electricity) models of allocation and consumption. More discussion, from the standpoint of the introduction, is focused on how the cloud differs from and is similar to the current computing models, as well as how these similarities and differences affect organisational, operational and technological approaches to network and information security practices. The keys to understanding how cloud architecture affects lock-in parameters are a common, succinct vocabulary, along with a consistent taxonomy [24], of offerings, by which cloud services and architecture can be dissected, mapped to a method of compensating security and operational controls, risk assessment and management frameworks and ultimately to business process compliance standards. Cloud is usually the preferred option when organisations procure new ICT services, as reflected in the UK government's cloud first policy. Against this background, it is essential that new services are chosen and built in a way that reflects their security needs. The European Council (EC) has pushed cloud computing because it may make cutting-edge software and services affordable for SMEs and other customers, driving the digitalisation of society and the economy. The US National Institute for Standards and Technology's (NIST) most official explanation of the cloud model explains why cloud computing is often likened to a utility model, similar to electricity or gas distribution. However, the cloud model is also widely used by universities and research centres for scientific computing and by governments for online public services. As companies continue to pursue the cloud for data processing needs, cloud data centres are becoming the new enterprise data repository. CSA [25] report suggests that consumers' understanding of the cloud has matured and signals a technology landscape where consumers are actively considering cloud migration.

The cloud is a service from the user's point of view. However, the architecture for cloud service providers, integrators and channel partners who build or construct the

cloud is made up of numerous cloud computing components. Hypervisors, cloud operating system components and other such cloud components are examples of, virtual desktop infrastructure platforms, cloud dedicated firewalls, etc. The most basic cloud computing is the operating system (OS). Through the utilisation of virtualisation technology, cloud OS virtualised hardware resources of physical servers and storage area network devices and supported software-defined networking. Cloud OS enhances the performance and security of cloud computing systems as well as the user experience of administrators and users. Cloud is a primary accelerator of innovation. As pointed out in ITU [26], understanding the emerging trend in ICT services known as cloud computing is a requirement for businesses to successfully utilise it and all of its advantages. Before implementing the cloud concept, it is frequently necessary to obtain specialised knowledge in the areas of data centre administration and commercial interactions.

Cloud simplifies rapid application development, allowing resources to scale on demand with flexible, consumption-based billing models. Migrating to the cloud also allows enterprises to implement turnkey solutions that use consistent processes and protocols while ensuring regulatory and business process compliance. Despite the benefits of the cloud, any change brings new risks. Ultimately, cloud services offer organisations and research institutes security protection beyond anything an individual agency could deliver in-house. Although the cloud may be secure in and of itself, it is still the organisation's job to ensure the security of applications developed and deployed to production in the cloud. Because there are many different types of code and application building blocks to secure while developing cloud-native applications, application security safeguards enterprise data. When working with cloud products and services, the remaining section of this chapter is aimed at providing businesses with recommendations on how to best achieve portability and interoperability. As cloud standards customer council [27] concurs that the lack of portability and interoperability between components of cloud solutions could mean that the potential business benefits of cloud computing are not met.

Cloud computing is one of the enablers of the European Commission Digital Strategy (ECDS) transformation [28]. The European Commission (EC) has promoted cloud computing towards companies and public administrations alike since the adoption of the first European cloud computing strategy in 2012. Cloud first with a secure hybrid multi-cloud service offering is the EC's vision for cloud computing. The cloud first approach implies that any development should preferably be cloud-native, and existing information systems would be reassessed for transformation, rewiring or replacement within the context of the modernisation plans foreseen by the ECDS, setting the opportunities arising in the business and application lifecycle. Cloud computing relies on the sharing of resources to achieve coherence and economies of scale, similar to a public utility. The international market for cloud services has led to the development of a new paradigm for transformational programming in which cloud-native information systems are constructed without reference to the underlying ICT infrastructure on top of a variety of cloud-based services. Code written at a much higher abstraction level results in a large reduction in the amount of code required to achieve the same functionality. This reduced code base enables faster rewrites to adapt to changes, boosts agility, lowers operational costs and requires less maintenance work. All of this enables companies to focus on business issues rather than ICT issues. Besides, the real value of cloud computing can only be unlocked by moving information systems to a cloud-native development pattern. ICT teams must start employing agile and cloud-native development practices such as DevSecOps and design systems

according to modern data-centric architectures supporting the consumption of loosely-coupled micro-services. Cloud systems should be conceived in such a way that they can benefit from the advantages of cloud-based delivery models regardless of whether the data or processing capabilities are on-premise or in the public cloud.

Cloud services must be designed and operated according to security best practices. The designers of new information systems would only be able to use a limited number of services if they tied an organisation to a single cloud provider. In order to avoid being dependent on a single public cloud provider, the organisation should opt for a multi-cloud strategy. As a result, the cloud service consumer organisation will, in a vendor-neutral manner, obtain ICT services from the cloud provider that is best suited for the services required, depending on the use case. The secure and safe usage of cloud services is intrinsically linked to an appropriate data classification for all data assets of an information system. Moreover, one of the most relevant factors for the success of the cloud is the ability to enable a modern way of managing Big Data. Cloud-based data services and solutions to manage the high volume of data and data operations are key elements for shaping the organisation of tomorrow. The usage of vendor-specific advanced cloud services increases the risk of lock-in with one particular cloud supplier. Such a situation is not inevitable though, but the switchability of one cloud provider to another one should just be a refactoring cycle away. Information systems that are cloud-native are always designed and built with a certain cloud platform in mind. The information system may be created in ways that make it difficult for portability and reusability in order to get the most out of the chosen cloud platform. This may result in a situation known as vendor lock-in, in which data or information systems are dependent on a single provider and are immobile [29]. The council recognises that one of the crucial elements for guaranteeing the stability and security of the internal market is avoiding vendor lock-in and diversifying ICT suppliers. Emphasises the importance of advocating for and putting into practice suitable measures that support vendor diversity and competitiveness in a way that is technology-neutral, further supports including provisions relating to preventing vendor lock-in in EU legislation. Accepts the proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), which aims to improve the interoperability of data processing services and remove barriers to switching between providers of data processing services. The next subsection(s) will discuss the different cloud delivery mechanisms and service deployment models as well as emerging trends in these aspects.

#### **4.1 Service models**

The choice of service models is important because it will largely determine the types and effectiveness of security separation mechanisms that are available. However, this choice of service model will also affect the amount of responsibility that one has for securing your data and workloads within the service and how much responsibility the cloud provider will take on your behalf.

- Infrastructure as a Service (IaaS)—According to Sen [30], cloud infrastructure can be a real risk as each implementation choice affects future scalability, service level and flexibility of the services being built. It is fair to denote that ‘future-proofing’ should be the primary concern of every system architect. There are huge incentives for any vendor to increase lock-in through contractual, fiscal and technical constrictions. Interest in cloud infrastructure has been driven by a

huge urge to break free of the existing enterprise vendor relationships for which the lock-in costs are higher than the value provided. Resist lock-in mechanisms in areas such as long-term contractual commitments and pre-paid arrangements distort decision-making, although technical lock-in remains one of the most difficult to avoid. Additionally, many suppliers encase exclusive APIs in distinct services so that future applications might adopt their style. These ‘stick services’ or ‘loss leaders’ give IT businesses strong incentives to choose the fastest route to value and incur some lock-in risk. This is a common type of technological debt, especially as new vendors introduce products that are more potent and distinctive in the same market or as better solutions emerge from OSS community. In addition, proprietary APIs invite strategic disruption from cloud providers in order to preserve customer lock-in.

- Platform as a Service (PaaS)—platform for cloud computing service provision (customer service management, billing, etc.). The consumer is given the ability to upload programs they have developed themselves or purchased using the provider’s supported programming languages and tools into cloud infrastructure. The consumer has control over the installed programs and perhaps the parameters of the application hosting environment but does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems or storage.
- Software as a Service (SaaS)—business applications, customer relations and support (CRM), human resource (HR), finance (ERP), online payments, electronic marketplace (for very small- and medium-sized enterprises). The consumer does not manage or control the underlying infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration.
- Process as a Service for Business—Business Process Outsourcing as a Service (BPaaS) is the provision of BPO services that are derived from the cloud and designed for multi-tenancy. When human process actors are needed, services are frequently mechanised, so there is not a labour pool that is extensively devoted to each client. Commercial terms with consumption—or subscription-based pricing schemes are used in a cloud-based service. Access to the BPaaS paradigm is made possible by web-based technology.
- Communication as a Services (CaaS): unified communications, e-mail, instant messaging, video and audio communication, collaborative services and data sharing (web conference).
- Network as a Service (NaaS)—managed Internet (assured speed, availability, etc.), paired with virtual private networks (VPNs) and cloud computing services, flexible and on-demand capacity.
- Serverless blurs the line between PaaS and SaaS. What sets serverless apart is that each government solves just one functional problem so multiple components must be combined to build an application.
- Containers such as Docker are widely used to deploy applications in the cloud. Services that run customers’ containers tend to fit somewhere between the IaaS



and PaaS (which varies depending on your choice of service). Containerisation is the emerging virtualization technology to support more elastic service frameworks due to its flexibility and small resource footprint.

## **4.2 Deployment models**

When assessing the suitability of a given cloud service, you will need to decide on the service model and deployment you adopt. This is the essential first step towards determining whether the separation measures needed for your intended use are in place. For enterprises cloud computing provides access to agile, robust and scalable solutions. These could be in the form of SaaS products or IaaS products that allow enterprises to add or remove servers with ease as they are needed.

- **Public cloud**—To make the public cloud economically viable, cloud providers do not usually provide each customer with dedicated compute resources. Instead, resources such as compute power, networks, storage and identity management are shared between multiple clients. In this scenario, the separation implemented within each of those shared resources will affect the security of your deployed workloads and data. This makes it imperative you choose a cloud service provider whose separation techniques match your security needs.
- **Private cloud**—The cloud infrastructure is operated solely for a single organisation. It may be managed by an organisation or a third party and may exist on-premises or off-premises.
- **Hybrid cloud**: The cloud infrastructure is made up of two or more clouds (private, community or public), each of which is distinct from the others but which are connected by standardised or proprietary technology that enables the portability of data and applications (such as cloud bursting for load-balancing between clouds).
- **Community cloud**: The infrastructure is shared by a number of organisations, supporting a number of communities with similar issues (e.g. mission, security requirements, policy or compliance considerations). The organisations or a third party may administer it and may exist on-premises or off-premises.
- **Edge Computing**—Some public cloud providers offer the ability for users to deploy some of their services in their own data centre using hardware that is provided by them. This is known as edge computing and should be treated as a variant of the public cloud since its control plane (and sometimes its data plane) will be shared with the public cloud. You will need to have confidence that you can trust your physical data centre (and the network that you use to host the provided edge devices), as well as the cloud service that provided the device. Edge computing is usually deployed by organisations that require extremely low latency between client and service, to each data on sites where internet connectivity is unreliable, or to reduce internet bandwidth requirements by pre-processing raw data, prior to sending or derivation of the cloud.
- **Multi-cloud**—A multi-cloud strategy allows you to take advantage of more than one cloud service provider. Different cloud services may better meet the needs of

different projects so it is common for an organisation to choose to use more than one platform to get the benefits of each.

Having read and understood to a certain degree the impact of cloud computing on businesses and institutions, the remainder sections of this chapter is meant to contribute to a further understanding of the overarching lock-in parameters.

## 5. Understanding cloud lock-in

In Refs. [14, 24], the author(s) have addressed several misconceptions regarding the cloud computing lock-in effect for the widespread adoption of cloud services. Organisations must approach the cloud with the understanding that they have to change providers in the future. It is advisable to do business continuity planning, to help to minimise the impact of a worst-case scenario. Various businesses will in the future suddenly find themselves with urgent needs to switch cloud providers for varying reasons. Companies seeking to adopt DevOps practices like continuous integration (CI) could face cloud lock-in due to the complexity of the required tools and effort needed to integrate them into their workflows. Even those companies that have already transitioned to DevOps could encounter lock-in, as the environments and tools are changing fast and constantly [31]. In the study by Opara-Martins [16], the author believes vendor lock-in appears when software companies become dependent on the tools they are using, not being able to substitute them when they need to is an issue that relates to the flexibility that is incompatible with DevOps. García-Grao and Carrera [32] concur that the DevOps paradigm is taking over software development systems, helping businesses increase efficiency, accelerate production and adapt quickly to market changes. A report by the UK Government (2019) states that there are generally two different types of lock-in. Many organisations have experience with commercial lock-in where long and inflexible contracts with providers can prevent organisations from changing their technology strategy when circumstances change. The opposite is true for public cloud services, where providers frequently use rolling, pay-as-you-go agreements. Although technically speaking you are free to discontinue utilising their services at any moment, in practice, this can be challenging and is referred to as technological lock-in. The lack of comparable services from other providers, technical architecture that depends on doing things a certain way, excessive integration with provider-specific services or products, and a lack of technical architecture expertise within the organisation are the main causes of this.

The popularity and use of cloud computing have largely been driven by the reported benefits on firm performance [33]. In this chapter, the author confirms that cloud adoption decisions [16] are complex and therefore require creativity, seeing as managers are advised to consider mindfulness as a criterion for job selection [34]. While several initiatives have been taken to prevent vendor lock-in risks [16], federated access control policies and identity management are too important features to design and implement inter-cloud security solutions [35]. In contrast to the aforementioned, Oulaaffart et al. [36] stipulate that the stakeholder may be reluctant to share information related to security with each other. This is to show that inter-cloud migration efforts have thus far been faced with several major solutions in terms of interoperability and security management.

In that context, moving resources across different cloud providers still frequently involves high prices, legal restrictions or even voluntary incompatibilities in

technology, which promotes effective management of cloud resources [16]. But the integration of these resources and the development of cloud composite services depend heavily on the portability and interoperability qualities. The study by Opara-Martins [37] has been discussed by previous and recent researchers on the current state of the adoption process and associated effects of cloud computing by SMEs means they are very much interested because of the cost savings, flexibility and scalability of ICT that a cloud provides. SMEs have helped to take advantage of technology to facilitate and improve business [38]. Recently, cloud computing and application environments have evolved from monolithic to microservice architectures and platform support [39]. Cloud lock-in which is a user difficulty of switching from one vendor to another is regarded as one of the major motivations in the adoption of cloud by developers and SMEs [37]. Cloud computing offers good tools for organisations to conduct business efficiently.

Individuals and ICT organisations have begun to profit from cloud providers such as Amazon Web Services (AWS), Google cloud platform (GCP), Microsoft windows azure and others based on their demand for IaaS, PaaS and SaaS resources with pay-as-you-go pricing model. Cloud lock-in is now a well-known phenomenon [40, 41] in spite of its involvement with big automation companies. The proper deployment of novel methods can greatly reduce vendor lock-in. Although cloud provisioning has a dark side, it too often prioritises economic gain over the cost of long-lasting sustainability [42]. Moreover, vendor lock-in is economically unsustainable for cloud users because it makes it difficult for them to react if a provider does not deliver the promised service, reduces their bargaining power and even puts their company assets at risk in the event of data breach or cyberattack on the cloud provider's end [16]. To recall, the author reiterates here that cloud lock-in is characterised by a time-consuming procedure to migrate one application, data or service to another competitive cloud or establish communication among distinct cloud entities. Several solutions have been proposed to overcome lock-in situations, and middleware platforms are one of them [43]. The main solution identified in the composition of services for supporting the lifecycle of digital products is less dependency on services, infrastructure, platform, programming language or third-party services [16].

From the dimension of services computing, the cloud provides techniques for the construction, operation and management of large-scale internet service systems. It represents the frontier development direction of software engineering and distributed computing [44]. Due to the fact that cloud computing is built on many pre-existing technologies, hence to understand the complexities in cloud adoption, there are various factors such as knowledge management, technology interoperability, business operations, system integration, ICT infrastructure update, etc., that need to be considered during cloud computing adoption [45]. Likewise, there is a body of research that has general factors that influence the adoption of cloud-based services [46, 47], but these factors do not specifically address complexity dimensions [16]. Standards are a critical topic in the field of cloud computing [48] as they allow customers to compare among and evaluate cloud providers [49]. Proprietary technologies make cloud migration hard for end-users, and some providers note that standards to support interoperability between devices are needed [50]. As more applications make use of the cloud and more providers appear, vendor lock-in becomes an increasingly important factor.

The need for a common and interoperable standard is further augmented due to the appearance of Fog computing [51]. Lack of understanding of cloud technology and lack of confidence in cloud security are the major risks of applying cloud

solutions [52]. The quest for supremacy among major players enhances their unwillingness to settle for a universal standard and thus upholding their incompatible cloud standards and design configurations [53]. One of the main hurdles in the cloud adoption of data-intensive applications is the absence of mature data management solutions that address vendor lock-in [54]. The risk of vendor lock-in can occur in any public-private collaboration, yet ICT products trigger particularly strong lock-in effects as a vendor can create a monopoly position by closing its technologies. Dependencies make the process of changing cloud providers or even the collaboration of processes between different providers a very difficult task. However, cloud service providers may also offer non-compatible solutions with proprietary interfaces, complicating the cloud landscape [16].

Cost of migration, integration, interoperability and customisation needs are attributed to a lack of skills in the effective implementation and management of a cloud solution. In Ref. [55], vendor lock-in is addressed by multi-cloud resource management (MCRM). To support the MCRM and exhibit a suitable automation level, different cloud modelling languages (CMLs) have been identified in many research projects and prototypes. The adoption of cloud computing and its implementation depend upon a variety of technical and non-technical factors. Cloud computing and the services that cloud providers offer are expanding much beyond simply the bare minimum of computation, storage and networking. These larger capabilities include edge caches, workflow managers, functions-as-a-service microservices, database services on demand and a variety of additional capabilities that are located higher up in the system stack. A group of remote users may also share these features from several suppliers. At the software-as-a-service level, this may likewise be done for any arbitrary, application-level services. When working with heterogeneous clouds, synchronisation of access, capabilities and resources is crucial. A multi-cloud strategy is possible when standard exchange mechanisms are accessible for services.

Interoperability and portability for data systems, and services are crucial factors facing consumers in cloud adoption. Consumers need confidence in moving their data and services across multiple cloud environments. A cloud system is a collection of network-accessible computing resources that customers (i.e. cloud consumers) can access over a network. The cloud system and its consumers employ the client-server model, which means that consumers (the clients) send messages over a network to server computers which then perform work-in response to the messages received. Cloud computing requires consumers to give up (to providers) two important capabilities: (1) control—the ability to decide with high confidence and what is allowed to access consumer data and programs and the ability to perform actions have been taken and that no additional actions were taken that would subvert the consumers intent. (2) Visibility—the ability to monitor, with high confidence, the status of a consumer's data programs and how consumer data and programs are being accessed by others. In order to guarantee proper security and privacy protection, new problems in cloud design, construction and operation must be overcome. The implementation of the required controls turns into a collaborative effort between suppliers and consumers.

The ownership of the computing resources within a cloud is determined by cloud business models. Cloud service offerings that rent traditional computing resources (such as VMs or disk storage, i.e. IaaS) are closely related to existing standards, and hence, some usage scenarios illustrating portability can be expressed using existing standard terminology. Portability relies on standardised interfaces and data formats, while cloud computing relies on both consensus and *de facto* standards such as TCP/



IP, XML, WSDL, IA-64, X509, PEM, DNS, SSL/TLS, SOAP, ReST. Moreover, most substantial applications are using the Internet today regardless of whether cloud computing is employed. Therefore, the reader should not assume that by avoiding a cloud a user automatically avoids risks associated with Internet outages. Cloud systems have been conceptualised through a combination of software/hardware components and virtualisation technologies. Managing various sorts of access to the service components is necessary for various service delivery models. These service delivery approaches may be seen as hierarchical. As a result, the same functional components in a higher service model can use the access control guidance of functional components in a lower-level service model.

Cloud systems offer application services, data, storage, data management, networking and computing resources management to consumers over a network. Access control (AC) dictates the subject (i.e. users and processes) can access objects based on defined AC policies to protect sensitive data and critical computing objects in the cloud systems. Cloud interoperability has emerged as a crucial business concern as business use cloud-based solutions at an increasing rate. ICT departments are aware of the need of being able to use cloud metadata to guarantee data protection and data portability, giving end users a safe way to remove their data from the cloud. This is especially useful in the event that you want to switch cloud service providers or if one of them goes out of business. ICT departments, therefore, anticipate providers to adhere to cloud data interoperation standards.

The academic literature pinpoints two issues as the two most important determining factors in this respect, with security ranking first, and vendor lock-in (specifically in PaaS and SaaS context) second. The current business methods of cloud service providers obstruct innovation and a free and open market, which has an effect on how data is used throughout the economy. Particularly, users are now prevented from migrating from one provider to another by porting their digital assets across due to contractual, financial and technical barriers. Over the past 10 years, this vendor lock-in has grown significantly more severe. It is made worse by the current trend, in which providers are increasingly offering a variety of cloud services within an integrated cloud ecosystem, preventing customers from switching providers. Such ecosystems frequently devolve into ‘data-silos’ that hinder the adoption of cutting-edge data-sharing tools and the market’s open nature for data processing. Achieving data portability will depend on the standardisation of the import and export functionality of data and its adoption of “data acts” by the providers. The next subsection describes some obstacles encountered during service migration.

## **5.1 Cloud migration hurdles**

Advances in cloud computing have in recent years resulted in a growing interest for migration towards the cloud environment [16]. The transition to cloud computing frequently involves unforeseen, additional expenditures. While these costs are manageable and do not jeopardise the benefits of adopting cloud, some activities may prove to be quite expensive, especially if they are not planned for in a timely manner. The frequent movement of data between the company and the cloud can also rack up costs, particularly in terms of bandwidth consumption where transfer times are lengthy. As things currently stand, lock-in is a perceived risk that there is more flexibility available in the cloud and users can become dependent on the products and services from a particular provider. In this case, switching from one technology or provider to another is difficult, time-consuming and disproportionately expensive. In

the cloud, the benefits of lock-in frequently outweigh the drawbacks. Using a cloud provider, for instance, to handle your storage lifecycle may result in lock-in, but it will also need less work to manage your service. Consumers of cloud services should be able to unilaterally provision computing capabilities such as server time and network storage as needed without requiring human interaction with service providers. Unless we implement new technologies, we keep an eye on fundamental goals and values. We will not be able to fulfil our consumers' increasing expectations, and we will not be ready for even more significant changes that are sure to occur as we deal with constantly increasing data quantities and a proliferation of devices and sensors, says [56].

The fact that, when selecting cloud services, engineers must consider heterogeneous sets of criteria and complex dependencies between infrastructure services and software images which are complex. Cloud providers such as Amazon Web Services (AWS), Salesforce.com or Google App Engine (GAE) give users the option to deploy their application over a network of infinite resource pools with low capital investment and with very modest operating costs proportional to the actual use. A migration strategy defines migration procedure in means of order and data transfer [57]. The following five steps outline a migration of an organisations web application to a cloud infrastructure service (IaaS), whereas migration of a company's asset to a software application/applistructure or SaaS involves six holistic decision steps [16] and the steps of a migration to a Platform-as-a-Service (PaaS) offering would differ in several regards [58, 59]. PaaS migration is the process of moving from the use of one software operating and deployment environment to another environment. In order to develop (or adapt) software for cloud-based development and deployment, cloud-specific architecture and programming techniques need to be followed. Cloud migration can be categorised in terms of the cloud stack layers [60].

Cloud migration is a process of partially or completely deploying an organisation's digital assets, services, ICT resources or application to the cloud. The cloud migration process may involve retaining some ICT infrastructure onsite. However, the migration process involves the risk of accidentally exposing sensitive business-critical information. Thus, cloud migration requires careful analysis, planning and execution to ensure the cloud solutions' compatibility with organisational requirements, while maintaining the security and integrity of the organisation's ICT system. A cloud migration process involves many concept variants and several ways of instantiation. As with any software development project, migration projects should be planned carefully and have a good methodology to guarantee successful execution. There is a need for live migration of virtual machines (VMs) at IaaS because the current cloud provider ecosystem is heterogeneous and, hence, hinders the live migration of VMs [61]. In spite of the aforesaid, with the combination of different paradigms, live migration can be conducted between edge servers, physical hosts in the local area network (LAN) and data centre sites through the wide area network (WAN). In the next subsection, security is presented as a bottleneck for service adoption.

## **5.2 Security lock-in**

Cloud environments challenge many fundamental assumptions about the application and data security. Cloud-based software applications require design rigour similar to applications residing in classic DMZ. With cloud computing, application dependencies can be highly dynamic, even to the point where each dependency represents a discrete third-party service provider. The cloud security environment embodies shared security and joint responsibility, which produces a form of lock-in

with the cloud services providers [59]. However, this form of lock-in differs from using security and tamper-resistance to explicitly hinder users' ability to switch cloud service providers. This article's author has confirmed in the works of [16, 24] that such lock-in is anti-competitive and motivates consumers to adopt anti-lock-in solutions such hybrid clouds, cloud management providers or brokers, and routine manual data exports [17]. In this aspect, functional misalignment with business needs and technical limitations in areas including integration, security or extensibility are major inhibitors to data switchability from one vendor to another [14]. If cloud service providers and their customers are fully informed of human error as a major root cause of security risks encountered in the cloud, both parties can fully benefit from the advantages this model of computing offers [62].

Previously, various vendors have introduced different types of clouds with heterogeneous resources available in each, varying with respect to computation (CPU/GPU) memory and telecommunication network capabilities. Quite recently, cloud providers like IBM cloud have offered multi-cloud capabilities to improve interoperability and facilitate data or computation portability between clouds [63]. The cloud industry has recently moved into a hybrid of cloud-edge computing, but this creates a whole set of new risks regarding interoperability and APIs, managing heterogeneous capacities, workload offloading data integrity and privacy, storage decentralisation application restructuring [64]. In the process of digital transformation, organisations respond to changes in the surrounding environment by exploiting digital technologies [65]. However, combining new Internet of Things (IoT) solutions can be challenging and technology with legacy systems aiming to exploit heterogeneous data from these different sources [66, 67]. Interoperability plays a prominent role in multi-vendor ICT platforms where various systems need to interact efficiently making standardisation crucial for collaboration [68].

The cloud lock-in is less when applications are dynamically developed in an agnostic cloud platform environment such as Google App Engine (GAE) or Microsoft Windows Azure and it is removed with substantial cost to a different platform. Moreover, both PaaS and SaaS as platforms create network effects that enable the growth of users across both supply and demand sides. But at the SaaS layer, the hurdle of data integration requires a combination of technical and business processes used to combine data from disparate sources into heterogeneously meaningful, valuable and reusable information [69]. Respectively, service developers making use of cloud services can use SaaS providers and APIs as building blocks to develop composite services by integrating data and composing functionality provided by different SaaS resources [70]. Security, usability and vendor characteristics are the three main areas of lock-in risks in the cloud computing environment when adopting enterprise-class software like cloud ERP systems. Effectively integrating cloud ERP into existing cloud computing infrastructure will allow suppliers to determine organisations and business owners' expectations and implement appropriate tactics [71]. Orchestration of cloud services is important for companies and institutions that need to design complex cloud-native applications or to migrate their existing services to the cloud. Tools such as Chef, Ansible and Puppet provide infrastructure as code (IaC) language to automate the installation and configuration of cloud applications. Clarity about security tasks and responsibilities is a crucial consideration in the procurement process. In this regard, it should be stressed that the responsibility for security cannot be outsourced [72].

Adaptation of containerisation and serverless technologies is the most trending microservices research area for practitioners focused on cloud-related domains. Solutions that provide cloud computing with end-to-end security reduce vendor



lock-in risks as it relates to stored data. The information must be protected in cloud storage and transmission to reduce this risk, so only the data provider and the final consumer can access or modify it [73]. Regarding stored data, cloud service providers integrate cryptographic mechanisms based on encryption protocols such as advanced encryption standard (AES) or Rivest-Shamir-Adleman (RSA). To a certain degree, cloud service providers practise security-induced lock-in when employing cryptography and tamper-resistance to limit the portability and interoperability of users' data and applications, says Satzger et al. [17]. This security-induced lock-in and users' anti-lock-in strategies intersect within the context of platform competition. Thus, cloud services providers, therefore, favour security-induced lock-in over price leadership. Continued advancement of computing and digital technologies is transforming markets, economics and society. Migration to the cloud is strongly affecting corporate ICT strategies.

The security benefits of moving to a cloud-based system are often overlooked. A good cloud service will mitigate some existing risks and bring new benefits as well. Cloud provider is the vendor and operator of the cloud services. Cloud services vary substantially in size, from an entire e-business suite to a single component within a software development ecosystem (such as a storage or cryptographic key management service). It is simple for the cloud service to use a text template (like IaC) that outlines the desired configuration and contacts the APIs to make the necessary modifications because cloud infrastructure is typically maintained through APIs. As a result, IaC enables you to track your configuration in text documents where changes can be examined, and analysis can be carried out automatically. The use of automated processes to enforce security or policy requirements is known as guardrails and is an emerging technique in the cloud. This could entail a stipulation that only a select group of authorised operating system images may be utilised for computing services, or that all bulk data storage encrypts data at rest. Cloud services have been designed with an array of security benefits for your organisation and it is worth taking the time to find out what is available (and how to apply it to your specific needs) in order to gain the most benefits. The more you take the time to understand the cloud services available, the bigger the benefits will be. When selecting a cloud service, make sure that it meets your needs and helps you to secure your data. The process of digital transformation involves adopting technologies that enhance operational and customer experiences. Evaluating cloud and business risk together provides a better understanding of its impact on enterprises' overall risk maturity, including adopting a shared fate partnership between cloud service provider and customers [74]. This chapter affirms that an organisation's best path to viable risk management involves ICT modernisation into the cloud or cloud-like on-premise infrastructure. The CSA [74] report further confirms that there is no consistency of data classification across the use of cloud platforms and services. Tripathi and Mishra [75] note that the cloud is becoming less of a risk to manage and more of a means to manage these risks and modernisation. The approach helps both businesses and providers to improve their cloud adoption. The next subsection presents DevSecOps as a philosophy to combat security lock-in issues in the cloud environment.

### **5.3 DevSecOps mitigates lock-in**

A number of additional problems regarding the tools and services needed to develop and maintain running applications are brought on by cloud computing. These consist of program administration utilities, coupling to external services,



development and testing tools, libraries and operating system dependencies, some of which may come from cloud providers. It takes a lot of work to design, integrate and deliver software in the modern software engineering process. Continuous integration (CI) is the process of automatically adding new code from several developers to the same version of the software while simultaneously checking it for bugs. When deploying new software to production using continuous delivery (CD), the frequency of the deployments differs from traditional software deployment being the frequency of deployment, which can happen multiple times every day. DevSecOps is a software engineering culture that guides, breaks down silos, and unifies software development, security and operations. IaC evolved to solve a real-world problem referred to as environmental drift in the release pipeline. It is important to consider vendor lock-in versus product lock-in when selecting technology or IaC formats.

While the debate on cloud lock-in lies on the heavy reliance on the single cloud provider or perhaps the inability to use services of multiple vendors, closed proprietary software or systems purposely encourage technology lock-in, ensuring long-term customers and revenues while discouraging innovation. Abu-Libdeh et al. [76] strongly note that going all-in with a single cloud provider may allow organisations to simplify things and become more agile, potentially achieving better quality as single vendor solutions are often better integrated. Since no application is platform-specific containerisation can help isolate software from its environment, while DevOps helps to maximise code portability and makes it easier to deploy to different environments. However, applications built for the cloud have developed into a standardised architecture made up of many small, loosely linked parts known as micro-services (implemented as containers), supported by a program known as mesh that runs services. A container orchestration and resource management platform, such as Kubernetes, is home to both of these components and is referred to as a reference platform. Now, DevSecOps have been found to be a facilitating paradigm for these applications with primitives such as continuous integration, continuous delivery and continuous deployment (CI/CD) pipelines for providing continuous authority to operate (C-ATO) using risk-management tools and dashboard metrics [77]. DevSecOps puts security at the forefront of requirements to avoid the costly mistakes that come from treating security as an afterthought. Traditional security has been about exclusion and using the security policy to prevent people from disclosing secrets. DevSecOps is about inclusion and working as a team. Successful implementation of DevSecOps happens when the security team provides knowledge and tools and the DevOps team runs them. However, there is no reason for a security team to run tooling as a completely out-of-band management process. Before concluding that DevSecOps is a methodology or framework for agile application development, deployment and operations for cloud-native applications, DevOps uses a forward process with a delivery pipeline and a reverse process with a feedback loop that forms a recursive workflow. The role of automation in these activities is to improve this workflow *via* the following tools for automation (e.g. Ansible [78], and Terraform [79]), DevOps stack (e.g. Maven [80] and Jenkins [81]) and programming languages like Kotlin [82].

For example, maven is a software project management and comprehension tool. Based on the concept of a project object model (POM), maven can change a project's build, reporting and documentation from a central piece of information to sharing jars across several projects. In other words, it can be used for enabling and managing any Java-based project and one of the goals of maven is allowing transparent migration to new features as it has become the *de facto* build system

for Java applications. When migrating an application to the cloud and selecting a cloud service provider, the cost weighs heavily on the mind of every ICT manager in the automation industry. As a result, using an open-source system such as Jenkins can integrate with any cloud provider. Selecting tools based on strengths rather than vendor merit will help to avoid using one cloud provider for everything (which often leads to a single point of failure). Designing a solution using well-known patterns decouples its functional characteristics from the underlying cloud implementation, making it easier to avoid lock-in or go multi-cloud. By adopting standardisation, automation, cross-platform programming languages and containerisation, organisations are flexible and adaptable. In the next subsection, SDN is presented as a means to surpass some of the incumbent networking challenges caused by technical lock-in parameters.

#### **5.4 Software-defined networks**

A more open standards-driven approach to networking is necessary for the cloud and digital transformation era as opposed to the proprietary network architectures and Application Specific Integrated Circuits (ASIC). Software-defined Networking (SDN), built on OpenFlow protocol, enables an organisation to virtualise their network, automate operations, enable efficient network configuration and integrate network functions across dozens of switches creating a unified network architecture [83], that is programmable and dynamically definable. SDN as an emerging paradigm is set to logically centralise the network control plane and automate the configuration of individual network elements. In cloud data centres, however, network and server resources are collocated and managed by a single administrative entity; still, disjoint control mechanisms are used for their respective management. While unified server-network resource management is ideal for such a converged ICT environment, machine virtualisation can have a negative effect on cloud systems, resulting in drastic changes in performance and cost that mostly relate to networking constraints rather than software limitations. For example, network congestion caused by consolidation itself, particularly at the core levels of data centre topologies, has a substantial impact on the infrastructure as a whole and becomes the primary bottleneck, impeding effective resource utilisation and, as a result, provider's income. SDN runs on the principle of centralising control-plane intelligence while maintaining the separation of the data plane in order to allow open user-controlled administration of the forwarding hardware of a network component. The switching fabric (data plane) is retained by the network hardware devices, while the controller receives the intelligence (switching and routing functionalities). Because the entire network is under centralised control, the administrator can configure the hardware right from the controller, which gives the network a high degree of flexibility. SDN is monitored and implemented using a variety of tools and languages. A developing platform called Onix has been the focus of some SDN attempts in order to instal SDN controllers as a distributed system for flexible network management. Veriflow, a network debugging tool has been introduced in other studies, is capable of finding the flaws in SDN application rules and preventing them from impairing network performance. With the help of additional initiatives, the routing architecture Routeflow was created. It is based on SDN concepts and allows for interaction between the performance of commercial hardware and adaptable open-source routing stacks. As a result, it makes it possible to switch from traditional IP deployments to SDN.

By separating the control plane and forwarding plane, SDN provides centralised topology discovery and networking management, which enables the capability of managing resource contentions in finer granularity [84]. This gives academics and industry more options in a variety of network virtualisation-related areas, including novel LAN and WAN networking protocols, optimised virtualised data planes, traffic and flow management, software function chaining *via* virtualised network functions, etc. As a result, OpenFlow and the OF-CONFIG management and configuration protocol are accepted as the *de facto* standard SDN communication and control protocols. With SDN, policies, configuration and network resource management can be implemented quickly, and a single control protocol may handle a variety of tasks such as access control, routing and traffic engineering. The majority of open-source SDN controllers (Ryu, POX, FloodLight, OpenDaylight) expose APIs to manage firewalls, configure network components and obtain traffic counters, among other things. Additionally, they have been widely employed for other network-related applications, including QoS management, participatory networking, new management interfaces and for complete network migration. Minimising vendor lock-in has become important due to the degree and pace of network transformation that is required to keep up with business modernisation, to reduce hardware manufacturer lock-in, the network must be made programmable, and control and other functionality must be abstracted using software-driven strategy. It is crucial for ICT experts to choose the appropriate network operating system when utilising such a strategy in order to maximise cost-effectiveness and prevent problems with system integration and network availability [85]. The right approach to avoiding vendor lock-in is to counteract it strategically from the outset, instead of relying on one vendor, focus on several different ones. Internal systems should be built with the goal that subcomponents may be replaced later. Where a technology or vendor may seem like a riskier choice in terms of vendor lock-in, an exit strategy should be defined, obtain cloud services from several rather than a single provider, avoid using proprietary solutions, APIs, and formats and reduce the cost to switch. The next subsection highlights the need for effective strategies to mitigate the concerns of vendor lock-in.

## 5.5 Strategies

Organisations are under pressure to find and implement new strategic ideas at an even faster pace to gain a competitive edge over rivals within the global market. Towards this goal, it is fair to highlight herein that the absence of standardisation may also bring disadvantages, when migration, integration or exchanges of resources are required [3]. Strategies can be understood by referencing cloud lock-in taxonomies [24], which illustrate various components from which a cloud environment can be composed. Combining components into a solution introduces boundaries between the various components of a cloud system such as operational boundaries and trust boundaries. During the course of ordinary business processing or as data and applications migrate to new providers or platforms, data and application processing commonly crosses boundaries. A crucial issue that can be solved by portability and interoperability is ensuring operational integrity across boundaries as processing demands migrate to the cloud. Moreover, it must be enunciated that customers must be aware that they might need to switch service providers due to unacceptably high contract renewal costs, service provider business operations ceasing, partial cloud service closures without migration plans, unacceptably low service quality and

business disputes between cloud customers and providers, among other reasons. Again, as part of risk management and security assurance for any cloud initiative, portability and interoperability should be taken into account upfront. It is also the core strategy in the process of migrating towards cloud technologies, both within the public and private sectors. Companies will be responsible for evaluating their sourcing strategy to fully consider cloud computing solutions as viable. An example of policy measures to consider in this respect is presented in the next subsection.

## 5.6 Policy measures

According to Lewis [86], the cloud computing community typically uses the term interoperability interchangeably with portability. Herein, the author makes a clear distinction to specify that the former refers to the ability to easily move workloads and data from one cloud service provider to another or between private and public clouds. On the other hand, the latter states the ability to move a system from one platform to another. While these two separate terms are pertinent to the enlisted policy measures below, the author also draws the readers' attention to the role of open standards in the cloud with an emphasis on mitigating potential areas of lock-in effect across the cloud ecosystem (whether in domestic or international settings). Standards will be critical for the successful adoption and delivery of cloud computing, both within the public sector and more broadly. Standards encourage competition by making applications portable across providers, allowing federal governments (e.g. G-Cloud) to switch service providers in order to benefit from cost-saving measures or cutting-edge new product features. Furthermore, standards are essential to ensuring that cloud platforms are interoperable so that services offered by various providers can coexist, regardless of whether they use public, private, community or hybrid delivery models [87].

- Support proposals to stipulate minimum requirements regarding data portability and retention periods to support migration.
- Lay a stable governance foundation that will outlast single individuals or administrations so as to empower the government for action, minimise unnecessary bureaucracy and ensure accountability for results.
- The European Council (EC) should set rules that govern cross-border operations as well as not lacking harmonisation of the regulatory framework.
- Explore and support further options to create a single market for digital services.
- Support the implementation of the consumer right directive.
- Support the harmonisation of data protection rules through the establishment of a common regulation.
- Address cloud-specific aspects within the E-commerce directive.
- Ensure global harmonisation of cloud computing standards.
- Support software adaptation process that facilitates the development of cloud applications that are not coupled to any specific platform.



While data protection attracts much attention and debate in current literature, other contractual clauses between cloud service providers and the clients including choice of law, intellectual property (IP) issues, terms of service and acceptance use also impact the adoption of cloud computing and are discussed herein [11]. Therefore, gaining the benefits of this more elastic environment requires appropriate planning to avoid being 'locked' into a cloud solution that may not measure up to the goals for moving to the cloud in the first place. For additional and supplemental policy measures, please refer to the study by Opara-Martins et al. [13]. The next section concludes this research output and contribution by maintaining that this chapter should be rated high as it has linked academia and industry with cutting-edge research to create new knowledge and innovation that converts ideas into wealth creation, jobs and human progress. Thus, researchers lacking adequate knowledge, dexterity and self-transformation cannot be helpful to society nor will they be useful to themselves.

## **6. Conclusion and future work**

Cloud computing, as a catalyst for innovation, will not just be more innovative than we imagine, but it will be more innovative than we can imagine. Essentially, cloud computing refers to ICT services that are now instantly, unconditionally and on-demand available to everyone, from data processing and storage to software applications. The cloud has already become a go-to resource for some businesses with proprietary lock-in, and the trends indicate that this model is set for major development provided certain standards and compliance policies (e.g. data act) are taken in a timely manner. The experience of enterprises to date points to cloud computing being used at different levels according to the institutions concerned. Indeed, many researchers, research institutes and federal government agencies have adopted this technology in Europe. In the UK, specific data privacy, jurisdiction, contractual clauses and security pose a threat in that regard.

In the interest of fostering the emergence of cloud computing technology, this chapter advocates actions such that when choosing cloud services most cloud users cannot find an appropriate cloud service matching their individual requirements when they are using a given cloud service for the first time. Research emphasis is laid on parameters important to guide users in cloud service selection to provide a guide in choosing the appropriate strategy to mitigate cloud lock-in, and the author presents a state-of-the-art review of existing works in interoperable, portable and standard cloud migration techniques. These parameters provide a set of common functionality to all cloud services built using the cloud platform. Where skills or training in regard to cloud computing is concerned, the author surveyed DevSecOps tools, technology stack, programming languages like Kotlin and technical considerations pertaining to SDN, Edge, multi-cloud and Guardrails in dealing with the cloud lock-in parameters. The ICT sector in Europe is characterised by the very rapid development of mobile cloud computing (MCC) telecommunication networks. At the same time, however, UK businesses are seeking business process management (BPM) solutions whereby they can catch up on the deployment of context-aware services.

Against this background, in today's business marketing the main types of cloud services are cloud hosting services, object storage services, cloud database services, cloud engine services, block storage services, cloud caching services, online application services, load balancing services and cloud distribution services. The evidence shows that the implementation of strategies relating to contracts, selection

of vendors and developed awareness of commonalities and dependencies among cloud-based solutions has greatly reduced the risks of cloud lock-in. Cloud computing could go a long way to mitigate ICT lock-in risks through a market oligopoly provided the corresponding technology is implemented on solid standard bases that inspire confidence in interoperability, portability and integration. To this end, enterprise decision-makers and leaders are in agreement CYNEFIN framework adheres to international requirements in terms of disorder as it pertains to heterogeneity of cloud technology ecosystem. Similarly, the deployment of vendor-neutral services with ensured business continuity, rapid elasticity and secure data storage in line with international standards organisations (like NIST, ENISA, CSA, SNIA, The OpenGroup, TOGAF, OASIS) constitutes the strong pillar of cloud computing for Europe. In conclusion, the study presents technical and policy recommendations related to regulation, SLA, contracts on cloud computing, the implementation of open (sourced) APIs, standardisation and the cross-border data plan. The main objective of these policy measure(s) is to ensure a harmonious and sustainable development of cloud products and services in the UK.


In future work, the author identifies opportunities for cloud platforms to support more secure, interoperable, portable, automated and systematic authentication within and between cloud-hosted components. This research has been mainly focused on solutions to avoid vendor lock-in making it an active area of study for circa 2023 and beyond.

## **Author details**

Justice Opara-Martins  
Computing and Informatics Research Centre, Bournemouth University, Poole,  
United Kingdom

\*Address all correspondence to: [dr.martinsjustice@gmail.com](mailto:dr.martinsjustice@gmail.com)

## **IntechOpen**

© 2023 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] Mell P, Grance T. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology [Online], Special Publication 800-145. 2011. Available from: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>. [Accessed: September 1, 2022]
- [2] Brynjolfsson E, Hofmann P, Jordan J. Cloud computing and electricity: Beyond the utility model. *Communications of the ACM*. 2010;**53**(5):32-34
- [3] Sahandi R, Alkhalil A, Opara-Martins J. Cloud computing from SMEs perspective: A survey based investigation. *Journal of Information Technology Management*. 2013;**24**(1):1-12
- [4] Gannon D. The Client Cloud: Changing the Paradigm for Scientific Research. Keynote Address, IEEE CloudCom. Indianapolis; 2010
- [5] Buyya R, Broberg J, Goscinski A. *Cloud Computing: Principles and Paradigms*. Melbourne, Australia: Wiley; 2011
- [6] Ismail UM, Islam S, Mouratidis H. Cloud security audit for migration and continuous monitoring. In: *Proceedings—14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. TrustCom; 2015, 2015. pp. 1081-1087. DOI: 10.1109/Trustcom.2015.486
- [7] Khajeh-Hosseini A et al. Decision support tools for cloud migration in the enterprise. In: *Proceedings of the 2011 IEEE 4th International Conference on Cloud Computing, CLOUD 2011*. Washington, USA: IEEE; 2011. pp. 541-548. DOI: 10.1109/CLOUD.2011.59
- [8] Opara-Martins J. A decision framework to mitigate vendor lock-in risks in cloud (SaaS category) migration. Doctoral dissertation, Bournemouth University; 2017
- [9] Opara-Martins J, Sahandi R, Tian F. Implications of integration and interoperability for enterprise cloud-based applications. In: *International Conference on Cloud Computing*. Cham: Springer; 2015. pp. 213-223
- [10] Foster I, Zhao Y, Raicu J, Lu S. *Cloud Computing and Grid Computing 360-Degree Compared, Grid Computing Environments Workshop*. Texas, USA: IEEE; 2008
- [11] Opara-Martins J, Sahandi R, Tian F. A business analysis of cloud computing: Data security and contract lock-in issues. In: *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*. IEEE; 2015. pp. 665-670
- [12] Opara-Martins J. *Understanding Cloud Computing From An SME Perspective*. White Paper. 2013. Available from: [http://www.budigitalhub.com/sites/default/files/white\\_papers/Cloud%20Computing.pdf](http://www.budigitalhub.com/sites/default/files/white_papers/Cloud%20Computing.pdf). [Accessed: October 1, 2013]
- [13] Opara-Martins J, Sahandi R, Tian F. Critical review of vendor lock-in and its impact on adoption of cloud computing. In: *International Conference on Information Society (i-Society 2014)*. IEEE; 2014. pp. 92-97
- [14] Opara-Martins J, Sahandi M, Tian F. A holistic decision framework to avoid vendor lock-in for cloud saas migration. *Computer and Information Science*. 2017;**10**(3):29-53

- [15] Clement N, Arce DG. Dynamics of Shared Security in the Cloud. 2022. Available from: <https://ssrn.com/abstract=4281973> or <http://dx.doi.org/10.2139/ssrn.4281973>
- [16] Opara-Martins J, Sahandi R, Tian F. Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing*. 2016;5(1):1-18
- [17] Satzger B, Hummer W, Inzinger C, Leitner P, Dustdar S. Winds of change: From vendor lock-in to the meta cloud. *IEEE Internet Computing*. 2013;17(1):69-73
- [18] Govindarajan A, Lakshmanan. In: Antonopoulos N, Gillam L, editors. *Cloud Computing*. Vol. 0. London: Springer London; 2010. pp. 77-89
- [19] Petcu D. Portability and interoperability between clouds: Challenges and case study. In: Abramowicz W, Llorente IM, Surridge M, Zisman A, Vayssiere J, editors. *Towards a Service-Based Internet*. Vol. 6994 LNCS, 2011. Poznan, Poland: Springer Berlin Hiedelberg; 2011. pp. 62-74
- [20] Gonidis F, Paraskakis I, Kourtesis D. Addressing the challenge of application portability in cloud platforms. In: *Proceedings of the 7th South East European Doctoral Student Conference (DSC 2012)*. Thessaloniki, Greece: SERC; 2012. pp. 565-576
- [21] Kumari P, Kaur P. A survey of fault tolerance in cloud computing. *Journal of King Saud University-Computer and Information Sciences*. 2021;33(10):1159-1176
- [22] Snowden DJ, Boone ME. A leader's framework for decision making. *Harvard Business Review*. 2007;85(11):68
- [23] Murphy B, Rocchi M. Ethics and cloud computing. In: Lynn T, Mooney JG, van der Werff L, Fox G, editors. *Data Privacy and Trust in Cloud Computing*. Palgrave Studies in Digital Business & Enabling Technologies. Cham: Palgrave Macmillan; 2021. DOI: 10.1007/978-3-030-54660-1\_6
- [24] Opara-Martins J. Taxonomy of cloud lock-in challenges. *Mobile Computing-Technology and Applications*. 2018. pp. 3-21
- [25] Cloud Security Alliance (CSA). *Cloud Security Alliance Offers Recommendations for Using Customer Controlled Key Store*. 2022. Available from: <https://cloudsecurityalliance.org/press-releases/2022/09/27/cloud-security-alliance-offers-recommendations-for-using-customer-controlled-key-store/>. [Accessed: September 5, 2022]
- [26] ITU. International Telecommunications Union Rec. Y.3536 (02/2022) *Cloud Computing*. 2022. Available from: [https://www.itu.int/ITU-T/workprog/wp\\_search.aspx?sg=13&wp=2](https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=13&wp=2). [Accessed: September 5, 2022]
- [27] Cloud Standards Customer Council (CSCC). *Interoperability and Portability for Cloud Computing: A Guide Version 2.0* [Online]. 2017. Available from: <https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf>. [Accessed: September 10, 2022]
- [28] European Council (EC). *European Commission Digital Strategy*. 2022. Available from: [https://ec.europa.eu/info/publications/EC-Digital-Strategy\\_en](https://ec.europa.eu/info/publications/EC-Digital-Strategy_en) [Accessed: September 20, 2022]
- [29] European Council (EC). *Council of the European Union*. Council



- Conclusions on ICT Supply Chain Security [Online]. 2022. Available from: <https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf>. [Accessed: September 29, 2022]
- [30] Sen J. Security and Privacy Issues in Cloud Computing. 2013. Available from: <https://arxiv.org/pdf/1303.4814.pdf>. [Accessed: September 30, 2022]
- [31] Shahin M. An Empirical Study of Architecting and Organising for DevOps (Doctoral Dissertation); 2018
- [32] García-Grao G, Carrera Á. Extending the OSLC standard for ECA-based automation in DevOps environments. New York, USA: Cornell University; 2022. pp. 1-25. arXiv preprint arXiv:2211.08075. 2022
- [33] Oredo J, Dennehy D. Exploring the role of Organisational mindfulness on cloud computing and firm performance: The case of Kenyan organizations. *Information Systems Frontiers*. 2022;**24**:1-22
- [34] Lin L, Cheung A. Cloud economy and its relationship with China's economy—A capital market-based approach. *Financial Innovation*. 2022;**8**(1):1-22
- [35] Santoro D, Zozin D, Pizzolli D, De Pellegrini F, Cretti S. Foggy: A platform for workload orchestration in a fog computing environment. In: 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). Hong Kong, China: IEEE; 2017. pp. 231-234
- [36] Oulaaffart M, Badonnel R, Festor O. C3S-TTP: A Trusted Third Party for Configuration Security in TOSCA-Based Cloud Services; 2022
- [37] Opara-Martins J. Creative technology research seminar. PPT [online]. 2014. Available from: <https://slideplayer.com/slide/12537021/> [Accessed: October 1, 2022]
- [38] Alshamaila Y, Papagiannidis S, Li F. Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. *Journal of Enterprise Information Management*. 2013;**26**:250-275
- [39] Bainomugisha E, Mwotil A. Crane cloud: A resilient multi-cloud service abstraction layer for resource-constrained settings. *Development Engineering*. 2022:100102
- [40] Mohbey KK, Kumar S. The impact of big data in predictive analytics towards technological development in cloud computing. *International Journal of Engineering Systems Modelling and Simulation*. 2022;**13**(1):61-75
- [41] Finta G. Mitigating the Effects of Vendor Lock-in in Edge Cloud Environments with Open-Source Technologies. Espoo, Finland: Aalto University; 2022
- [42] Cai Z, Yang G, Xu S, Zang C, Chen J, Hang P, et al. RBaaS: A robust Blockchain as a service paradigm in cloud-edge collaborative environment. *IEEE Access*. 2022;**10**:35437-35444
- [43] Mane AS, Sonaje M, Tadge P. Data security in cloud computing using an improved attribute-based encryption. In: *Data Intelligence and Cognitive Informatics*. Singapore: Springer; 2022. pp. 261-272
- [44] Agarwal P, Sharma DK, Varun VL, Venkatesh PR, Kanchibhotla C, Ventayen RJM, et al. A survey on the scope of cloud computing. *Materials Today: Proceedings*. 2022;**51**:861-864
- [45] Morawiec P, Sołtysik-Piorunkiewicz A. Cloud computing, big data, and

Blockchain technology adoption in ERP implementation methodology. Sustainability. 2022;**14**(7):3714

[46] Won D, Hwang BG, Samion BM, N.K. Cloud computing adoption in the construction industry of Singapore: Drivers, challenges, and strategies. Journal of Management in Engineering. 2022;**38**(2):05021017

[47] Jayeola O, Sidek S, Abd Rahman A, Mahomed ASB, Hu J. Cloud computing adoption in small and medium enterprises (SMEs): A systematic literature review and directions for future research. International Journal of Business and Society. 2022;**23**(1):226-243

[48] Krishnaraj N, Bellam K, Sivakumar B, Daniel A. The future of cloud computing: Blockchain-based decentralised cloud/fog solutions—challenges, opportunities, and standards. Blockchain Security in Cloud Computing. 2022;**2**:207-226

[49] Vinoth S, Vemula HL, Haralayya B, Mamgain P, Hasan MF, Naved M. Application of cloud computing in banking and e-commerce and related security threats. Materials Today: Proceedings. 2022;**51**:2172-2175

[50] Ramalingam C, Mohan P. Addressing semantics standards for cloud portability and interoperability in multi cloud environments. Symmetry. 2021;**13**(2):317

[51] Ramchand K, Baruwal Chhetri M, Kowalczyk R. Enterprise adoption of cloud computing with application portfolio profiling and application portfolio assessment. Journal of Cloud Computing. 2021;**10**(1):1-8

[52] Shabbir M, Shabbir A, Iwendi C, Javed AR, Rizwan M, Herencsar N, et al. Enhancing security of health information using modular encryption standards in

mobile cloud computing. IEEE Access. 2021;**9**:8820-8834

[53] Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber security in iot-based cloud computing: A comprehensive survey. Electronics. 2021;**11**(1):16

[54] Mukherjee S, Chittipaka V, Baral MM, Srivastava SC. Integrating the challenges of cloud computing in supply chain management. In: Recent Advances in Industrial Production. Singapore: Springer; 2022. pp. 355-363

[55] Munteanu VI, Şandru C, Petcu D. Multi-cloud resource management: Cloud service interfacing. Journal of Cloud Computing. London, England: SpringerOpen; 2014;**3**(3):1-23. DOI: 10.1186/2192-113X-3-3

[56] Zulifqar I, Anayat S, Kharal I. A review of data security challenges and their solutions in cloud computing. International Journal of Information Engineering & Electronic Business. 2021;**13**(3):30-38

[57] Schlögl E. The Perception of Customer Relationship Management by Customers Versus Managers as a Critical Success Factor (Doctoral Dissertation, SOE); 2021

[58] AlTwaijiry A. Cloud Computing Present Limitations and Future Trends. ScienceOpen Preprints; 2021

[59] Costa B, Barreto PS. A risk perception indicator to evaluate the migration of government legacy systems to the cloud. International Journal of Information Systems in the Service Sector (IJISSS). 2021;**13**(1):68-87

[60] El Ioini N, Barzegar HR, Pahl C. Trust management for service migration in multi-access edge computing environments. Computer Communications. 2022;**194**:167-179

- [61] Mansour IEA, Bouchachia H, Cooper K. Exploring live cloud migration on amazon EC2. In: 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud). Prague, Czech Republic: IEEE; 2017, August. pp. 366-371
- [62] Palwe R, Kulkarni G, Dongare A. A new approach to hybrid cloud. International Journal of Computer Science and Engineering Research and Development (IJCSERD). 2012;2(1):1-6
- [63] Rafique A, Walraven S, Lagaisse B, Desair T, Joosen W. Towards portability and interoperability support in middleware for hybrid clouds. In: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Toronto, Canada: IEEE; 2014. pp. 7-12
- [64] Yussupov V, Breitenbücher U, Leymann F, Müller C. Facing the unplanned migration of serverless applications: A study on portability problems, solutions, and dead ends. In: Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing. Stuttgart, Germany: ACM; 2019. pp. 273-283
- [65] Liu Y, Ni Z, Karlsson M, Gong S. Methodology for digital transformation with internet of things and cloud computing: A practical guideline for innovation in small-and medium-sized enterprises. Sensors. 2021;21(16):5355
- [66] Briscoe G, Marinos A. Digital ecosystems in the clouds: Towards community cloud computing. In: 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies. New York, USA: IEEE; 2009. pp. 103-108
- [67] Ferrer AJ. Inter-cloud research: Vision for 2020. Procedia Computer Science. 2016;97:140-143
- [68] Mansour I, Sahandi R, Cooper K, Warman A. Interoperability in the heterogeneous cloud environment: A survey of recent user-centric approaches. In: Proceedings of the International Conference on Internet of Things and Cloud Computing. Cambridge, UK: ACM; 2016. pp. 1-7
- [69] Kaur K, Sharma DS, Kahlon DKS. Interoperability and portability approaches in inter-connected clouds: A review. ACM Computing Surveys (CSUR). 2017;50(4):1-40
- [70] Zhang Z, Wu C, Cheung DW. A survey on cloud interoperability: Taxonomies, standards, and practice. ACM SIGMETRICS Performance Evaluation Review. 2013;40(4):13-22
- [71] Ullah S, Xuefeng Z. Cloud computing research challenges. New York, USA: Cornell University; 2013. pp. 1397-1401. arXiv preprint arXiv:1304.3203
- [72] ENISA. Cloud Security Guide for SMEs [Online]. 2022. Available from: <https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes>. [Accessed: October 25, 2022]
- [73] Kratzke N. Lightweight virtualization cluster how to overcome cloud vendor lock-in. Journal of Computer and Communications. 2014;2(12):1
- [74] CSA. Security Guidance for Cloud Computing [Online]. 2022. Available from: <https://cloudsecurityalliance.org/research/guidance/>. [Accessed: November 19, 2022]
- [75] Tripathi A, Mishra A. Cloud computing security considerations. In: 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). Xi'an, China: IEEE; 2011. pp. 1-5

- [76] Abu-Libdeh H, Princehouse L, Weatherspoon H. RACS: A case for cloud storage diversity. In: Proceedings of the 1st ACM Symposium on Cloud Computing. Indianapolis, USA: ACM; 2010. pp. 229-240
- [77] Bohn RB, Messina J, Liu F, Tong J, Mao J. NIST cloud computing reference architecture. In: 2011 IEEE World Congress on Services. Gaithersburg, USA: IEEE; 2011. pp. 594-596
- [78] Hochstein L, Moser R. Ansible: Up and Running: Automating Configuration Management and Deployment the Easy Way. Sebastopol, USA: O'Reilly Media, Inc.; 2017
- [79] Brikman Y. Terraform: Up and Running. Sebastopol, USA: O'Reilly Media, Inc.; 2022
- [80] Ebert C, Gallardo G, Hernantes J, Serrano N. DevOps. IEEE Software. 2016;**33**(3):94-100
- [81] Riti P. Pro DevOps with Google Cloud Platform: With Docker, Jenkins, and Kubernetes. Westmeath, Ireland: Apress; 2018
- [82] Iglesias JAM. Hands-on Microservices with Kotlin: Build Reactive and Cloud-Native Microservices with Kotlin Using Spring 5 and Spring Boot 2.0. Birmingham, UK: Packt Publishing Ltd.; 2018
- [83] Bailey J, Stuart S. Faucet: Deploying SDN in the enterprise. Communications of the ACM. 2016;**60**(1):45-49
- [84] Brief OS. OpenFlow-enabled SDN and network functions virtualization. Open Netw. Found. 2014;**17**:1-12
- [85] Shackleford D. A Devsecops Playbook. Rockville, USA: SANS Institute; 2016
- [86] Lewis GA. Role of standards in cloud-computing interoperability. In: 2013 46th Hawaii International Conference on System Sciences. Pittsburgh, USA: IEEE; 2013. pp. 1652-1661
- [87] Kundra, V. Federal Cloud Computing Strategy. Washington, USA: White House; 2011