# The Impact of Cloud Computing and Virtualization on Business

Teresa Guarda[1,2,3,6(✉)], Maria Fernanda Augusto[1,2,4], Ismael Costa[6], Pedro Oliveira[5], Datzania Villao[1], and Marcelo Leon[7]

[1] Universidad Estatal Península de Santa Elena, La Libertad, Ecuador
[2] CIST – Centro de Investigación y Innovación en Sistemas y Telecomunicaciones, Universidad Estatal Península de Santa Elena, La Libertad, Ecuador
[3] Algoritmi Centre, Minho University, Guimarães, Portugal
[4] BiTrum Research Group, Leon, Spain
[5] Polytechnic Institute of Bragança, Bragança, Portugal
pedrooli@ipb.pt
[6] ISLA Santarém, Santarém, Portugal
[7] Universidad Tecnológica Empresarial de Guayaquil, Guayaquil, Ecuador

**Abstract.** In the begin cloud computing was seen as a thing of "startup" and visionary users, but nowadays it is a reality in organizations of any sector, type and size. Investments in data centers are replaced by the consumption of IT resources from a cloud provider. There are several types of virtualization, and that essentially means the abstraction of computational resources for different purposes; one of the ways, widely used, is to create virtual machines, which simulate a complete environment with software and hardware resources for the user. Despite being a technique that has existed for a long time, the growth of cloud computing has made this concept to be widely discussed. Significant innovations in virtualization, distributed computing, high-speed communications, and IoT, have aroused more and more interest in Cloud Computing. In this sense, we will analyze and evaluate the impact of cloud computing and virtualization on organizations.

**Keywords:** Cloud computing · Virtualization · Business impact · Security issues

## 1 Introduction

Cloud computing is currently a major challenge in the management of organizations, being a technology that allows you to distribute your computing services and access them online without the need to install programs. As it does not require the installation of programs or data storage.

The emergence of Cloud Computing services has changed the economics of IT organizations. The Cloud has come to standardize and automate resources in many of the tasks performed manually, being currently a commercial success, making it clear that in the coming years it will have an indisputable role in the IT areas.


T. Guarda et al. (Eds.): ARTIIS 2021, CCIS 1485, pp. 399–412, 2021.
https://doi.org/10.1007/978-3-030-90241-4_31

Despite the obstacles and limitations presented by some managers, the evolution of the Cloud Computing market has been happening at an accelerated pace. Services can be accessed remotely, from anywhere and anytime. The distribution of services is done through a platform of cloud services via the Internet with a price definition according to use.

Improving resource utilization through virtualization of IT infrastructures is a priority for many companies. A successful deployment requires prior preparation to determine the appropriate component infrastructure as well as the architecture, which is also suitable.

Virtualization refers to technologies created to provide an abstraction layer between computer hardware systems and the software that runs on those systems. It is a way to hide the physical characteristics of a computational platform from users.

There are several reasons for organizations to move from traditional IT infrastructures to Cloud Computing. One of the most impactful benefits is its economy.

This change will have a profound impact on the structure cost of organizations, and therefore can have a significant effect on the creation of new businesses, and probably on the economic performance of a country.

In this paper we will analyze and evaluate the impact of cloud computing and virtualization on organizations. The document has organized in six sections. The second section present cloud computing and virtualization concepts, and security issues. The third section, analyses the relation between virtualization and cloud computing. In turn, the fourth section assesses the impact of cloud computing and virtualization on the business, identifying the advantages and disadvantages. In the last section, the conclusions has presented.

## 2 Background

### 2.1 Cloud Computing

Cloud computing is the provision of computer services (servers, storage, network, software, analysis) over the Internet to make flexible resources and scaling savings faster.

The concept of Cloud arises from the physical arrangement of the elements involved in the model. The servers that host data and applications are located in data centers of companies anywhere in the world, which led to the need for a term that abstracted this location. The term Cloud, has adopted with the meaning of a tangle of servers available via the Internet.

#### 2.1.1 Cloud Computing Models

There are different models of cloud, and not all are suitable for all companies. These models, types, and corresponding services have evolved a lot in the last few years. Facilitating access to appropriate solutions for the different needs of companies [1].

For each organization, must be determined the type of cloud computing architecture in which the cloud services will be implemented.

In its typology, cloud computing can be classified based on the deployment model, or based on the service model offered by the provider [2] (see Fig. 1).

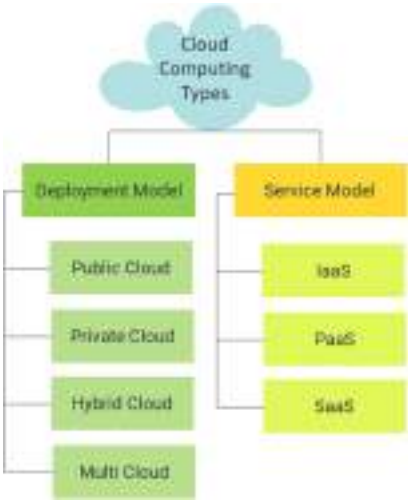


**Fig. 1.** Cloud computing types.

We present in Fig. 2 the deployment models. In the case of public clouds, organizations can use the cloud functionality of others that offer services to users outside the organization, which they can exploit their own purposes. In this sense, companies can outsource their services, reducing the infrastructure costs [1, 3].

Generally, private clouds propriety of the respective organization, that is, their use are dedicate to a single organization [3]. In a typical private cloud implementation, companies are committed to consolidating distributed resources and virtualizing those resources in data centers. This allows to provide a more profitable management and provide faster services [2].

Public clouds allowing companies to outsource parts of its infrastructure for cloud computing users, and that may causes the loss of control over resources, and data management, which is not a viable option for companies [3]. It is in this context that hybrid clouds appear, which, are a mix of private and public cloud infrastructures, allowing reduce costs through outsourcing, maintaining the control over sensitive data applying private cloud policies [1].

With the evolution of cloud services, and the needs of customers, Multi cloud appears. Multi cloud characterized mainly by the mixed use of various cloud services.

The multi cloud initially allowed circumventing the problems that resulted in data loss and downtime. There are some tendency to compare hybrid cloud & multi cloud systems, due to some confusion. Multi cloud refers to the administration of cloud services from multiple partners without the requirement of interconnection between the functions of the systems the hybrid cloud requires this interdependence, since the hybrid cloud structure works as a combination of private and public cloud services, so that both are integrated and interconnected, so that the service can work correctly [2].

Cloud vendors typically have a specific type of provisioning, although there is no potential restriction on not being able to offer different types at the same time [1].

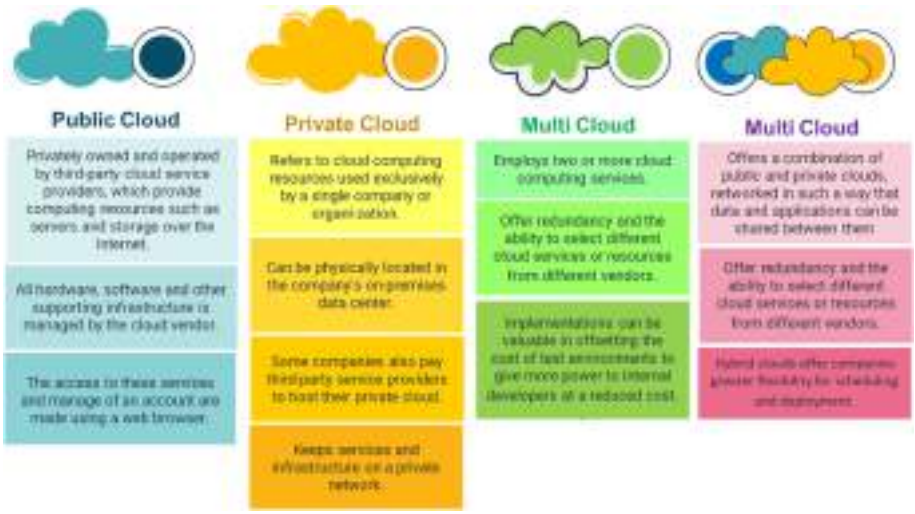


**Fig. 2.** Cloud computing implementation models.

Cloud Computing is the present, people are spending money on a good computer for their homes and businesses, they will hire services in the cloud to meet their needs and leave all the boring part of taking care of computer in the hands of big companies like Google, Microsoft and Amazon.

A cloud is a set of virtualized computing resources, which support a variety of different workloads, allowing them be scaled quickly through rapid provisioning of virtual machines or physical machines; provide redundant support, programming models, and self-recovery; and monitor the use of resources in real time, in order to allow the rebalancing of the assignments whenever necessary.

In the case of the service model, we have three types of services: Infrastructure as a Service (IaaS); Platform as a service (PaaS); and Software as a service (SaaS). The Infrastructure as a Service (IaaS) model is very successful in organizations. Instead of having its own server in its facilities, the organizations hires this type of service, for example, using Amazon AWS, for which you can have data or processing servers at super affordable prices.

It is important to note that the prices of infrastructure use may seem cheap; depending on the usage profile, it can be quite expensive and lead companies to seek new alternatives.

Platform (PaaS), offers a platform for development, testing, making applications available on the web for developers. It allows integration with web services, database and includes middleware as a service, message as a service, integration as a service, information as a service, and connectivity as a service. Such a layer makes it possible to meet the needs of users by providing infrastructure based on demand. For this type of service, we have Google App Engine.

Software-as-a-service (SaaS), offers implementations for specific business functions and for business specific processes, which are provide by specific cloud capabilities, that is, provide applications / services using an infrastructure (IaaS) or platform (PaaS). The same software can be used by multiple users, whether people or organizations. This type of service is performed and made available by servers in data centers that are the responsibility of a supplier company, that is, the software is developed by a company that instead of using it for exclusive benefit, makes it available at a certain cost for multiple organizations or users. In this model, users instead paying licenses for the complete software, which often has several features that we will never use, they pay for how much they use it. A classic example is Google Drive or SalesForce.

Infrastructure as a Service (IaaS), offers a platform for development, testing, making applications available on the web for developers. It allows integration with web services, database and includes middleware as a service, message as a service, integration as a service, information as a service, and connectivity as a service. This layer allows meet the needs of users by providing infrastructure based on demand.

### 2.1.2 Security Issues for Cloud Computing

There are several security concerns in a cloud computing technology, more specifically data security, data privacy and data safety [4].

Due to the nature of cloud computing architecture most clients are able to connect to the cloud computing via web browser or web service, which in turn means the cloud computing is vulnerable to web service attacks. Exchanging resources in a cloud-based network is done by Simple Object Access Protocol (SOAP) messages. The SOAP relies in XML signatures to secure the communication. It is then possible to attack the cloud system utilizing an XML wrapping attack. This attack consists on inserting the body of the SOAP message therefore creating a new body with the operation that the attack desires to do [5].

Browser security is another point of vulnerability for the cloud computing technology. Generally, web browser does the access to a remote cloud computing system. The user needs authorization and authentication to request services from the cloud, however web browser possess a security issue in which they can't provide XML Signature or encryption to WS-Security for authentication of an user and protect the data from users that are not authorized [6]. Another characteristic of cloud computing is the allocation of resources based on use, creating a dynamic adaption of hardware requirements to the actual workload occurring. In a security perspective, this concept can lead to several vulnerabilities. One of these is the ease of being attacked by a flooding attack or a Denial of Service attack. To perform this attack, the intruder floods the cloud computing system with non-sense requests for a service causing an increased workload for the server [5]. The cloud computing system has several more vulnerabilities than those mentioned above, which stem from the unique characteristics of the system. It is vital for the organization to be aware of the shortcomings and weak points of the cloud computing technology and prepare counter measures to mitigate the risk of utilizing this technology.

There are several data security risks in the cloud; we will are mention some of them: the APIs and unsafe protocols; Data interception; the leakage of data; public cloud storage; and virtualization [5].

Insecure APIs and security protocols can authorize access to data in the cloud. A basic cloud architecture depends on interfaces for management, orchestration and monitoring. APIs are an integral part of the security and availability of services in the cloud and specify how certain software components should interact with each other [7].

Data interception is a risk that occurs in the cloud due to the flow of data that circulates from side to side. The data in transit can be targeted by attackers, who can for example change the data. Encryption methods must be applied in order to ensure the integrity of the data that circulates between the user and the cloud [4].

Data leakage is one of the data security risks resulting from multi-use. Sharing the same computing resources by multiple users can result in accidental leakage of private data to other users. On the other hand, a system failure can allow other users or attackers to have access to the rest of the data. A security measure to counter this risk is the authentication of users before accessing data [8].

Public cloud storage is also a risk to data security, due to the sharing of computational resources between several users. One way to ensure data security is to use a private cloud for extremely sensitive data. Another way is to use a community cloud mode that adds the privacy protection module based on the Hadoop MapReduce concept. In this way, computing in the cloud will be performed based on the retention of privacy [6]. This community cloud mode consists of separating tasks; sensitive private data is disposed in the private cloud and non-sensitive data in the public cloud. The user must assign the sensitive data, otherwise the mode (community cloud based on privacy) will not do anything to the sensitive data.

Other data security risks result from virtualization, such as: compromising the functioning of the hypervisor, which can result in data exposure to other VMs. Resource allocation and deallocation also poses a risk to data security in the cloud. The careful use of resources, and the proper authentication of data before the resources are depleted are factors to be taken into account.

### 2.2 Virtualization

Virtualization allows to create a virtual computing environment (also known as a virtual machine), instead of running each environment on its own unique hardware. With sufficient resources (CPU, RAM, Storage) a single system can host countless guests, thus saving companies money and helping them to become more agile [9].

There are several types of virtualization, and that means the abstraction of computational resources for different purposes [10].

One of the ways, widely used, is to create virtual machines, which simulate a complete environment with software and hardware resources for the user [11]. However, the technique is quite broad and used for other purposes, such as application, desktop and server virtualization, for example.

Despite being a technique that has existed for a long time, the growth of cloud computing has made this concept to be widely discussed.

### 2.2.1 Types of Virtual Machines

They are virtual replicas of the entire logical component of a real computer, and it is not noticeable to the user whether a virtual machine or a physical computer is used. Regarding the kernel of a virtual machine, its system is purely logical, consisting of a series of files that store the configuration, the memory status, disk space, system logs and snapshots (small restores points) [12].

The creation and management has done by software installed on a physical machine called Hypervisor. There are two types of Hypervisors: type 1 and type 2. Hypervisors type 1 or bare metal are installed on the physical machine and consist of an operating system kernel for hypervisor functions in which it uses only the resources established for virtual machines. A good example of usage for these types of hypervisors are the servers and datacenters [13].

Hypervisors type 2 or hosted works as an application in an operating system and that allows applications to be run om the physical machine that are hosted on the virtual machines. The best example in the creation of a website, the installation of the web server is done on a virtual machine and running or testing the website on the physical machine (host) [14].

System containers, they function as an instance of the real system, called "lightvisors" because they share the same kernel as the real machine. In fact, this is one of their limitations, if we update or change libraries and frameworks the kernel remains the same [15]. There are two types of containers, system containers and application containers. Applications containers. They work creating a dedicated container for each application, being isolated form the operating system and other applications. The application requires various modules, and each module would be place in a container [16].

One of the most well known containers platforms are Dockers and Kubernetes. One great advantage of application containers is that permit the developer teams and the operations teams working at same time (devops). Docker platform nowadays supports containers of Linux systems, Windows and Mac in which with virtual machines for each System ensures that containers from different operating systems can be run on the same host operating system, containing tools that allow to integrate and interconnect the various containers to work as one. Docker's containers can run in the real System, in a virtual machine or inside the container itself [17].

The Kubernetes Platform that, in the execution of an application, creates and destroys containers according to your needs, automating the necessary configurations for the execution of the applications [18].

### 2.2.2 Virtualization Security

In recent years, virtualization has enjoyed considerable acceptance in companies and, more than a trend, it has become a standard in the security industry. The adoption of this technology includes benefits mainly related to the storage and processing capacities in an increasingly reduced infrastructure.

In the process of adopting and migrating to these types of solutions, several issues must be consider to keep services reliable and available. For this reason, security becomes

a necessary element to mitigate digital threats, in order to prevent the functioning of virtualized systems from being impact by an eventual incident.

Digital threats can affect systems that operate in physical or virtual environments. However, for protection there are specific conditions for each environment, as well as the implementation of security measures [19]. Especially if we consider that the management of virtualized systems works from a hypervisor.

The hypervisor is the software that allows imitating the hardware on which the virtual machines are running, in such a way that it can work directly on the hardware of the physical equipment or on an operating system. Regardless of how it works, the risks can be hidden. It is possible to identify threats that escape the virtual environment, as in the case of Venom, a vulnerability that allowed a cybercriminal or a malicious program to leave the environment of a virtual machine and affect the host computer or other virtual machines, running on the equipment [20].

The vulnerability was present in the hypervisor's source code, considering that the flaw could affect the main operating systems found in virtual environments. The vulnerability corresponded to an overflow of data, after sending data from specially modified parameters to the hypervisor controller, which would allow the execution of arbitrary code and gain access to the system.

In addition, if the hypervisor is running on an operating system, there may be greater exposure to threats that can affect not only virtualized systems, but also those that seek to affect the host operating system. In other words, you need to deal with threats that are properly focused on operating systems that have been virtualized and targeted to host systems.

Is essential to know how to deal with potentially sensitive data and code, they can affect systems. It is important to ensure, before moving to the Cloud, that the security management processes are properly defined, and that the chosen provider is able to implement them.

## 3 Virtualization Versus Cloud

It is easy to confuse virtualization with the cloud, mainly because both involve creating usable environments from abstract resources. However, virtualization is a technology that allows you to create multiple simulated environments or dedicated resources from a single physical hardware system, while clouds are IT environments that abstract, group and share scalable resources across a network. In short: virtualization is a technology and the cloud is an environment.

Typically, they are created to enable cloud computing, which is the execution of workloads within that system.

The cloud infrastructure can consist of a variety of elements, including bare metal, virtualization or container software, used to abstract, group and share scalable resources across a network and create the cloud [9]. At the base of cloud computing, there is a stable operating system, such as Linux. This layer gives users independence to operate in public, private and hybrid environments.

If we have access to the Intranet, the Internet or both, virtualization can be use to create clouds, although this is not the only option.

In virtualization, a software called hypervisor resides in physical hardware to abstract the machine's resources, which, in turn, made available in virtual environments, called virtual machines. These resources may include raw processing capacity, storage, or cloud-based applications containing all the resources and execution environment code required for deployment. Up to this point, it is a virtualization process, not a cloud process [15].

We could say that a cloud has created, if we have configured an IT system, and can be accessed by other computers, through a network; that contains a repository of IT resources; and that can be provisioned and scaled quickly.

Clouds provide the additional benefits of self-service access, automated infrastructure scaling and dynamic resource pools, which is the main distinction between cloud and traditional virtualization.

Virtualization has its own benefits, such as server consolidation and hardware optimization, which reduces the need to increase data center power, space and cooling. In addition, virtual machines are isolated environments and are therefore a good option for testing new applications or setting up a production environment.

Virtualization has three characteristics that make it ideal for cloud computing, which are [21] (see Fig. 3).

| Partitioning | Isolation | Encapsulation |
|---|---|---|
| Run multiple operating systems, and many applications on one physical machine | Each virtual machine is isolated from its physical host system and other virtualized machines | A virtual machine can be represented as a single file, so that it can be easily identified based on the service it provide |
| Full use of server services | Isolate faults and security at the virtual machine level | Encapsulate the entire state of the virtual machine in hardware-independent files |
| The available resources being divided according to the needs of each one | Dynamically control CPU, disk and network resources per virtual machine | The encapsulated process could be a business service |
| Support high availability by clustering virtual machines | Data is not shared between one virtual container and another | Save the virtual machine state as a snapshot in time |
| | Guarantee service levels | Reuse or transfer whole virtual machines with a simple file copy |

**Fig. 3.** Virtualization has three characteristics.

The more virtualized the environment, the better the results will be in the cloud deployment process. The main benefits will be the improvement of the management of the IT environment, information security and the considerable cost reduction. Because they have broad and interconnected concepts, it is necessary to analyze each of the technologies so that there is no confusion and to understand what the needs and objectives of each company have.

With virtualization, a single resource is able to behave like many. With cloud computing, different departments or companies have access to the same pool of automatically provisioned resources, through a private or public cloud, respectively.

Virtualization projects have been the focus of many IT professionals, especially those trying to consolidate servers or data centers.

Virtualizing IT resources can be toughed for organizations to increase processing power, memory, and bandwidth and storage capacity for the fewest hardware platforms possible and then allocate those resources to operating systems and applications on a time-sharing basis.

Thus, organizations will be able to reduce a significant number of physical servers; and can simply instead having multiple physical servers running, having on a single machine with multiple virtual servers. This allows IT departments to have the possibility of have more than one operating system, applications and services running on a single machine, controlled by a virtualization management console.

In this sense, infrastructure costs are fixed and constant, and not aligned with the mission of reducing complexity and problems. Reducing the number of physical devices reduces costs, energy consumption, and more free space.

Virtualization contributes to higher levels of business continuity in several ways. With the decoupling of applications, operating systems and hardware platforms, less physical device redundancy is required to serve primary machines [22]. To achieve high availability in traditional configurations, a 1:1 ratio of primary device to backup device is often required, in addition to a 1:1 ratio of software to hardware. In the virtualized environment, however, multiple servers can fail over to a set of backup servers.

This then allows for a many-to-one configuration ratio, which increases the availability of the service.

At the configuration level, virtualization sometimes comes down to simple clicks, and in server and network virtualization, companies can define their own policies, such as priority applications, request for competing resources, among others. Therefore, with fewer servers and consequent less maintenance, virtualization allows support a higher-level management, security and monitoring, allowing a better cost and efficiency ratio.

These features make virtualization and cloud computing very compatible. These two technologies are at the top of the priorities for IT professionals.

## 4 Impact on Business

The organization's motivation to implement and use a system in the cloud computing, it is dependent on the benefits that it may achieve.

Cloud computing providers insistently promote the change of workloads to a Cloud environment, as a fundamental factor for cost reduction that they justify with the elimination of the expenses of buying hardware and software.

Cloud computing represents a paradigm shift in the way information technology services are invented, developed, deployed, scaled, updated, maintained, and paid for [23].

To develop more efficient and sustainable processes and operations, the focus of business organizations will be directed to their core business. In this way, organizations

will be able to achieve excellence business success [24]. Cloud Computing has become a fact of existence essentially originated by 3 factors, the rapid technological evolution, changing concepts at the management executive level and the accessibility of abundance figuring limits to giants like Google or Amazon [25]. The ease of adaptation and use, sharing and cooperation, protection and security, reliability, and minimization of costs, are characteristics of high relevance at the time of decision by business organizations for solutions based on cloud computing [26, 27].

The reduced cost, unlimited scalability, flexibility, better mobility, improved communication, reliability, increased storage, easier updates, disaster recovery, security, can be identified as the main benefits of cloud computing. These benefits are at the basis of the motivation of business organizations to migrate their local infrastructure to a cloud computing solution. Instead of building their own infrastructure, organizations prefer to take advantage of the services offered by cloud computing. This solution is an important help to achieve business goals, allowing increasing revenue and having a positive impact on business organizations. However, there are also challenges to be faced, some of which are interoperability, security and privacy in the cloud, sensitive data, and portability, imprisonment of suppliers, organizational aspects, and regulatory and legal restrictions. Using encryption techniques, alternate backups, hiring qualified and experienced professionals, subcontracting security services, investing in education, adequate selection of cloud providers, auditing the services present in the cloud and selective migration of business applications, will be some of the solutions to follow by business organizations to overcome the challenges of migration to cloud computing [28].

In OECD countries (Organization for Economic Cooperation and Development), small and medium-sized business organizations (SMEs) account for approximately 2 thirds of total employability (60–70%). These organizations (SMEs) represent 95% of all business organizations. For these organizations, cost reduction or the economic factor will not be the most relevant factors to consider when migrating to a cloud solution. On the other hand, the factors "Ease of use and convenience" and "security and privacy" are the most important facts for this migration. Cloud computing is having a real impact on SMEs, slowly infiltrating the business strategy in the present and in the near future [29].

According to a Gartner study published in 2020, cloud technology will continue its growth as organizations continues to move to distributed, hyper scale, and hybrid solutions in cloud. The crisis of COVID-19 and the consequent technological needs, have led to greater investments in IT by business organizations, thus accelerating the migration to the cloud. These investments represented 9.1% already in 2020 and, according to the consultant's projection; they will represent 14.2% of the total investments of the organizations in 2024. In 2025, transformational business models will be adopted in more than 50% of organizations. These models will be implemented through solutions based on distributed cloud, located anywhere of choice. Compared to less than 1% in 2020, the consultant also predicts that by the end of the year 2023, hyperscale cloud providers will manage 20% of installed edge computing platforms [30].

Boosting greater efficiency in the use of data and system resources, the virtualization layer must adapt its state over time according to the resources available, thus overlapping some activities and decisions specific to the management of organizations. The requests made by the customer are translated into actions sent to the virtualization system, which

implies a close and strong coordination between this system and the organizations' own management system. These two systems are difficult to separate, and their effective functioning is dependent on their joint treatment. A virtualization layer should be one of the components of the organization's management system, with its own assessment, advice, and action resources [31]. Solving several complex problems and providing a superior computing experience, this type of technological solution will have a high impact on SMEs, considering that it allows a reduction in hardware, administration, and system maintenance costs. Virtualization should therefore be considered as an important component of the organization's management, enhancing its success and sustainability. According to the Mordor Intelligence consultant report published in January 2021, the desktop virtualization market represented a volume of $ 6.712,8 million in 2020. The same consultant predicts that a volume of US $ 12.290,22 million will be reached in 2026, with a CAGR growth of 10.6% over the forecast period (2021–2026) [32].

## 5 Conclusions

With Cloud Computing, it will also be possible to have equipment operating more efficiently and, therefore, less expensive than in traditional organizations' environments.

However, the benefits of Cloud Computing are not that obvious. The savings provided by the Computing Cloud, as well as the increase in efficiency, would depend on many factors: the intensity of the workload, the frequency with which the application will be use in the coming years, the necessary storage capacity, among others. It also depends on the approach and the previous study done by the organizations in order to meet what they really want and thus facilitate a smooth migration.

In general, companies are moving to the Cloud at a good pace, starting a giant tide that multiplies the number of new implementations. Hiring paid cloud computing services according to the user's needs becomes a good solution. The systems adapt to the requirements of the business. Among the main suppliers, Google, Microsoft and Amazon can be highlight, offering a wide range of solutions for organizations.

Migrating to the Cloud Computing is a complex evolution for many companies, and it is essential that IT companies and executives are align with the initiatives. It is necessary to carry out a preliminary study of the real organization's needs, and how it is going to do, so it is therefore important to prepare IT professionals for such a change. Only then and being properly prepared, an organization can remove the due performance from the Cloud Computing.

Moving a company's workloads to the Cloud Computing is see as a factor in reducing costs. At a minimum, it eliminates the capital expenditures necessary to purchase equipment and software. The savings provided in the Cloud Computing will depend on many factors: the intensity of the workload, the frequency with which the application will be used in the coming years, the storage capacity required and the software licensing costs.

## References

1. Frantsvog, D., Seymour, T., John, F.: Cloud computing. Int. J. Manag. Inf. Syst. (IJMIS) **16**(4), 317–324 (2012)

2. Senyo, P.K., Addae, E., Boateng, R.: Cloud computing research: a review of research themes, frameworks, methods and future research directions. Int. J. Inf. Manage. **38**(1), 128–139 (2018)
3. Varghese, B., Buyya, R.: Next generation cloud computing: new trends and research directions. Futur. Gener. Comput. Syst. **79**, 849–861 (2018)
4. Gupta, A., Thakur, S.: Cloud computing: its characteristics, security issues and challenges. Rev. Comput. Eng. Stud. **4**(2), 76–81 (2017)
5. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Gener. Comput. Syst. **28**(3), 583–592 (2012)
6. Venkatesh, A., Eastaff, M.S.: A study of data storage security issues in cloud computing. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. **3**(1), 1741–1745 (2018)
7. Walia, M.K., Halgamuge, M.N., Hettikankanamage, N.D., Bellamy, C.: Cloud computing security issues of sensitive data. In: Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing. IGI Global, pp. 1642–1667 (2021)
8. Fu, X., Gao, Y., Luo, B., Du, X., Guizani, M.: Security threats to Hadoop: data leakage attacks and investigation. IEEE Network **31**(2), 67–71 (2017)
9. Shukur, H., Zeebaree, S., Zebari, R.Z.D., Ahmed, O., Salih, A.: Cloud computing virtualization of resources allocation for distributed systems. J. Appl. Sci. Technol. Trends **1**(3), 98–105 (2020)
10. Khalid, M.F., Ismail, B.I., Mydin, M.N.M.: Performance comparison of image and workload management of edge computing using different virtualization technologies. Adv. Sci. Lett. **23**(6), 5064–5068 (2017)
11. Feoktistov, A., et al.: Multi-agent approach for dynamic elasticity of virtual machines provisioning in heterogeneous distributed computing environment. In: International Conference on High Performance Computing & Simulation (HPCS) (2018)
12. Alqahtani, A.S., Daghestani, L.F., Ibrahim, L.F.: Environments and system types of virtual reality technology in STEM: a survey. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **8**(6), 77–89 (2017)
13. Vojnak, D.T., Đorđević, B.S., Timčenko, V.V., Štrbac, S.M.: Performance comparison of the type-2 hypervisor VirtualBox and VMWare workstation. In: 7th Telecommunications Forum (TELFOR) (2019)
14. Norine, C., Shaffer, A., Singh, G.: Artifact mitigation in high-fidelity hypervisors. In: Proceedings of the 54th Hawaii International Conference on System Sciences (2021)
15. Karmel, A., Chandramouli, R., Iorga, M.: Nist definition of microservices, application containers and system virtual machines. National Institute of Standards and Technology (2016)
16. Sharma, P., Chaufournier, L., Shenoy, P., Tay, Y.C.: Containers and virtual machines at scale: a comparative study. In: 17th International Middleware Conference (2016)
17. Modak, A., Chaudhary, S.D., Paygude, P.S., Ldate, S.R.: Techniques to secure data on cloud: Docker swarm or Kubernetes? In: Second International Conference on Inventive Communication and Computational Technologies (ICICCT) (2018)
18. Shah, J., Dubaria, D.: Building modern clouds: using Docker, Kubernetes & Google cloud platform. In: IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (2019)
19. Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. **4**(1), 1–13 (2013)
20. Abdoul-Kader, C., Chang, S.H.: A novel VENOM attack identification mechanism in cloud virtualization environment. Commun. CCISA **24**(1), 61–72 (2018)
21. Ahmed, I.: A brief review: security issues in cloud computing and their solutions. Telkomnika **17**(6), 2812–2817 (2019)

22. Sehnem, S., Campos, L.M., Julkovski, D.J., Cazella, C.F.: Circular business models: level of maturity. Manag. Decis. **57**(4), 1043–1066 (2019)
23. Srivastava, P., Khan, R.: A review paper on cloud computing. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **8**(6), 17–20 (2018)
24. Khan, S.: Cloud computing paradigm: a realistic option for the business organizations -a study. J. Multi Disc. Eng. Technol. **12**(2), 85–97 (2018)
25. Rajaraman, V.: Cloud computing. Resonance **19**(3), 242–258 (2014)
26. Devasena, C.L.: Impact study of cloud computing on business development. Oper. Res. Appl. Int. J. **1**, 1–7 (2014)
27. Viswanathan, S.: A study on influence of cloud computing on business developments. Int. J. Pure Appl. Math. **118**(18), 3637–3643 (2018)
28. Dar, A.: Cloud computing-positive impacts and challenges in business perspective. Int. J. Comput. Sci. Eng. **7**(1), 786–789 (2019)
29. Gupta, P., Seetharaman, A., Raj, J.R.: The usage and adoption of cloud computing by small and medium businesses. Int. J. Inf. Manage. **33**(5), 861–874 (2013)
30. Gartner: Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021, 17 September 2020. https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021. Accessed 28 Mar 2021
31. Sven, G., Ralf, K., Vijay, M., Jim, P., Sahai, A., Aad van, M.: Impact of virtualization on management systems. Hewlett-Packard Laboratories, 1501 Page Mill Road, Palo Alto, CA 94304, USA (2003)
32. Mordor Intelligence, Desktop Virtualization Market - Growth, Trends, Covid-19 Impact, DND Forecasts (2021–2026) (2021). https://www.mordorintelligence.com/industry-reports/desktop-virtualization-market-industry. Accessed 28 Mar 2021