International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 08, ISSN No. 2455-2143, Pages 01-07
Published Online December 2024 in IJEAST (http://www.ijeast.com)

THE LIST, BENEFITS, AND CHALLENGES IN CLOUD COMPUTING

Sai Varun Reddy Bhemavarapu
Application Security Engineer
Department of Information Technology Management,
Illinois Institute of Technology

Agathamudi Vikram Naidu
Application Security Architect
Department of Information Technology Management,
Illinois Institute of Technology

Dr . Professor Ray Trygstad
Department of Information Technology Management,
Illinois Institute of Technology

The List, Benefits and Challenges in Cloud Computing

In recent years, cloud computing has emerged as a powerful technology that has revolutionized the way businesses and individuals use and access computing resources. With cloud computing, users can access computational resources, including servers, storage, analytics, and networking, on-demand and through the internet. This has led to increased efficiency, flexibility, and scalability in computing, as well as cost savings for many organizations.

Despite its numerous benefits, however, cloud computing also poses several potential challenges that must be addressed in order to ensure its successful implementation. These challenges include security concerns, limited control, and downtime, among others. Therefore, while the advantages of cloud computing are clear, it is important for businesses and individuals to understand both the benefits and the potential risks associated with this technology.

As cloud computing continues to evolve and expand, it is becoming increasingly important for businesses and individuals to understand its benefits and challenges. This paper will explore the different aspects of cloud computing, including its definition, benefits, and challenges, as well as the various models and deployment options available. By the end of this paper, readers will have a better understanding of the potential of cloud computing as well as the challenges that must be addressed in order to fully realize its benefits.

Cloud computing is a powerful tool that can offer many benefits, but it is important to be aware of the challenges associated with it before making the decision to move to the cloud.

What Is Cloud Computing?

Cloud computing is an OnDemand service delivery ofcomputational resources (Computational resources are the physical and software elements that are used to perform computations) which include Servers (A server is a computer that provides resources to other computers, known as clients), Storage, Analytics, and Networking through the internet (Dr. CH. V et al., 2016).

How does Cloud Computing work?

These cloud computing services are provided to the clients by having companies maintain a large pool of computers or data centres that can help with storage, security and power of computation.

Examples of Cloud Computing. Some of the examples for cloud computing are Gmail, Twitter, Facebook, Salesforce, Google Drive, Messenger, Telegram, Github, Dropbox, etc. We use most of these apps because it makes life easier and all of these platforms use Cloud Computing. Later in this paper, we will go further into it.

Cloud Computing Models:

Cloud computing models have two types, one is Service or Delivery Model and the other is Deployment Model. In simpler terms, an organisation or individuals acquire platforms related to Computing and Information Technological infrastructure through internet and Host, Run, and Deploy their respective applications in cloud and give users services to access their Software, Data and Hardware resources in a transparent way.

Service Models. A Service model is a kind of Business model where the Delivery of a service is provided by the service provider. There are Four Service models that are provided by service vendors, they are: Software as a

Service, Platform as a Service, Infrastructure as a Service, and Container as a Service.

Software As A Service. Software as a Service (SaaS) is a cloud computing delivery model where users can access software applications over the internet through a web browser or mobile app, on a subscription basis. With SaaS, users don't need to install or maintain any software on their own computers, which saves them money on IT costs. SaaS is becoming increasingly popular among businesses of all sizes, as it offers the latest software features and updates (Rani & Ranjan, 2014).

Example for Software as a service is Microsoft 365 where there is a subscription plan to use the services or applications like Microsoft Word, Microsoft Excel, Microsoft Powerpoint etc., . This service is majorly used by business users to email support, and automation of office support works. Which helps in making business tasks easier.

Platform As A Service. PaaS stands for Platform as a Service. It is a way to build and run applications without having to worry about the underlying infrastructure. The PaaS provider takes care of all the hardware, software, and networking, so you can focus on building your application.In a simpler language, just think if you want to build a sand castle you have to buy sand, buckets, shovels yourself and it could be a lot of work and you might not have the tools needed. So instead you go to the beach where you have plenty of sand and the beach provides all the tools needed to build a sandcastle and you can just focus on having fun.

Example for Platform as a service is VMware which helps in running Virtualized software without installing the software on the host machine. It helps install multiple operating systems on your primary operating system; for example, you can install Kali Linux on your Windows 11 which is your primary operating system.This service is majorly used by developers and deployers to test the applications that have been developed recently.

Infrastructure As A Service. IaaS stands for Infrastructure as a Service. It is a way to rent computing resources, such as servers, storage, and networking, from a cloud provider. This allows you to focus on building your applications, without having to worry about managing the underlying infrastructure. In simpler language, imagine you want a house to live in a new city that you moved to recently. You could build a house but that requires buying a piece of land and other tools which would be a lot of work to do; instead you rent a house from a landlord without worrying about getting the physical infrastructure and management.

Example for Infrastructure as a Service is Google Cloud Program where this program allows users to build applications with just an internet connection without having its customer to have a powerful physical infrastructure at his place because the vendor provides all the infrastructure to its customer over the internet and manages it for the customer. It is majorly used by System managers creating Virtual environments for all the employees.

Container As A Service. Caas stands for Container as a Service. Here, customers of Cloud service providers can subscribe to the Deployment containers without owning Servers, Network infrastructure, and Storage. Which helps developers to move the code from one server to another. Just like if you want to move all the goods to a new place then instead of buying a moving truck you rent it for a specific time.

Example for Container as a service is Google Kubernetes Engine, Amazon Elastic Container service. This Service is majorly used by developers to start and stop the applications that are in the container.

Deployment Models. Deployment model means the way in which the service is made available to the users. There are four models in which the cloud services are deployed named Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud; each of the deployment models have their respective features and advantages. There are many organisations that provide all the cloud services such as Amazon Cloud , Google Cloud, IBM Cloud, Oracle Cloud, etc.

Public Cloud. A public cloud is a cloud computing model in which a third-party provider makes computing resources which include servers, storage, databases, networking, software, analytics that are available to the public over the Internet. Public cloud services are self-service, pay when you use, and scalable, with resources dynamically provided and are released based on demand.

Public cloud providers offer a broad range of services, from Infrastructure as a Service (IaaS) to Platform as a Service (PaaS) to Software as a Service (SaaS). IaaS provides the basic building blocks for cloud IT—compute, storage, networking, and databases. PaaS provides a platform for developers to build, deploy, and manage applications. SaaS provides ready-to-use applications that can be accessed from anywhere with an Internet connection.

Private Cloud. A Private Cloud is a Cloud Computing model where Security is enhanced when compared to Public Cloud as this Deployment model as this type of cloud is dedicated to a single organisation. It has a dedicated environment and features like enhanced security where most of the companies try to manage their environment using a centralized concept or it can be hosted virtually. As Sen (2021) explains, “This is best suited for applications which require complete control and configurability of the infrastructure and security. As the name implies, the externally hosted private clouds are hosted externally with a cloud provider in which the provider.”

Hybrid Cloud. Hybrid Cloud Deployment Model is a mixture of Both Public Cloud and Private Cloud. It is a model where the transportability of application and data can be done simultaneously. This model allows organizations to utilize the benefits of both Public and Private clouds while maintaining control over their data and applications. In a

hybrid cloud, some workloads are run in the public cloud, while others are run in the private cloud. The two environments are connected, allowing for data and application portability. Hybrid clouds are ideal for organizations with fluctuating workloads, as they can scale resources up or down as needed, and for those with strict compliance or security requirements, as sensitive data can be stored in the private cloud while less sensitive data can be stored in the public cloud. To achieve a successful hybrid cloud deployment, it is important to ensure compatibility between the public and private cloud environments, and to have a solid strategy for workload placement and data management.

Community Cloud. Community Cloud Deployment Model is different from the other three deployment models in which the infrastructure is shared by a specific community of organizations that have shared concerns (security, compliance, jurisdiction, etc.), In this model, the community members share the cost and responsibilities of building, managing, and maintaining the cloud infrastructure. The community cloud is designed to provide a secure and flexible computing environment that meets the specific needs of the community members.

The community cloud can be managed by one or more of the community members or by a third-party service provider. The community members can have varying degrees of control over the cloud infrastructure, depending on their requirements and agreements. The community cloud can provide a range of services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Patel & Kansara, 2021).

What Are Benefits Of Cloud Computing ?
Advantages
Cloud computing provides many benefits to businesses and individuals. In the coming sections we are going to look into the Economical Aspect and Service Aspect.

Economical Aspect.
One of the biggest advantages is that it helps in reducing the cost of physical infrastructure which can incur a lot of cash burn upfront for a business. It can also save a lot of expense for a company by paying only for the resources the company uses, rather than having to invest in excess capacity. Additionally, cloud computing provides scalability and flexibility, allowing businesses to easily increase or decrease their resources as needed. Cloud services also offer increased reliability and security with backups and redundancy which protect against data loss or system failures. Lastly, cloud computing enables collaboration and remote access, allowing individuals and teams to work together from anywhere in the world and help employees save a lot of time travelling which can save fuel cost and time spent in traffic.

Service Aspect.
Cloud computing has a lot of positive aspects related to services., Cloud computing makes it possible to provide the services on-demand such as allowing users to access resources and services at any time from anywhere in the world. This enables businesses to be more quick and responsive to customer needs which allows them to quickly adapt to the market conditions. Apart from that, cloud computing services are highly scalable, allowing businesses to easily increase or decrease the resources they use as their needs change. This provides a high level of flexibility, allowing businesses to easily adjust their operations to meet the demands of the market. Cloud computing services offer a high level of reliability and availability, with many providers offering service level agreements (SLAs) which guarantee a certain level of uptime and performance.

Disadvantages:
As there are advantages there are disadvantages as well in Cloud computing like Downtime, Security, and Limited Control.

Downtime:
When a cloud provider's infrastructure experiences an outage, resulting in the unavailability of services to users, it is called Downtime (Defect, Overproduction, Waiting, Non-Utilized Talent, Transportation, Inventory, Motion, and Extra Processing) . This can be a major issue for businesses that rely on cloud services for critical operations. Even if there is minor downtime it could cause a significant loss in both production and financially in a business. Cloud providers may have service level agreements (SLAs) that guarantee a certain level of uptime, but they do not always compensate users for any downtime that occurs. It can be caused by a variety of factors, such as hardware failures, software bugs, or network outages. Providers of Cloud may have different definitions of downtime, making it difficult to determine whether an outage qualifies as downtime or not.So, downtime remains a significant disadvantage of cloud computing that users must be aware of and plan for accordingly.

Security:
Cloud Computing also has some security concerns. Among them the primary concern with cloud computing is the issue of data security and Storing sensitive data on a third-party server can increase the risk of data breaches and unauthorized access to information. Cloud providers can also be targeted by cybercriminals, and security breaches can result in the loss of valuable data or even reputational damage. Additionally, if the businesses are using public cloud services then it might be difficult for the business to

ensure the Governance, Risk and Compliance, and Regulations with data privacy.Usually, Cloud providers have their own security protocols in place, but it is important for businesses to take additional measures to secure their data and ensure compliance with applicable regulations.

As Srinivasan (2013) explained, one of the challenges for any new technology is the availability of global standards. Cloud computing is evolving rapidly but there are not many commonly accepted standards yet. ISO 27001, NIST and Cloud Security Alliance are all working toward providing guidelines for the cloud industry.

Limited Control:

When using cloud computing, you are essentially renting computing resources from a cloud service provider which means that you have limited control over the physical infrastructure that your applications and data are running on. For example, you may not be able to choose the specific hardware that your applications are running on, or you may not be able to make changes to the operating system or network configuration. There are a number of reasons why cloud providers limit control over their infrastructure. One reason is that it allows them to scale their services more easily. If a cloud provider has to manage a large number of different configurations, it can be difficult and time-consuming to make changes to all of them. By limiting control, cloud providers can make it easier to make changes to their infrastructure, which can help to improve the reliability and performance of their services.

Another reason cloud providers limit control is that it can help to improve security. If users have too much control over their infrastructure, they may make changes that could make it more vulnerable to attack. By limiting control, cloud providers can help to ensure that their infrastructure is more secure.

What Are The Challenges Of Cloud Computing?

Security Analysis

As there are growing users of Cloud computing there are several challenges that arise with the growing user base. They are Network Security, Software Security, Risk Management, Vulnerability and Threat Management for newer risks in the cloud and Governance and Compliance to Security standards.

Cloud Security

With the growing base of the cloud users the security aspect also needs to be considered by the cloud service providers. The major challenge of Cloud computing is to secure the data of the users. Cloud security is a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. It is a critical component of any cloud computing strategy, as it helps to ensure the confidentiality, integrity, and availability which is the base of Cyber Security.

Network Security. When it comes to Cloud security, Network security is one of the main aspects to implement because the servers and computers talk through the network; if it is not secured properly it could lead to attackers sniffing all the data that is being transmitted to the user. As Abdul-Jabbar et al. (2020 para 1) mentioned "For networks, clouds are distributed over local area networks (LANs), wide area networks (WANs), and metropolitan area network (MANs)." If we look at the attack vectors in cloud computing one of the major attacks is Denial of Service as explained by Grance& Jansen, (2011) "A denial of service attack involves saturating the target with bogus requests to prevent it from responding to legitimate requests in a timely manner. An attacker typically uses multiple computers or a botnet to launch an assault."

Software Security. The implementation of secure coding practices is very important as the risk of data loss and data breach have increased rapidly. This can be done by incorporating security standards, ensuring the security of software in cloud computing is essential to protect sensitive data, applications, and infrastructure from potential cyber threats. One way to achieve this is through measures into the software development lifecycle, such as testing for vulnerabilities, data encryption, and access control, developers can build more secure applications and use the software that is up to date.

Risk Management For Newer Security Risks. As cloud computing continues to evolve, new security risks and threats emerge. To mitigate these risks, organizations must implement an effective risk management strategy that includes identifying potential threats, assessing their impact, and implementing appropriate controls. Some newer cloud security risks that organizations must address include insider threats, API vulnerabilities, and container security. To manage these risks, organizations can implement measures such as access controls, encryption, and monitoring of user activity. Additionally, organizations can work with cloud service providers to ensure that they have appropriate security measures in place and that they are compliant with relevant industry regulations and standards. It is also essential for organizations to regularly review and update their risk management strategy to ensure that it remains effective in addressing newer cloud security risks.

Organisations usually tend to concentrate on the core business. So they hand over all the security parts to some of the third party vendors. These vendors usually set the perimeter for the business. As we can see many organisations from the past few years have been migrating all their workforce and tasks towards cloud. On the contrary, some of the organisations were not willing to cloud due to the limited control.

Vulnerability and Threat Management. As in every field, Information technologyhas some vulnerabilities; even Cloud Computing also has some vulnerabilities which get updated on a daily basis as new vulnerabilities arise such as Zero-day Exploits. As it is very well explained by Al-Rushdan, et al. (2020) "The term "zero-day" refers to the number of days available to the software or hardware vendor to issue a patch for this new vulnerability. Currently, the best-known defence mechanism against the zero-day attacks focuses on detection and response, as a prevention effort, which typically fails against unknown or new vulnerabilities." Some of the vulnerabilities are well explained by Ramachandra, Mohsin , & Farrukh (2017) as well.
According to IBM "Threat management is a process used by cybersecurity professionals to prevent cyberattacks, detect cyber threats and respond to security incidents". Most of the Organisation use NIST Framework which guides the organisation to improve the security infrastructure as in the Cloud Computing Synopsis and recommendations (Lee , Tim , Robert , & Jeff , 2012).

Physical Security
Physical security in cloud computing is the protection of hardware, software, and data from physical threats. This includes protecting against unauthorized access, theft, damage, or destruction. Some of the key physical security measures that can be implemented in a cloud computing environment include physical access control, video surveillance, fire protection, environmental controls, and power protection. By implementing these physical security measures, cloud computing providers can help to protect their customers' data from physical threats. We can mitigate these threats by implementing proper Access Control, Video Surveillance, Power protection, and Regular auditing of physical security.
Infrastructure Security. Infrastructure security is a critical component of cloud computing, as it involves protecting the physical and virtual resources that make up the cloud environment. Infrastructure security measures include protecting data centers and servers, securing network connections, implementing access controls, and encrypting data. It is essential to ensure that physical security measures are in place to protect against theft, natural disasters, and other physical threats to the data center. Virtual security measures include the use of firewalls, intrusion detection and prevention systems, and data encryption to protect against unauthorized access, data breaches, and other cyber threats. Regular security audits and vulnerability assessments can also help identify and address potential security issues before they can be exploited by malicious actors. Infrastructure security is a complex and ongoing process, requiring constant vigilance and regular updates to ensure the highest level of protection for cloud resources.
Storage Security. Storage security is the protection of data stored on storage devices, such as hard drives, solid-state drives, and tape drives. It is important to protect data from unauthorized access, modification, or destruction. Ensuring storage security is critical in cloud computing to safeguard the confidentiality, integrity, and availability of data. Encryption is a crucial aspect of storage security, where data is converted into a form that can only be read with a decryption key which keeps data secure even if it is compromised. Access controls are very much important when it comes to Storage security and must be implemented to ensure that only authorized personnel can access the data which includes implementing user authentication measures such as multi-factor authentication, password policies, and role-based access control. Regularly monitoring and auditing storage infrastructure is also important to detect any unauthorized access or changes to data. In the event of a security incident, having a robust incident response plan in place can help to minimize the impact and ensure that the security of the storage infrastructure is maintained.

Performance Analysis
Performance analysis in cloud computing is the process of measuring and evaluating the performance of cloud-based applications and services which make sure that applications are performing as expected and that they are meeting the needs of users. Performance Analysis is Measured by Response time(It is the time taken for an application to respond to a user request.), Throughput (The number of requests that an application can handle per second.), Scalability (The ability of an application to handle increasing loads without performance degradation.), Availability (The percentage of time that an application is up and running.) all these details are to be discussed by the Cloud provider before making a Service Level Agreement.

Environmental Analysis
Cloud computing has a significant environmental impact, due to the energy consumption of data centres due to the transportation of data over the internet and associated carbon emissions. However, cloud providers have made efforts to increase the energy efficiency of their data centers and use renewable energy sources to power their operations. Use of virtualization technology and shared infrastructure can reduce the overall energy consumption and carbon footprint of cloud computing compared to traditional on-premises data centres. It is important for organizations to consider the environmental impact of their cloud usage and select providers that prioritize sustainability and transparency in their operations.
Organizations can optimize their cloud usage by implementing strategies such as using cloud services only when needed, optimizing resource allocation, and leveraging automation to reduce waste and increase efficiency. Overall, while cloud computing may pose environmental challenges, it also presents opportunities for reducing the overall carbon footprint of IT operations.

Legal Challenges

Cloud computing has raised a number of legal issues related to data privacy, security, and ownership. One of the main concerns is compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in the EU and the Health Insurance Portability and Accountability Act (HIPAA) in the US. Organizations must ensure that they are compliant with these regulations when handling sensitive data in the cloud, or risk facing significant legal and financial consequences. Another issue is the potential for breaches of data privacy, where third-party cloud providers may access or use data without consent. This raises questions about data ownership and control, and organizations must carefully review their contracts with cloud providers to ensure that they retain ownership and control over their data. In addition, issues such as intellectual property rights, liability for data breaches, and cross-border data transfers also present legal challenges for organizations using cloud computing. It is important for organizations to work closely with legal professionals to navigate these complex legal issues and ensure compliance with relevant laws and regulations as mentioned in Legal Concerns and Challenges in Cloud Computing (Krishnan & Lei , 2014).

Ethical Cloud Computing Analysis

Ethical issues in cloud computing such as Ownership arise when data is stored in the cloud, and it is often owned by the cloud computing provider. This means that the provider has the right to access, use, and even sell the data. This can be a problem for users who want to keep their data private. Accountability is another concern with cloud computing. When data is stored in the cloud, it is often difficult to determine who is responsible for the data. This is because the data may be stored on servers that are owned and operated by multiple companies. This lack of accountability can make it difficult to hold anyone responsible for data breaches or other problems. Privacy is a major concern with cloud computing. When data is stored in the cloud, it is often accessible to a wide range of people, including the cloud computing provider, its employees, and other users of the cloud. This can be a problem for users who want to keep their data private. Baig (2021) explained the Ethical issues concerning Cloud computing ethical issues in A review paper to investigate and provide suggestions for solving data privacy issues of cloud computing.

CONCLUSION

Cloud Computing provides businesses and consumers with numerous benefits such as cost savings, scalability, and accessibility to computing resources. However, there are also potential challenges that must be addressed to ensure successful implementation of cloud computing. These challenges include security, performance, legal issues, environmental impact, and ethical considerations. To address these challenges, it is important for organizations to conduct thorough security analyses, implement best practices for infrastructure and storage security, and ensure compliance with legal and ethical standards. With careful planning and management, the benefits of cloud computing can be fully realized while mitigating potential risks and challenges. As technology continues to evolve, it is important for organizations to stay up-to-date with emerging trends and best practices in cloud computing to remain competitive in today's digital landscape.

REFERENCES

[1]. Raghavendran, Ch. V., Ganti, N. S., Penumathsa, S. V., &Gummadi, J. M. (2016). A Study on Cloud Computing Services. International Conference and Expo on Advanced Ceramics and Composites 2016, 4, 1-6. Florida: International Journal of Engineering Research & Technology.

[2]. Varghese, B., &Buyya, R. (2018). Next generation cloud computing. Future Generation Computer Systems, 79(3), 849-861.

[3]. WANG, L. (2010). Cloud Computing: A Perspective Study. Ohmsha, Ltd. and Springer, 28, 139.

[4]. Rani, D., & Ranjan, R. (2014). A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, 4(6), 459.

[5]. Cloud Computing. (n.d.). Retrieved 4 17, 2023, from www.gartner.com: http://www.gartner.com/technology/topics/cloud-computing.jsp

[6]. Sen, J. (2021). Security and Security andPrivacy Privacy Privacy Issues in Cloud Computing. Research Gate(https://doi.org/10.4018/978-1-4666-6539-2.ch074), 5.

[7]. Patel, H. B., & Kansara, N. (2021, march). Cloud Computing Deployment Models: A Comparative Study. International Journal of Innovative Research in Computer Science & Technology , 9(2), 45-50.

[8]. Srinivasan, S. (2013). Is Security Realistic in Cloud Computing? Journal of International Technology and Information Management, 22(4), 51.

[9]. Abdul-Jabbar, Safa. S., Ali Aldujaili, Saja G. Mohammed, & Hiba S.Saeed. (2020, feb). JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, 55(1), 2.

[10]. Grance, T., & Jansen. W. (2011, dec). Guidelines on Security and Privacy in Public Cloud Computing Special Publication (NIST SP).

National Institute of Standards and Technology, 1-80.

[11]. Rushdan, H., Shurman, M. M., Alnabelsi, S. H., &Qutaibah, A.. (2020). Zero-Day Attack Detection and Prevention in Software-Defined Networks. IEEE, 1-6.

[12]. Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A Comprehensive Survey on Security in Cloud Computing. The 3rd International Workshop on Cyber Security and Digital Investigation , 110, 465-472.

[13]. IBM. (n.d.). What is Threat Mangement ? (IBM) Retrieved April 2023, from Threat management: https://www.ibm.com/topics/threat-management

[14]. Badger, L., Grance, T., Patt-Corner, R., &Voas, J. (2012). CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS. National Institute of Standards and Technology Special Publication 800-146, 1-81.

[15]. Krishnan, S., & Lei. C. (2014). Legal Concerns and Challenges in Cloud Computing. International Symposium on Digital Forensics and Security (pp. 81-85). Houston: ISDFS'14.

[16]. Baig, M. M. (2021). Cloud Computing Ethical Issues: A Review Paper To Investigate And Provide Suggestions For Solving Data Privacy Issues Of Cloud Computing. Turkish Journal of Computer and Mathematics Education, 7, 1433-1438.