Best Cloud-Based Solution

Liam Bergerson

CSU - Global

ITS442-1

R. Brown

3/12/23

Best Cloud-Based Solution

Cloud computing is a concept that is widely used by organizations around the world. More organizations are making the transition from traditional, on-premises data centers to the cloud. The migration from on premises data centers to the cloud is a complicated and arduous process. However, the transition can be smooth and effective with a well thought out plan. The CIO of my company is interested in hosting new and existing applications from the cloud. In order to determine which cloud computing solution will be used, several considerations must be discussed in order to maximize the benefits and limit the drawbacks. Factors such as cloud deployment models, service models, storage, security, management, and solution design are to be discussed in this paper.

Cloud Deployment Models

There are four primary cloud deployment models that organizations can choose from. They are the private cloud, public cloud, hybrid cloud, and the community cloud. When choosing a deployment model to use, many considerations must be taken into account. Scalability is crucial for optimal performance of operations. When network traffic experiences huge spikes, cloud resources must be scaled quickly to accommodate those spikes. Which cloud solution the organization is willing to pay for should also be considered. Many cloud solutions are too expensive compared to the amount of functions they offer. In-depth analysis of each cloud solution must be performed to determine a balance between cost and functionality offered. Accessibility of resources must

also be considered. When resources need to be quickly scaled up for network traffic spikes, latency can be a detriment. When choosing a cloud solution, data center locations must be considered in order to minimize any latency. Lastly, and perhaps, most importantly, security must be heavily considered. Cloud solutions assist organizations with performing functions and storing data. Proper security measures must be in place that protects the confidentiality and integrity of data, as well as the availability of operations.

Public Cloud

The public cloud is an environment completely managed by a third-party vendor in which organizations pay for their services (Hiral, 2021). The public cloud has no capital cost. It offers a pay-as-you-go model. Each cloud solution has a starting price for which organizations pay and the price scales based on resources used. Public cloud solutions also have low IT overheads. Overheads are the costs associated with day-to-day operations. Public cloud solutions have an extreme range of scalability. When organizations need to scale their resources to accommodate for traffic spikes, there is an extremely low chance that they will run out of resources to use. There is, however, a lack of customization with public cloud solutions. Since they are often owned and managed completely by the vendor, there are limited options for custom deployments. There is also a potential for latency. Data center locations are what need to be considered when limiting latency. If a data center is far away from the organization, there will be

more latency. Research can be done to determine where data centers are for a solution that is to be considered.

Private Cloud

The private cloud is an environment completely owned and managed by the organization (Hiral, 2021). The private cloud has an extremely high capital cost for implementation. That is because since it is on premises, proper equipment acquisition and configuration of equipment needs to be performed. High IT overheads are also associated with private cloud models because running the data center daily requires high costs. However, since it is fully owned and managed by the organization, it is fully customizable to the desires of the organization. Superior performance is also a benefit for the organization. Performance issues within public cloud models need to be fixed by the vendor, which can result in increased wait times. However, with a private cloud model, any performance issues can be immediately addressed because the data center is owned and managed by the organization. Functions tend to be underutilized with a private cloud model. This is because when functions are maximized to their limit, the cost drastically increases and the chance of equipment failure also increases. Higher levels of security can be achieved because proper security measures can be discussed and implemented. In a public cloud model, the organization is completely at the mercy of the vendor for proper security measure implementation.

Hybrid Cloud

The hybrid cloud is an environment made up of a combination of the public and private cloud (Hiral, 2021). The cost for implementing a hybrid cloud solution is somewhere in between a public cloud and a private cloud. It's not as high as a private cloud model, but not as low as a public cloud model. IT overheads are also somewhere in the middle because daily operations are both on the public and private cloud. Scalability is a benefit of hybrid cloud solutions because scalability is achieved through the public cloud. Since management of data is performed through the private cloud in a hybrid cloud, security is high. This is because configuration of security measures is performed by the organization. Since both private and public clouds are used, flexibility is maximized. This is because instead of just one or the other deployment models being used, both are used in combination for the maximum amount of benefits in both worlds.

Community Cloud

The community cloud is an environment where the infrastructure is shared by two or more organizations in a collaborative effort. The cost for implementing a community cloud is shared between all collaborators. The customizability of the infrastructure is dependent on what each organization in the cloud needs. Security issues are often difficult to handle because instead of just one organization having security issues, there are now two or more organizations with security issues. The community cloud is a less popular deployment model

because of the requirement of collaboration with other organizations on the infrastructure.

Cloud Service Models

There are three main cloud service models available today. They are Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). In order for this organization to determine which cloud service model will be chosen, several things must be considered. The cost of the service model must be considered. Service models have different costs because of the functionality they bring. Cost must be a primary consideration when choosing a service model. Accessibility must also be considered. Service models such as Software as a Service (SaaS) can be accessible anywhere because it lies in the web browser. If there is an abundance of remote workers, a SaaS solution may be desired. When organizations experience a spike in traffic, they will need a service model that will immediately accommodate for those spikes. Therefore, on demand scalability must be considered.

Software as a Service (SaaS)

Software as a Service (SaaS) is a cloud model in which the software application and underlying infrastructure is completely owned and managed by a third-party vendor (Shallal & Bokhari, 2016). Customers and organizations pay to use their services for their operations. SaaS solutions typically have a low cost of implementation. This is because SaaS solutions are generally known for their data storage and sharing capabilities. There is no need to install and run any

applications. SaaS solutions run directly from the web browser. Because of this, SaaS solutions can be accessed anywhere, at any time, on any device. The only thing that is required is some kind of connection to the internet. Updates and security patches are all done by the vendor, so there is no requirement for patching and updating by the organization. Since SaaS solutions are completely managed by the vendor, there are limited customizability options. If an organization wishes to have more customizability options, a SaaS solution may not be desired. Stated earlier, SaaS solutions handle patching and updates. This may not be desired for some organizations that have functionality or compatibility issues and choose to remain on older versions of software.

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is a cloud model in which vendors provide organizations with a development environment, private networks, secure data storage, and components for software development and testing. The cost of implementing an IaaS solution is reasonable because the equipment needed to run the infrastructure is owned and managed by the vendor. The organization does not need to purchase any equipment needed to run a data center. IaaS solutions also have on-demand scaling. If an organization encounters traffic spikes, resources can be scaled up quickly to accommodate those spikes. IaaS solutions are also extremely reliable. This is because workloads are spread across various data centers. If one data center experiences an outage, or is rendered unavailable, operations are still available. IaaS vendors completely

handle security with their solutions. The organization has little to no control over security. When an organization chooses an IaaS solution, they will need to research what kind of security measures are in place.

Platform as a Service (PaaS)

Platform as a Service (PaaS) is a cloud model that provides access to development tools and APIs for organizations. Users are granted access to virtual development environments for building, testing, and running applications. PaaS solutions offer fast development for applications. Projects can be completed on an accelerated timeline without affecting quality because of the ease of use. PaaS solutions have multi-platform capabilities. Instead of restriction to any one device or network, applications can be designed across many types of operating systems and devices. Applications can still be developed regardless of where the developer is. PaaS solutions offer remote capabilities that enable remote workers to still develop and release applications. As with IaaS solutions, organizations have little to no control over security measures with PaaS solutions. PaaS solutions are also lacking in scalability, however, this is not to say that PaaS solutions do not offer scalability. The scalability technology for PaaS solutions is a little more rigid which challenges organizations that look for growth. There also is an increased risk of hardware compatibility issues with PaaS solutions. Since PaaS solutions are managed by the vendor, organizations are at the mercy of vendors with what hardware is compatible with each other. When

organizations choose PaaS solutions, compatibility is a primary aspect to consider.

Cloud Data Storage

Cloud data storage is a crucial aspect of cloud computing as it is where sensitive data is stored. Many considerations have to be taken into account in order for sensitive data to be properly protected. Organizations need to look for proper security capabilities when choosing a cloud data storage platform. Sensitive data is still vulnerable to threat actors without any, or adequate, security measures. To ensure full protection of data, proper security measures must be in place. Price needs to be considered as well. If an organization is not getting the full range of use of a platform that is overpriced, they are wasting their money. A balance between features and price for those features needs to be determined when choosing a cloud data storage service. Data center locations must be determined to maximize the availability of data. If the data center is far away, availability may be affected due to latency. A cloud data storage service must also have multiple other data centers in case one data center is rendered unavailable. When the organization encounters a problem that is out of their control, the tech support team needs to be connected to handle the problem. When choosing a cloud service, the tech support team must be timely and efficient when responding to problems.

Cloud Security

Cloud security is another crucial aspect of cloud computing as it governs how sensitive data is protected. In order for organizations to determine what cloud provider is to be chosen, multiple security measures have to be in place. Authentication methods will further secure the login process. A username and a password is simply not enough to secure the login process. Those credentials can be discovered by a threat actor. A multi-factor authentication service will further secure the login process by requiring the user to input a randomly generated number code via a third party application. Proper encryption methods must be in place in order to obfuscate data in cloud repositories. Advanced Encryption Standard encryption will encrypt data to make it unreadable to the user unless a decryption key is provided. While talking about encryption, the cloud service must have an encryption key management system in place so as to not lose track of encryption keys. As more data is encrypted, the keys used to decrypt data accumulate and can easily become unorganized. The organization must have a proper access management system in place to limit the amount of access users have. If every user has elevated privileges, a threat actor will have more points of entry into the systems and networks of the cloud service, therefore, resulting in an increased risk of stolen data.

Cloud Management

Cloud management is a concept that refers to the exercise of control over cloud infrastructure resources and services. In order for workflow efficiency to be

maximized, several considerations must be discussed (Semilof et al., 2021). Security management is not the sole responsibility of the cloud provider. Organizations must also take responsibility in order to protect sensitive data. Configuration management ensures that all systems are configured correctly to minimize vulnerabilities from misconfigurations. Proper logging and access management is also another responsibility of the organization. As discussed earlier, access management ensures that every employee only has the necessary permissions in order to perform their work operations. This is otherwise known as the principle of least privilege. Log management is also crucial as logs can tell the administrators if there are any suspicious actions being done. Proper management of logs will ensure that every operation is tracked to ensure that any data breaches can be identified immediately.

Cloud Solution Design

Within the cloud solution design, there are functional and nonfunctional requirements that need to be considered. Functional requirements are features that must be implemented to enable the users to achieve their goals (Scand, 2021). A functional requirement is what an application must or must not do when data is inputted. Functional requirements show software developers how the system is intended to behave. If the system does not meet the functional requirements, the system doesn't work properly. Nonfunctional requirements determine the performance standards and quality attributes of software, system usability, effectiveness, security, etc. (Scand, 2021). Nonfunctional requirements

describe how the system does an operation. For example, a website must handle more than one million users without any performance decline, or a website must not load for more than three seconds. If nonfunctional requirements are not met, user experience will be negatively impacted.

Conclusion

There are many factors to consider when making a cloud computing decision. When an organization is interested in hosting existing and new applications in the cloud, several aspects of cloud computing must be considered. The deployment model, service model, storage, security, management, and solution design must be thoroughly discussed in order for an organization to choose a cloud computing solution or multiple solutions in order to satisfy these aspects.

References

Hiral, P. (2021). *Cloud Computing Deployment Models: A Comparative Study*. Researchgate. https://www.researchgate.net/publication/350721171_Cloud_Computing_Deployment_Models_A_Comparative_Study

Semilof, M., Bigelow, S. J., & Casey, K. (2021, July 12). *What is cloud management? Everything you need to know*. Cloud Computing. https://www.techtarget.com/searchcloudcomputing/definition/cloud-management

Shallal, Q., & Bokhari, M. (2016). *Cloud Computing Service Models: A Comparative Study*. Researchgate. https://www.researchgate.net/publication/333117926_CLOUD_COMPUTING_SERVICE_MODELS_A_COMPARATIVE_STUDY

Scand. (2021). *Functional vs Non-Functional Requirements: The Definitive Guide*. https://scand.com/company/blog/functional-vs-non-functional-requirements/