Science and Technology 2019, 9(1): 7-11
DOI: 10.5923/j.scit.20190901.02

Cloud Migration- Risks and Solutions

Simanta Shekhar Sarmah

Business Intelligence Architect, Alpha Clinical Systems Inc, USA

Abstract A real IT revolution, cloud computing offers businesses the opportunity to save money and simplify their IT infrastructure, while increasing productivity. The migration to the cloud remains complex; we must choose an efficient and secure solution adapted to the business strategy. This paper gives and overview on Cloud Computing and its various compositions. The paper also describes the advantages and disadvantages of migration to cloud and discusses the security challenges and risks of Cloud. Finally, the paper presents solutions to reduce risks and How to reduce risks and to develop security in Cloud.

Keywords Cloud Computing, Cybersecurity, Security threats, Security risks, Cloud Security

1. Introduction

Cloud computing [1] is a very popular technology among the companies because of its backup services. As an ideal solution to deliver enterprise applications, Cloud Computing technology is being adopted in small to large-sized enterprises. Indeed, the benefits of Cloud Computing are numerous. The cloud has many types of offerings, as does have many cloud service providers. This paper discusses the various solutions proposed, their advantages and disadvantages which would help to opt for the cloud solution most suited to base on the modes of operation. The cloud offers many benefits to companies wishing to outsource all or part of their IT infrastructure:

1.1. A Reduction of Costs

Cloud services are less expensive than traditional physical systems and costs are phased in via a monthly subscription.

1.2. Improved Productivity

Cloud services improve the management of IT resources. They are easy to use and easy to configure.

1.3. Optimal Flexibility

The IT department is freed from the management and support of its IT infrastructure on a daily basis.

1.4. A Favoured Professional Mobility

Cloud enables employees to work together remotely via online backup with real-world data processing.

2. The Composition of the Cloud [2]

Cloud security is often considered a duty of the service provider. By adopting the cloud, some companies believe they are offloading a significant burden. To illustrate the level of responsibility, three models must be distinguished.

Virtually all the company's IT services are designed to find its way into cloud computing, but there are generally three service models:

2.1. The Software as a Service (SaaS) Application

This application, managed entirely by the Cloud Computing provider, replaces or complements client-managed applications. It can be mail clients (Gmail), sales management software (Salesforce), data storage software (drop box), etc. For the customer, this type of offer allows to completely outsource the technical management of the application and the underlying infrastructures (servers, network, operating systems, etc.). On the other hand, the software offered is generally very standardized and the client cannot adapt it to particular needs. This is why the SaaS service still rarely deals with business applications. Another disadvantage with SaaS is the customer does not control the data processing, the provider can for example outsource hosting without having to ask permission from its customers.

2.2. The Platform as a Service (PaaS)

In this type of cloud services, the customer uses an online service to develop [11] and execute specific applications implemented by him. Google App Engine and Windows Azure are such examples. This type of service, intermediate between the other two services, allows the customer to

* Corresponding author:
sarmah.simanta@gmail.com (Simanta Shekhar Sarmah)
Published online at http://journal.sapub.org/scit

benefit from a certain level of abstraction on the infrastructure while being able to personalize the applications as per customer's needs. Hence, the customer gains flexibility, but in a technical environment defined by his supplier.

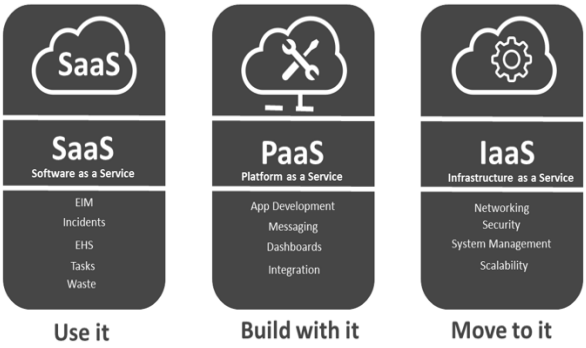

Figure 1. Service models of Cloud

2.3. The Provision of Infrastructure (Infrastructure as a Service or IaaS)

It consists of with an offering of a service for data storage, computing capacity, network capacity or any other type of IT resource. Amazon Web Services offers, for example, a data storage solution (Amazon S3, for Simple Storage Service), but also a computing infrastructure solution (Amazon EC2, for Elastic Compute Cloud). This type of service allows the client to delegate only the physical and logical management of the infrastructure, but to define itself the software and operating systems used. In addition, the customer has greater control over the processing done with his data, with the exception of their location (and possible backups and redundancies).

3. Types of Migration Benefits and Weakness? [3]

The cloud can bring value to your organization on the platform where the infrastructure is deployed. Yet before reducing the IT site size for the service provider model, you must understand the features, benefits, and limitations of the cloud.

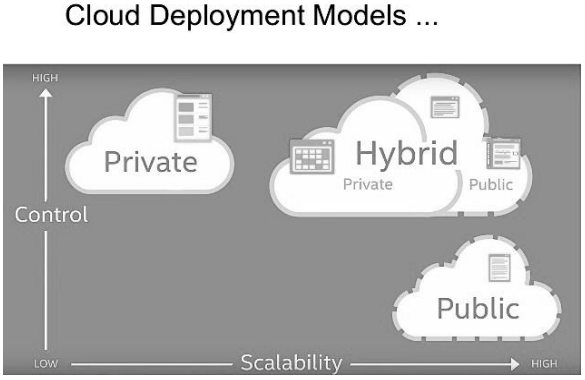

Figure 2. Cloud deployment models

3.1. Private Cloud

The private cloud, also called Cloud Dedicated is a backup mode dedicated to a single company. The goal is to share information within a single company. Each of your collaborators will have access to all or part of the documents, files saved on the private cloud of the company (according to the authorizations set up for each user), and this from any device, to any moment and in the premises of your company or outside which is ideal for promoting remote work.

Private cloud offerings give organizations direct control over their data and minimize IT security risks (for example, you no longer need to mobilize a team to maintain your servers).

3.1.1. Benefits of the Private Cloud

Organizing your private cloud fits perfectly with your local organization. You will have the opportunity to organize scores as you see fit.

In addition, experts recommend this type of cloud because it offers a good level of security, whether in terms of its execution or its mode of access. Indeed, a private cloud is accessible only through secure private network links, and not via the public Internet.

3.1.2. Disadvantages of the Private Cloud

Setting up this infrastructure is more expensive than renting a partition in a public cloud. In addition, this cloud mode will be less responsive in the event of "hard" data load.

3.2. Public Cloud

The public cloud is also called shared cloud. As its name implies, this cloud backup mode is not just for your organization and instead you rent a partition. Many companies opt for this cloud solution which is much more flexible in case of increased needs. OneDrive, Microsoft's public cloud available in Office 365, is probably the best-known example of Public cloud.

3.2.1. Benefits of the Public Cloud

The time and cost of implementation are derisory because you have an existing infrastructure. In addition, you will pay only according to your use, according to the model "Pay as you use". This backup mode is very flexible and remains very efficient and responsive in the event of a sharp increase in your storage capacity requirements.

In addition, as the company does not buy hardware or software, there is no question of maintenance as this part being provided by the service provider.

3.2.2. Disadvantages of the Public Cloud

Since the public cloud will adapt to your needs, it is therefore possible that the cost of subscription would increase over time, but this is necessary to cope with the

stored volume. In addition, with the existing infrastructure, it is possible that it does not stick perfectly to your business as time passes.

Limitations include the configuration, security, and specificity of service level agreements, making it a less than ideal solution for organizations that use sensitive data subject to compliance rules.

3.3. Hybrid Cloud

This cloud data backup solution is often used by large organizations with complex organizational structure and needs. The idea is to use private and public cloud solutions, independent of each other, while maintaining the possibility of portability of this data. Opting for a hybrid solution makes it possible to benefit from the power of public solutions for non-sensitive data.

3.3.1. The Benefits of the Hybrid Cloud

It has the advantage of cost saving for the company because it only pays for the public part of its infrastructure only when it is needed.

In addition, its workload is contained in a private cloud, but it retains the ability to spontaneously increase the latter and achieve peak usage on the public cloud. In addition, the hybrid cloud provides both a centralized on-premise infrastructure and scalable and flexible servers.

3.3.2. Disadvantages of a Hybrid Cloud

While Hybrid cloud can save some costs, which can benefit the business, there are some disadvantages too using a hybrid cloud.

One of the disadvantages that Hybrid cloud has is that deployment requires IT experts to ensure maximum data security. For this reason, moreover, most companies opt for this type of solution to store non-sensitive data.

There is also the compatibility issue that may arise because a successful on-site infrastructure may not be able to function properly with a less efficient public infrastructure, which can affect the effectiveness of the hybrid cloud. However, with the use of expert services and the adoption of appropriate resources, the disadvantages of the hybrid cloud can be avoided.

4. The Security Challenges and Risks of Cloud [4]

There are several security challenges related to cloud migration to know

While cloud computing has many advantages, the implementation of cloud migration raises many issues. Several options relating to the type of cloud environment exist (private cloud, public, hybrid, etc.). It is important to choose the option that best meets the company's strategic requirements and ambitions, considering the following elements:

1. New solution or evolution of an existing solution?

Acquiring a new solution and deploying it requires many resources, know-how and time. For structures that do not, the public cloud is a suitable solution.

2. Criticality of solutions and strategy [10]

For strategic activities, companies seek to maintain greater control over the associated IT solutions (customization, configuration, management, etc.). For these uses, hybrid or private cloud is recommended.

3. Sensitivity of the data

To protect confidential data, two options are recommended: a private cloud system or a hybrid system (running applications in a public cloud and storing sensitive data in a private cloud).

Because of its operation, cloud computing involves both risks for the customer and technical and operational risks due to the loss of control of the customer on his own data processing. It also introduces new risks, whether for sharing responsibilities, data localization or pooling, for example there are 3 risk related to cloud.

4.1. Risk 1: A Shared Responsibility Difficult to Manage

In the law Informatique et Libertés, the "controller" is the entity that determines the purposes and means of treatment. Conversely, the role of the "subcontractor" is limited to executing the orders of the manager and carries little responsibility. In the case of cloud computing, however, the division of responsibilities is not easy: if the client necessarily assumes responsibility for the IT treatments he chooses to implement, the qualification of the provider is more complex. In particular, it can be seen that public cloud offers (especially SaaS applications) are almost entirely defined by the service provider. In addition, suppliers often remain intentionally vague about the security measures they use because they consider this information as commercially sensitive and likely to generate attacks in case of disclosure. This choice of security by the darkness and the difficulty or even the impossibility for the customers to carry out audits of their supplier leave these totally dependent on the supplier, even though the regulatory obligations, notably in terms of security, continue to weigh on the customers.

In the case of individuals using cloud computing services, this imbalance is even more obvious because people are not able to understand the information provided by the service provider. For example, a large number of users of the DropBox service were convinced that their data was protected by an encryption mechanism whose key depended on their password, when in fact the encryption keys are defined by DropBox.

4.2. Risk 2: Uncertainties about the Location of the Data

The geographic location of the data is not a problem when IT processes are managed internally or even outsourced conventionally. Cloud computing, on the other hand, often results in a geographical spread of data, which

the customer may not be able to control.

Indeed, the fact that cloud services are accessible over the Internet allows a cloud provider to pool on a single infrastructure the services used by its customers in Europe, the United States and Asia, because the peak loads of each zone will be shifted in the day. In return, in many cases, the data is hosted on a single potentially localized infrastructure in the United States.

In practice, leading cloud vendors use multiple [13] data canters around the world, and data can move from one data center to another, depending on their respective load and how often they are used. Thus, for a European user of an e-mail service, it is quite possible that his inbox is stored in Europe during the day, then in Asia during the night, and that his archived mails are stored at United States. This organization also ensures better availability and latency for customers.

4.3. Risk 3: Risks Related to the Use of Shared Resources

In terms of security, the main novelty of the Cloud is related to the use of shared IT [14] resources between several organizations. The reliability between the different treatments of the different organizations will be guaranteed only by the logical security measures implemented by the provider Cloud and its policy of management of the authorizations.

In case of failure of these security mechanisms, the risks of breach of data confidentiality are extreme. The Drop Box online storage service has recently been the subject of such a failure: an update of the service has rendered the access control mechanisms inoperable, allowing at least one user to access data from other accounts [5]. Detected quickly, the flaw could however be corrected.

More generally, any security vulnerability or problem affecting the availability of the service can potentially impact all the customers of a provider, and therefore also the people whose data is being breached. In this respect, suppliers generally indicate the level of availability they achieve, but not all of them agree to enter it in a contract as a Service Level Agreement (SLA).

Finally, with cloud, network access is crucial, especially if business applications are hosted in the cloud. In case of a malfunction of the access of the customer or the supplier, the whole organization will be strongly impacted.

5. Risks Mitigation and Offered Solutions to Secure Cloud [5]

To reduce the risks, in general [15], the move to Cloud computing requires a change in the company's approach to IT services: the abandonment of the technical and operational management of infrastructure must be compensated by a strengthening of the management of the supplier's services. The move to the cloud also implies a change in user practices: as an example, the security issue with user authentication becomes much more crucial when the data of the company is accessible from any station connected to the network such as Internet. For the customer, the transition to the Cloud therefore requires a thorough review of internal procedures and investment in staff training.

As a best practice to protect data in the cloud [9], it is mandatory to ensure that providers and client follow the methodologies of data security assurance mechanisms and security solutions.

5.1. Insurance Mechanisms for Providers

5.1.1. Security Standards

Use of PCI DSS Level standard usually opted by Payment card industry with Data Security Standard [6].

5.1.2. Audits et Certifications

Auditing consists of verifying the data, records, operations and performances (financial and other) of a company.

5.1.3. The IS02700X Standard [7]

It offers an IS management system that ensures the appropriate selection of security controls that protect the company's assets while giving the parties (trusted company, customers, service providers) access to the system.

5.2. Security Solutions for Clients

5.2.1. Data Localization

Clients should be able to locate geographically its data and should be able to assure its customers that their data are stored in the country where they reside. [15] Proper Plans should be in place for the retrieval of information in case of judicial seizure (ex: mail hosted in the Cloud).

5.2.2. Data Protection

There are several encryptions methods which could offer better security on cloud based on various situations.

1. Data encryption: Applicable for data encryption in the databases or in the files.
2. Transparent encryption: This encryption is an On-the-fly encryption by the application or database: easy in SaaS mode. Encryption keys are necessarily stored in the cloud and hard to deny cloud administrator access to keys.
3. End-to-end encryption: The keys are held by the end customers. Cloud provider cannot decrypt data but requires a client or encryption proxy (difficult in SaaS mode).

5.2.3. User Authentication

There are several authentication methods used in cloud and these methods would mainly rely on based on the suitability for various applications and budget.

a. API Keys- This type of authentication authenticates users by associating a key to a project. This type of authentication is vulnerable and as they are less secured.
b. Firebase- This type of authentication is used to authenticate users to an app (both mobile and web app).
c. Google Authentication: In the method, the user is authenticated by allowing the users to login to their google account.
d. Auth0- This type of authentication is used to authenticate both apps and API. Like Firebase, it also can be used to authenticate both mobile and webapp.

There are three possible solutions:

1. 2 separate directories (company + Cloud) with synchronization.
2. Authentication delegation.
3. Federation of identities (SAML, WS-Federation...) of the ISD.

5.2.4. Authorization and Access Control

1. Establishment of fine access permissions on resources and resources data.
2. Prohibit generic accounts and account sharing.

5.2.5. Traceability

Two types of needs:

1. Monitoring access to resources in the cloud.
2. Investigation / forensics in the event of an incident.
   - Collect sufficiently complete traces (centralize or cross log logs).
   - Protect access to traces by the cloud provider.
   - Organize the consultation or the transmission of the logs to the customer of Cloud.
   - Plan to purge the logs beyond a certain period.

6. Conclusions

Cloud computing, a multifaceted concept covering a wide range of services from hosting to the management of all the business applications of a large group, is a major development in information technology, for small to large size businesses.

The implementation of these new services, however, requires a complete review of the procedures and security measures to be implemented within the company as the successful transition to cloud computing is not so simple that the providers want to believe.

In addition, the regulatory framework imposes several constraints on treatments, especially when they [8] include personal data. It also maintains the primary responsibility of the customer who chooses to use the cloud, even when, in practice, he can hardly control the provider.

Therefore, it is advisable to consider a transition to the Cloud in a gradual manner, starting with low-risk treatments, and carrying out risk analyzes covering the technical, legal and business environment in order to achieve this transition in all security for both client organizations and people whose data is getting migrated to the cloud.

REFERENCES

[1] Predictions 2018: Cloud Computing Accelerates Enterprise Transformation Everywhere - Dave Bartoletti, Vice President, Principal Analyst, Nov 7 2017.

[2] Cloud: Computing Services And Deployment ModelsCh Chakradhara Rao1, Mogasala Leelarani2, Y Ramesh Kumar.

[3] https://www.levelcloud.net/why-levelcloud/cloud-education-center/advantages-and-disadvantages-of-cloud-computing/.

[4] A Review of Challenges and Security Risks of Cloud Computing - Hussam Alddin S. Ahmed, Mohammed Hasan Ali, Laith M. Kadhum, Mohamad Fadli Bin Zolkipli, Yazan A. Alsariera.

[5] Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions - (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[6] A Survey of Challenges Facing PCI DSS Compliance in Cloud Environments, Kenga M. Derdus, May 2016.

[7] Information Security Management System - International Journal of Computer Applications (0975 – 8887) Volume 158 – No 7, January 2017, Sahar Al-Dhahr, Manar Al-Sarti, Azrilah Abdul Aziz, PhD.

[8] Simanta Shekhar Sarmah, Data Migration, Science and Technology, Vol. 8 No. 1, 2018, pp. 1-10. doi: 10.5923/j.scit.20180801.01.

[9] Karve, Shrikant V., et al. "Cloud based data migration and replication." U.S. Patent No. 9,075,529. 7 Jul. 2015.

[10] Zhang, Gong, Lawrence Chiu, and Ling Liu. "Adaptive data migration in multi-tiered storage-based cloud environment." 2010 IEEE 3rd International Conference on Cloud Computing. IEEE, 2010.

[11] Subash Thota, The Cloud Promise (Moving Data to Cloud), Advances in Computing, Vol. 7 No. 3, 2017, pp. 74-79. doi: 10.5923/j.ac.20170703.02.

[12] Noorzaei, J., Viladkar, M. N., Godbole, P. N., 1995, Influence of strain hardening on soil-structure interaction of framed structures, Computers & Structures, 55(5), 789-795.

[13] Ferris, James Michael. "Data compliance management associated with cloud migration events." U.S. Patent No. 9,052,939. 9 Jun. 2015.

[14] Khajeh-Hosseini, Ali, David Greenwood, and Ian Sommerville. "Cloud migration: A case study of migrating an enterprise it system to iaas." 2010 IEEE 3rd International Conference on cloud computing. IEEE, 2010.

[15] Beserra, Patricia V., et al. "Cloudstep: A step-by-step decision process to support legacy application migration to the cloud." 2012 IEEE 6th international workshop on the maintenance and evolution of service-oriented and cloud-based systems (MESOCA). IEEE, 2012.