EAI Endorsed Transactions
on Cloud Systems
Research Article EAI.EU

Challenges of Cloud Solutions Adoption in Large Corporations

Aqeel Alsadah[1,*], Hussain Alhajjaj[1]

[1]SaudiA Aramco, Corporate Applications Department, Saudi Arabia

Abstract

The concept of cloud-provided IT solutions has changed from being an emerging technology to a reality that most large corporations have adopted or are planing to adopt. Accordingly, many companies have already moved some of their applications or a portion of their infrastructure to the cloud. This adoption varies between the different categories of cloud offerings: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). This paper will discuss the challenges of cloud adoption from the three perspectives of successful organizations: people, process, and technology.

Received on 11 November 2018; accepted on 12 February 2019; published on 15 March 2019

Keywords: cloud, cloud challenges, cloud adoption

doi:10.4108/eai.13-7-2018.158415

1. Introduction

Cloud computing has recently emerged as an effective technology that enables businesses to host and deliver services over the Internet. According to IDG Enterprise's 2016 Cloud Computing Executive Summary [1], 70% of participating companies have already moved at least one application or a portion of their infrastructure to the cloud. Namely, moving computing services to the cloud helps corporations to achieve increased business agility and flexibility. Deployment of services, whether Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS), is faster than the traditional on-premises approach and the end-to-end time to market is significantly reduced [2]. Financially, cloud services operate on a subscription model, which relieves corporations from the challenge of long term capital planning. Additionally, the operational cost of delivery, maintenance, and support of cloud services is generally lower than on-premises hosted services, which results in reduced Total Cost of Ownership (TCO). According to Nasdaq Cloud Computing: Industry Report and Investment Case [3], organizations may incur 30% in cost savings if they were to switch from an on-premises infrastructure (i.e., having physical servers, databases, etc.) over to a cloud framework ($630 per core per month compared to $440) as shown in Figure 1. Cloud solutions can also be scaled up or down easily to meet business demand without the need for costly projects and resources. Last but not least, most cloud providers invest heavily in new technological trends and innovative solutions such as the Internet of Things (IoT), machine learning (ML), and artificial intelligence (AI), which gives cloud consumers the advantage of leveraging the latest technologies and innovations.

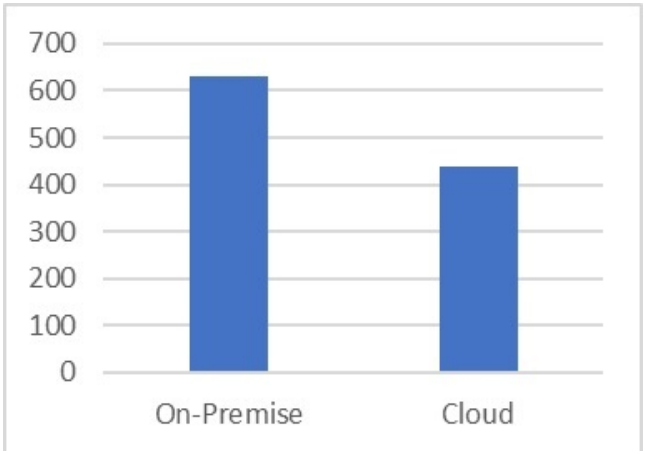

Figure 1. Cost of Ownership – On-Premises vs. Cloud ($ per Core per Month)

*Corresponding author. Email: ageel.sadah@aramco.com

Despite the above listed advantages and benefits of cloud computing, they are challenging to achieve and require organizations to perform extensive analysis and planning before making the decision to move to the cloud [2]. This paper sheds light on these issues and discuss various challenges of cloud adoption in large corporations. Examples of these challenges are: business-case justification, vendor lock-in, data privacy and security, integration with on-premises systems in hybrid architecture scenarios, and business transformation. Most of the challenges discussed in this paper are real challenges we faced at Saudi Aramco while transforming major business processes such as Human Resources (HR) and Supply Chain Management (SCM) to the cloud. Additional challenges are lessons learned from the literature and analyzing the experience of other companies during our cloud adoption journey [4].

2. Business Case Justification

According to Nasdaq Cloud Computing: Industry Report & Investment Case [3], IT cloud spending has been increasing and will continue to increase through 2020, from $77 billion in 2015 to $205 billion in 2020. There are also similar trends for private and hybrid cloud spending as shown in Figure 2.

Organizations seek maximum Return on Investment (ROI) out of this huge spending on cloud solutions. Most cloud implementation initiatives sound very promising in terms of cutting cost and ROI at the beginning. However, several hidden cost elements are discovered later during implementation and post-implementation operations that inflate the total cost of ownership (TCO) and cause the business-case justification for cloud adoption to fail. Examples of these hidden cost elements are network redesign to meet minimum bandwidth requirements from cloud solution providers (CSPs) and additional middle-ware components required to maintain integration with on-premises systems. These hidden cost elements must be considered during the planning phase to avoid the failure of the business case justification [5].

The subscription model (pay-per-use) of cloud-based solutions makes it easy and attractive for organization to scale up. However, this scalability often involves cost implications, which must be considered and planned to avoid cost inflation of cloud adoption initiatives.

In addition, several organizations begin their cloud adoption initiatives with the aim to decommission locally managed on-premises systems. However, they end up moving partial functions to the cloud while maintaining some other functions in legacy on-premises systems. This can be due to multiple reasons such as slow business transformation or legality/data privacy issues. Maintaining both systems in parallel defeats the purpose of cloud adoption and can fail business-case justification.

Planning the cloud migration properly and aligning it with any required business transformation is the solution to mitigate the risk of business case justification failure. Planning should consider all hidden cost elements and future growth to solidify the business case.

3. Vendor Lock in

Many companies find themselves locked to the technology provided by a single Cloud Service Provider (CSP) or locked in a long-term contract that makes the situation extremely costly and difficult to migrate to an alternative CSP, which offers more attractive services. Another possible reason for vendor lock in is acquisition of one or multiple CSP(s) by a larger provider as part of market consolidation [5].

Several preventive measures should be considered to mitigate the above risks of vendor lock in:

- Soliciting services from well-established and mature CSP(s) minimizes the risk of acquisition by a larger CSP and hence being locked to a single vendor.
- Capitalizing on open-source technologies whenever possible, which can simplify movement around different cloud technologies and different vendors.
- Adopting hybrid cloud strategy that involves the selection of multiple best-of-breed cloud providers for different business functions. Despite the increased complexity of management and integration in this option, it significantly decreases the risk of vendor lock in.
- Considering all variables and aspects such as performance, cost, and service levels when

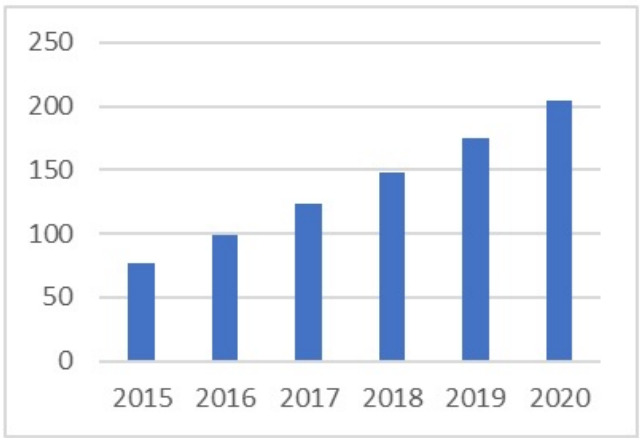

Figure 2. Public IT Cloud Spending ($Billions)

performing evaluation and comparison between multiple vendors, which helps in making the right selection and long-term sustainability of the selected vendor.

4. Data Privacy and Security

Data privacy and security continues to be a major concern for most cloud consumers. Moving critical corporate data out of tightly controlled and monitored on-premises environments creates a psychological fear: will the public or hybrid cloud be more secure than my locally managed data center? Any data breach can jeopardize the reputation of the affected company and can also lead to financial and market share loss [6, 7].

Although most of the customer data is stored in shared infrastructure managed by CSPs, the providers are required to comply to strong government regulation rules such as The European Union General Data Protection Regulation (GDPR). These regulations and the penalties associated with them makes data privacy and security top of the priority list for most reputable cloud providers.

Having said that, companies must take additional security measures when moving corporate data out of locally managed data centers. These measures include, but are not limited to, strong data encryption mechanisms, digital certificates, and two-factor authentication. Additional measures are also required when running Infrastructure as a Service (IaaS) model such as anti-virus tools, intrusion detection, and denial-of-service (DoS) attack monitoring [8].

When running a hybrid architecture scenario where there is integration between locally managed IT solutions and the cloud, it is important for companies to have full understanding of the security architecture of their cloud provider(s). There have been many integration failures due to the misalignment of security measures such as firewall rules and encryption/decryption methodologies.

Another recommendation and lesson learned from best practice cloud implementations is to the creation of a secure communication channel to the cloud provider environment. This can be achieved by whitelisting the company's IP addresses, allowing traffic only from these whitelisted addresses, and blocking traffic from all other sources.

Last but not least, companies should follow an adaptive security approach when guarding their data in the cloud based on the classification of the data and the regularity requirements associated with the data classification. Companies should not spend the same resources and spin their wheels to protect publicly available company data similar to the efforts they spend to protect their employees' confidential information as an example [9].

5. Integration with On-premises Systems

Transferring IT infrastructure and applications to the cloud in large corporations is usually done in a phased approach. Therefore, companies will mostly end up maintaining a portion of their IT infrastructure on-premises while gradually transforming some business functions to the cloud in a hybrid architecture model. A hybrid cloud architecture creates a challenge of maintaining integration between on-premises and cloud systems. Many cloud transformation projects have failed due to the challenges of this integration.

5.1. API Limitations

SaaS cloud vendors provide Application Programming Interfaces (APIs), which allow consumers to perform operations on their data stored in the cloud. The challenge of using these APIs to implement integration comes in the following forms:

- Most cloud vendors put limitations on the number of transactions or amount of data exchanged through these APIs. This limitation is set by the vendors to control performance and prevent excessive load on their cloud environments. This challenge enforces customers to continuously optimize their integration architecture and minimize data exchange and transactions.

- APIs provided by cloud vendors usually expose only a subset of the data model. Even when data entities are exposed, customers need to ensure that all the properties of these data entities are accessible via APIs. This challenge becomes particularly visible for consumer created custom elements, which sometimes require additional development by the cloud vendor to be exposed via APIs. This development can incur additional charges from the cloud vendor.

- APIs provided by cloud vendors do not support full CRUD (Create, Read, Update, and Delete) operations on certain data entities. Similar to the previous challenge, supporting missing operations require additional development by the cloud vendor with its corresponding additional charges if not agreed in the contractual agreement.

5.2. Data Migration

This part of the integration is particularly challenging when loading a large amount of data during initial migration from on-premises to cloud environments. There are three approaches to overcome this challenge:

- Parallel processing: large data migration is divided into separate processes that are executed in parallel. In this approach, special attention

needs to be paid to the relationships between different data entities to avoid data integrity issues.

- Incremental loading: In this approach, data is typically migrated during downtime when users are off the system. In an incremental loading approach, data is moved based on change date from oldest to newest. The two systems eventually synchronize to the point that downtime for cutover is only based on the data change rate, not the size of data.
- External key cross referencing: This method works by linking keys across systems in a highly available local data store, which speeds up access by limiting search overheads.

5.3. Data Governance

Maintaining integrity of the data between on-premises and cloud systems is a major challenge in a hybrid cloud model. Integrity becomes particularly an issue when periodic polling is used to exchange data between the two systems. If data changes multiple times within a polling period, the details of the interim changes are lost. For maintaining high levels of integrity, it is recommended to build integration solutions triggered by data being changed rather than relying on polling. As a lesson learned from best practice cloud implementations, it is highly recommended to use a middleware as an Enterprise Service Bus (ESB) to implement integration between on-premises and cloud systems. An ESB architecture helps in systems decoupling, and monitoring and troubleshooting of exchanged integration messages, and integration can be easily extended in the future by plugging new components to the enterprise bus in a service-oriented architecture (SOA).

6. Business Transformation

Many cloud transformation initiatives have failed in the past for one single reason: trying to mirror on-premises systems in the cloud. There is no one-size-fits-all when it comes to SaaS cloud solutions. Cloud providers will never be able to build solutions that satisfy the specific business processes and customizations of all customers. Cloud providers would rather focus their efforts on building solutions that implement best practices and satisfy the needs of the majority of customers.

Successful cloud implementation is a journey that requires business transformation. Companies must focus their efforts on minimizing complexity, reducing special features that might be relevant to a few number of users, and emphasizing features that bring value to the corporation.

Change management teams play a vital role in this business transformation. Their role is to create the alignment between a company's specific procedures and processes and the worldwide best practices adopted by cloud providers. While some specific procedures and processes can be implemented in the cloud by configuring or extending SaaS cloud solutions, others must be changed to follow best practices or kept in on-premises systems.

7. Human Resources Challenge

When it comes to the skills required for cloud adoption, there is a paradigm shift. Organizations have been experiencing major gaps, especially in the areas of security and integration. This will require organizations to shift resources, hire new resources, and invest heavily in training their existing staff in new skills and technologies. In addition, organizations responsible for managing locally hosted physical infrastructure are subject to downsizing/restructuring as a result of cloud adoption.

From the business perspective, the implementation of SaaS solutions gives more power to business analysts as most of the business scenarios can be achieved via configuration of SaaS cloud applications and require zero or less development from IT teams. This gives IT teams opportunities to focus on strategic long-term initiatives that bring value to the organization rather than the routine maintenance of on-premises systems.

8. Conclusion

Organizations investing in cloud solutions and technology have a huge potential to unlock. The unlocked benefits include, but are not limited to: business agility, cost saving, shorter implementation cycle time, scalability, and the leveraging of the latest innovations.

This paper articulated the challenges faced in large corporations to achieve above potential benefits. The challenges have been discussed from the three perspectives of successful organization: people (example is human resources challenge), process (example is business transformation challenge), and technology (example is integration with on-premises systems challenge).

Each challenge has been supported with examples and recommendations to overcome the challenge. These recommendations are the results of our experience at Saudi Aramco in transforming major business processes such as Human Resources (HR) and Supply Chain Management (SCM) to the cloud. During our transformation journey, we also learned from the experience of other leading companies and the best practices followed worldwide.

Cloud computing will play a major role for the continuing development of the Fourth Industrial Revolution (IR 4.0). The Fourth Industrial Revolution

will be driven by the integration of resources and new technology. By integrating critical cloud technologies, businesses will be able to develop new applications and services to grow in the future - and in some cases, take them to an entirely new level [10].

Acknowledgement. The authors would like to thank the management of Saudi Aramco for their support and permission to publish this article.

References

[1] "2016 idg cloud computing survey - idg," 2016. [Online]. Available: https://www.idg.com/tools-for-marketers/2016-idg-enterprise-cloud-computing-survey/

[2] M.-G. Avram, "Advantages and challenges of adopting cloud computing from an enterprise perspective," *Procedia Technology*, vol. 12, pp. 529–534, 2014.

[3] G. Pendse, "Cloud computing: Industry report and investment case ." 2017. [Online]. Available: http://business.nasdaq.com/marketinsite/2017/Cloud-Computing-Industry-Report-and-Investment-Case.html

[4] T. Dillon, C. Wu, and E. Chang, "Cloud computing: issues and challenges," in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*. Ieee, 2010, pp. 27–33.

[5] "The cloud is here: embrace the transition," Dec 2017. [Online]. Available: https://www2.deloitte.com/ca/en/pages/consulting/articles/cloudtransition.html

[6] S. Kuyoro, "Cloud computing security issues and challenges," *International Journal of Computer Networks*, vol. 3, no. 5, pp. 247–55, 2011.

[7] K. Popović and b. p. y. o. Hocenski, Zeljko, "Cloud computing security issues and challenges."

[8] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *arXiv preprint arXiv:1609.01107*, 2016.

[9] F. B. Alomari and D. A. Menascé, "Self-protecting and self-optimizing database systems: Implementation and experimental evaluation," in *Proceedings of the 2013 ACM Cloud and Autonomic Computing Conference*. ACM, 2013, p. 18.

[10] P. Giraud, "How cloud is driving the next industrial revolution." [Online]. Available: https://www.oracle.com/uk/cloud/paas/features/next-industrial-revolution.html