2012 International Conference on Economics, Business and Marketing Management
IPEDR vol.29 (2012) © (2012) IACSIT Press, Singapore

Hybrid Cloud Considerations: Managerial Perspective

Peter Géczy[1], Noriaki Izumi[1], Kôiti Hasida[1]

[1]National Institute of Advanced Industrial Science and Technology (AIST) 2-3-26 Aomi, Koto-ku Tokyo, Japan

Abstract. Cloud computing services have been regarded by organizations as a highly promising and lucrative trend. However, cloud-based services have numerous inherent risks that outweigh benefits. The services are distributed and provided on-demand via networks. Distribution and network-based access of services are the roots of benefits and risks. Primary risks are costs, security, loss of control, accessibility and insufficient legislative. Private cloud architectures eradicate most pressing problems but are costly. Public clouds are economical in short term, but present the highest risks. Hybrid clouds have a potential to provide balanced solutions. Unfortunately, there is a notable scarcity of proper studies of hybrid cloud systems that expose constructive balancing of risks and benefits. This study attempts to bridge the gap. We explore relevant aspects of hybrid cloud systems and highlight both beneficial and unfavorable aspects. Presented material provides actionable knowledge for managers and information technology professionals. It facilitates competent decision making required for adoption and management of hybrid cloud systems.

Keywords: hybrid cloud systems, cloud computing, cloud based services, information technology management, knowledge management, actionable knowledge.

1. Introduction

Information services, technologies and data processing are at the vanguard in knowledge-intensive organizations [1]. Organizations and their members substantially rely on a broad range of information technologies. They extend from networking infrastructures and physical computing, to social networking platforms and high-level knowledge management. Knowledge workers have been becoming increasingly dependent on information technologies and resources for improving work efficiency and streamlining business processes [2].

Widespread information technology deployment and investments have been attracting attention of providers and suppliers. The earlier-day networked delivery model resurfaced as so-called cloud computing [3, 4]. The cloud computing model aims at delivering information technology services over networks for appropriate remuneration [5]. The cloud-based services, platforms and infrastructure can be located within or outside an organization. The internal delivery of services over internal networks and ownership of infrastructure refers to private clouds [6], whereas the external ones denote public clouds [7]. Mixture of both private and public cloud systems underlines so-called hybrid clouds.

Cloud-based architectures have their specific advantages and disadvantages. Providers of public cloud computing services generally stress advantages, such as speed and ease of deployment. However, they often downplay or hide significant risks associated with public clouds. Security, loss of control, availability, performance and legislative issues are among the most important risks associated with cloud systems that affect operating efficiency of organizations [8]. Organizations adopting public clouds must account for them [9]. Hybrid cloud model has a potential to institute a proper balance between risks and benefits of public and private cloud-based systems. However, organizations should approach hybrid cloud adoption carefully and after significant considerations.

This study reveals pertinent actionable knowledge for proper consideration and adoption of the hybrid cloud model. It highlights both risks and benefits inherent in public and private clouds, and shows how they affect the hybrid cloud systems. Understanding of these essential elements enables informed decision-making and effective risk management.

2. Hybrid Cloud Architecture

The cloud computing models provide on-demand information technology services over networks. Private clouds represent the model where networking infrastructure and services are owned by the organization and provided internally within the organization. Private clouds are the most beneficial, but require higher initial investments. Public clouds are polar opposites of private clouds. In the public cloud model, services and their supporting infrastructure are owned by an external provider. The services are accessed over internet. The public cloud model poses the highest risks for organizations that adopt it; however, it is relatively economical—for a short term implementation (e.g. as a temporary solution before transitioning to private cloud). Hybrid cloud model is a combination of private and public models. The essential architecture of a hybrid cloud is depicted in finger 1.

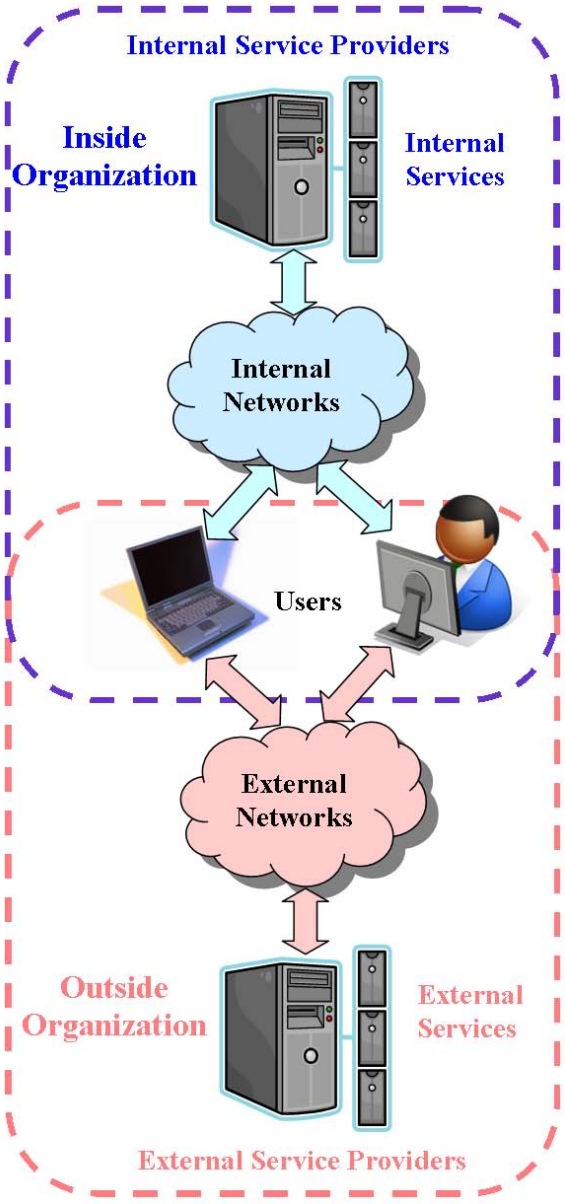

Figure 1. Depiction of hybrid cloud architecture.

In hybrid cloud architecture, part of information technology services is owned by the organization and provided internally, while other part is owned and provided by external providers. Internal services are accessed over internal networks—organizational intranets. Third party external services are accessed over external networks, such as internet and/or mobile networks. Users generally interact with and access external services via web-based interfaces. Hybrid cloud architecture incorporates advantages and disadvantages of both private and public clouds.

3. Benefits

Hybrid cloud architecture features both private and public system segments. The majority of benefits of the hybrid cloud architecture are associated with the private segment. However, the public segment of hybrid clouds has also some benefits. We present a concise list of notable benefits that should be well understood and accounted for by information technology managers.

- **Balanced Approach**: Hybrid cloud architecture has a potential to balance benefits and risks of its private and public segments. Managers should take advantage of beneficial features of private and public clouds, and minimize their disadvantages.
- **Similarity**: Cloud adoption is similar to outsourcing. This holds for both private and public segments of hybrid cloud architectures. Thus, information technology managers may utilize their outsourcing experience for faster and efficient adoption.
- **Speed**: Cloud-based architecture and services can be deployed relatively fast. Public clouds are specifically designed for fast deployment. There are also numerous readily available private cloud solutions.
- **Ease**: New cloud-based services may be deployed with relative ease. Generally, adoption of new public cloud services or existing ready-to-use private cloud solutions is easy. Unfortunately, this does not hold for transfer of services.
- **Savings**: Elimination and/or transfer of costly cloud-based services to third party providers may reduce costs.
- **Scalability**: Resources can be dynamically and timely scaled with increasing demand. Both hardware and software resources can be easily and dynamically scaled.
- **Payments**: Common payment model for cloud-based services is 'pay-for-use'. Users pay only for the resources they consumed. This is beneficial for short-term planning and cost estimates.

4. Risks

Contemporary hybrid cloud-based architectures present various risks that require proper assessment and considerations. Major risks of hybrid cloud architectures are inherent in the public cloud segment. The private cloud segment features comparatively minor risks. Managers and professionals should assess at least the following risks associated with hybrid cloud architectures.

- **Inappropriate Balance**: Balancing private and public cloud segments inappropriately may cause elevation of potential risks.
- **Fragmented Control**: It is important to maintain control over data and services. The full control is maintained only in the private cloud segment. The full control is lost in the public cloud segment.
- **Fragmented Customization**: Lost and/or limited control over data and services in public clouds leads to limited or no customization.
- **Security**: Public cloud exposure results in significant security risks. Valuable organizational data and services may be compromised.
- **Accessibility**: Accessing data and services over networks has risks. If the network is inaccessible, users are unable to use critical services and/or data.
- **Liability**: Public cloud providers build legal barriers against liabilities. This is particularly imperative in damages such as data loss and/or compromization, and security breaches.
- **Legislations**: Public cloud services are distributed among data centers and infrastructures world-wide. Hence, valuable organizational data may be located in regions with no legal protection.t.

5. Managerial Implications

Weighing benefits and risks of hybrid cloud architectures with respect to local information technology deployment and utilization in organizations is crucial. Hybrid cloud architectures may be suitable for some organizations, while unsuitable for others. Managers should vigilantly consider what benefits and risks may hybrid cloud architectures provide with respect to the local conditions and projected future. One should account for various factors; such as the present state of information technology and human resources, lifetime of computing hardware, computing power, network infrastructure, security, skills of technical staff, budget, etc.

The long-term adoption perspective of hybrid cloud architectures should be prioritized over the short-term one. It is central to realize that contemporary public cloud systems and services are economical only for a relatively short term—about 1-2 years. If an organization plans to utilize cloud-based services for longer than two years, it is advisable to aim at the private cloud implementation from the beginning. Essential aspect is also planning of an early transfer of services from public to private clouds. Issues such as interoperability, compatibility, backups and removal of data at the side of a public cloud provider shall certainly arise. Early planning can minimize transition and costs.

Hybrid cloud architecture should be adopted in line with the best practices within both the organization and the relevant industry. Take advantage of modular architectures in hardware, software and other tools. Modular systems are generally easier to upgrade, update and scale. Avoid vendor lock-in and highly specific systems. Open source solutions may often provide greater cost-performance benefits than the commercial ones

6. Conclusions

Hybrid cloud architecture consists of two main segments: private and public. Each of them has benefits and risks. Benefits and risks of hybrid cloud systems have two essential dimensions: inherent and unique. Inherent benefits and risks originate straightforwardly from private and public cloud segments. Unique benefits and risks are derived from the unique combination of private and public cloud segments. The majority of inherent benefits are associated with the private cloud segment; while the majority of inherent risks are rooted in the public cloud segment. The primary benefits of hybrid clouds include capability to balance inherent risks and benefits of public and private segments, similarities in deployment among both segments, and relative ease and speed of deployment. The essential risks are security, fragmented control and customization, accessibility, liability and legislative aspects. Appropriate hybrid cloud adoption strategy aims at maximizing benefits, minimizing risks, and efficiently maintaining and improving the balanced state over a lifetime of implementation—in accordance with the local conditions in organizations.

7. Acknowledgements

The authors would like to thank the members of the Social Intelligence Technologies Research Laboratory at the National Institute of Advanced Industrial Science and Technology (AIST) for their valuable discussions and comments.

8. References

[1] M. Alvesson, "Knowledge Work and Knowledge-Intensive Firms," Oxford University Press, Oxford, 2004.

[2] T. H. Davenport, "Thinking for a Living - How to Get Better Performance and Results from Knowledge Workers," Harvard Business School Press, Boston, 2005.

[3] D. S. Linthicum, "Cloud Computing and SOA Convergence in Your Enterprise," Addison-Wesley Professional, New York, 2009.

[4] N. Howie, "Computing on a Cloud," Canadian Manager, vol. 35, no. 1, pp. 9-10, 2010.

[5] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, "Cloud Computing - The Business Perspective," Decision Support Systems, vol. 51, no. 1, pp. 176-189, 2011.

[6] E. Orakwue, "Private Clouds: Secure Managed Services," Information Security Journal, vol. 19, no. 6, pp. 295-298, 2010.

[7] P. Hofmann, D. Woods, "Cloud Computing: The Limits of Public Clouds for Business Applications," IEEE Internet Computing, vol. 14, no. 6, pp. 90-95, 2010.

[8] G. Anthes, "Security in the Cloud: Cloud Computing Offers Many Advantages, but Also Involves Security Risks," Communications of ACM, vol. 53, no. 11, pp. 16-18, 2010.

[9] S. Subashini, V. Kavitha, "A Survey of Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.