HYBRID CLOUD MANAGEMENT: FOUNDATIONS AND STRATEGIES

Peter Géczy, National Institute of Advanced Industrial Science and Technology (AIST)
Noriaki Izumi, National Institute of Advanced Industrial Science and Technology (AIST)
Kôiti Hasida, National Institute of Advanced Industrial Science and Technology (AIST)

ABSTRACT

Adoption of cloud-based systems has been relatively modest—regardless of significant marketing push by major public cloud providers. The cloud-based model utilizes distributed information technology services accessible over networks. The networks can be internal part of organizations' infrastructure—intranets, or external, such as internet or mobile networks. Utilization of internal networks and services is preferred by organizations—private clouds. External networks and services provided by public cloud providers pose significant risks. The major risks associated with public clouds are security, control and accessibility. In public clouds, valuable organizational data can be compromised and damaged by external entities. Organizations utilizing public clouds lose control over their critical data and services, while external entities gain control. Furthermore, external networks are inherently insecure, monitored and substantially less reliable than organizational intranets. Despite numerous disadvantages of public clouds, there is a potential in combining private and public cloud systems—hybrid clouds. Hybrid clouds present unique challenges and possibilities. We explore pertinent aspects of hybrid clouds and introduce suitable strategies for their effective management. Such actionable knowledge is essential for managers of information technologies.

JEL: M15, O14, O32, O33, L86, K12, K23, K42

KEYWORDS: Hybrid Clouds, Cloud Hybridization, Cloud Management, Cloud Computing, Cloud-based Services, Information Technology Management, Actionable Knowledge

INTRODUCTION

Organizations cannot rely on public cloud systems for their valuable data and services—it is too risky. Many organizations had to learn this lesson the hard way; for example WikiLeaks. The WikiLeaks' case clearly exposed the risks of adopting public cloud computing model and services (Sternstein, 2011). WikiLeaks contracted Amazon's public cloud services for hosting web content and data. After years of service, Amazon abruptly removed WikiLeaks' data and content, and terminated their services due to controversial issues. This happened simply based on the inquiry by US federal lawmakers without any legal proceedings (MacAskill, 2010; O'Connor, 2010). Businesses worldwide were stunned with Amazon's behavior—and accordingly adjusted their perspective on public cloud services. Amazon had already bad reputation for reliability. Amazon's cloud service outages and data damages have been causing numerous problems and economic losses for organizations (Bright, 2011; Clark, 2011; Musil, 2011).

Google extends the dangers of public cloud services to entirely new levels. It is well know that Google collects excessive amounts of data via their web and mobile services, intentionally tracks users across web sites, devices, and even geographically—via global positioning satellite sensors, geolocation and wifi network location technologies. Google has entrenched hostility to privacy (Privacy International, 2007). It bypasses privacy settings and undermines any regulatory initiatives aimed at privacy, data protection and retention (MSDN, 2012). Google also employs numerous questionable practices to accumulate increasingly more data about users, businesses and governments (Doctorow, 2012; Mfonobong, 2012;

Loftus, 2012). Google then analyses, processes and explores the collected data for its own economic benefit without any regard or concern for the original sources. Placing any data on their servers means complete loss of control and significant exploitation. The message is clear: public clouds pose risks that organizations cannot afford.

Despite surmounting dangers of public clouds, cloud computing is still considered a promising trend. Understandably, the primary advocates of public cloud services are the public cloud providers themselves. However, public cloud systems are not the only ones available to organizations. There are three main cloud architectures: public, private and hybrid. Each one has its own benefits and risks. The most beneficial are the private clouds. Conversely, the most risky are the public clouds. Hybrid clouds represent a combination of private and public clouds. They have a potential to balance their inherent risks and benefits. Managing cloud adoption requires significant considerations and planning (Géczy et al., 2012). Properly managed and deployed hybrid cloud-based systems can alleviate operational efficiency of organizations.

Organizations devote notable resources to information technologies. Information technologies, resources and services are among the core constituents of knowledge-intensive organizations (Alvesson, 2004). Knowledge workers increasingly rely on information technologies for their work (Ringel-Bickelmaier and Ringel, 2010; Davenport, 2005). Considerable investments in information technologies attract various providers—including cloud providers (Marston et al., 2011).

The cloud service model resembles the outsourcing model. By outsourcing non-core services to cloud providers, organizations should gain economic benefits. The outsourcing costs should therefore be lower than the corresponding information technology investments. Since cloud providers offer services to a number of organizations, they employ the economy of scale to lower their operating costs and achieve reasonable margins (Kambil, 2009). The analogies to outsourcing models are straightforward and appear rational. However, there are numerous challenging issues requiring careful considerations.

This study addresses important issues for practical adoption of hybrid cloud architectures. It is organized as follows. First, we present a literature review and a historical perspective; then, we introduce the hybrid cloud model. Hybrid clouds have both inherent and unique benefits and risks. We concisely outline pertinent benefits and risks associated with hybrid clouds in the section 'Characteristics of Hybrid Clouds'. This risk-benefit analysis opens avenues for effective managerial strategies. The section 'Actionable Managerial Strategies for Cloud Hybridization' introduces actionable knowledge crucial for feasible deployment of hybrid cloud systems. This enables effective decision-making and allows managers to assess the key strategic points. Discussion of the key points and conclusive remarks are provided in the final section.

LITERATURE REVIEW AND HISTORICAL PERSPECTIVE

Cloud computing is nothing new—technologically (Howie, 2010). It merely represents a suitable merger of already existing technologies. The technologies enabling cloud computing have been available for a relatively long time. In fact, what is called a 'cloud computing' today has been known as a 'distributed computing' to information technology professionals for decades (Cubitt et al., 2011). Then, why suddenly cloud computing (or distributed computing) re-emerged as a promising contemporary information technology trend? To answer this question, one has to gain a perspective on how information technologies have paved their way to organizations, and how information technology companies built and utilized their services.

Organizations have utilized various approaches for information technology adoption; however, there are common points. In early days, each organization had its own way of building information technology

resources and infrastructures. This period is characterized by relative absence of information technology departments and hence also absence of coordinated long-term strategy and planning (Butler and Murphy, 2007). Individual departments had been implementing their own information systems and infrastructures. It had been sufficient to meet only the local requirements of individual departments (Palanisamy et al., 2010). However, information technology companies provided multi-purpose hardware and software. This led to multiplicity of systems at various departments that had overlapping functionalities and components, but lacked interoperability (Papastathopoulou et al., 2007). Rapid progress in information technologies required frequent upgrades. Information technology costs had been rising sharply. The challenge was to bring the costs under control and optimize deployment of information technology resources.

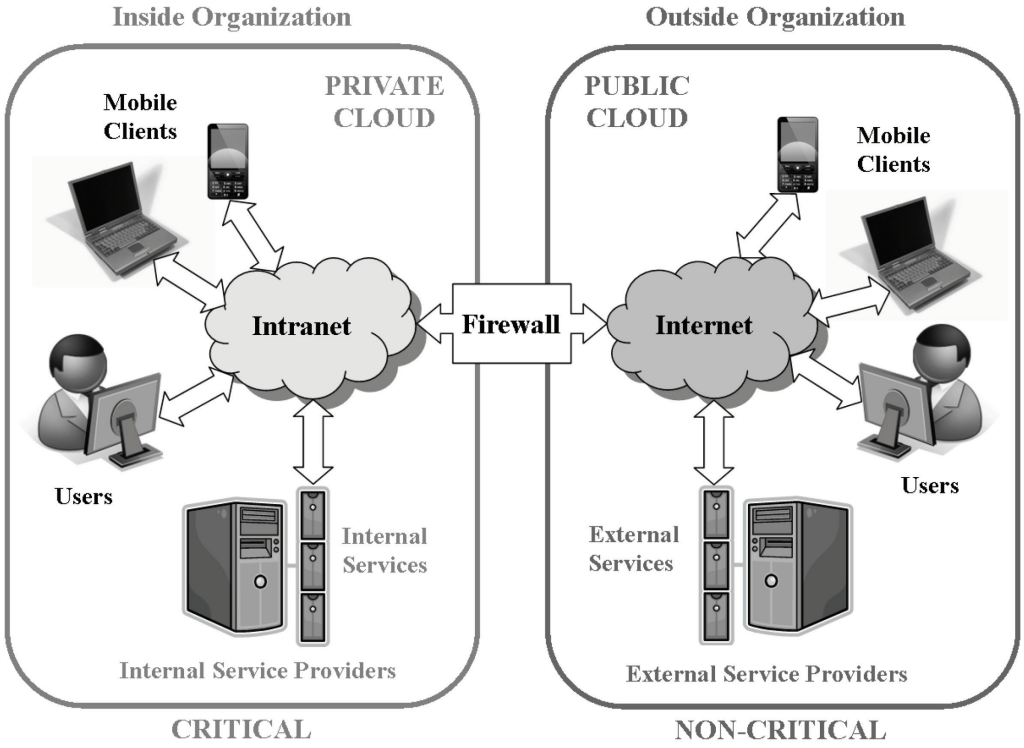
The necessity of coordinated planning and deployment of information technologies in organizations has emerged (Georgantzas and Katsamakas, 2010). However, radical changes to already deployed systems would impede operating efficiency of organizations. Solutions that would utilize existing, often legacy technologies, have been preferential. A viable solution has been found: organizational portals that provide single-point access to systems and services distributed among various departments (Oertel et al., 2010; Sullivan, 2004; Collins, 2000). Portals have featured uniform front-end interface to a variety of back-end implementations. The technological enablers for portals have been standardized network communication protocols, web technologies, and service-oriented architecture and design (Rosen et al., 2008).

Uniform front-end to distributed resources and services (together with networked access) are the main characteristics of cloud computing (Linthicum, 2009). Services can be accessed via local intranets, or via global internet. Hence, in the networked environments, the service providers can be both inside and outside of organizations. Internal provision of services over local intranets refers to private clouds, while external provision of services over internet refers to public clouds. This permits sufficient specialization of both external organizations and internal data centers on providing *on-demand* services (Iyer and Henderson, 2010). The providers can optimize their infrastructures and resources to reach higher efficiency. However, cloud-based systems have associated risks and benefits (Subashini and Kavitha, 2011; Hamlen et al., 2010; Julisch and Hall, 2010). Security, control and legal protection of data and services are among the most important aspects for organizations (Anthes, 2010; Lanois, 2010).

Hybrid Cloud Model

Common characteristics of cloud-based models are on-demand supply of resources and services, their distributed nature, and access over networked infrastructures (Rimal et al., 2011). Resources and services are provided according to the need of organizations or users. The needs may vary over time. Cloud-based implementations should respond to dynamically changing needs (Goscinski and Brock, 2010). Cloud-based environments should be dynamically scalable. Dynamic demand for resources should be automatically matched by appropriate supply. On-demand provisioning of resources and services allows flexible accounting. Organizations and users pay only for what they use. This is advantageous if the use significantly fluctuates.

Figure 1: Hybrid Cloud Model Illustration



Cloud-based models feature distribution of information technology resources and services both internally–inside an organization and externally–outside an organization. The hybrid cloud model contains critical services and resources inside organization. They are provided internally and accessed over local intranet. Non-critical services and resources are located outside organization. They are supplied by external providers and accessed over public internet.

Services and resources are distributed both physically and logically. Physical distribution refers to different geographical locations and/or hardware. For example, data centers hosting hardware can be build in different geographical locations. Locations are chosen according to availability of energy resources, skilled labor, suitable legislation and economic incentives. Logical distribution underlines distribution on the same hardware. This is achievable via virtualization technologies (Loganayagi and Sujatha, 2011). Several virtual environments can be present concurrently on a single hardware resource. Virtualization system maintains separation among individual virtual environments.

Cloud-based services and resources are generally accessed over communication network infrastructures (Frischbier and Petrov, 2010; Haeberlen, 2010). Communication infrastructures are owned and provided by various operators. For instance, mobile operators provide wireless access while other communication companies provide wired access. Global network access is over internet. Organizations have also their own local networks—intranets. Services and resources are accessed over these various networks by standardized protocols. Higher-level standardization facilitates accessibility over different networks.

Three main cloud-based models are commonly distinguished: private, public and hybrid. They differ in accessibility, ownership and location of cloud-based environments. Illustration of cloud-based models is presented in Figure 1. The left-hand side shows essential configuration of private cloud architecture, while the right-hand side shows the public one. Combination of private and public clouds underlines the hybrid cloud architecture.

Private clouds are the most beneficial for organizations (Orakwue, 2010). Organizations can exercise full control over their data, services, resources and infrastructure. The private cloud environments are owned

by organizations and hosted within their premises. Services and resources are accessed over local intranets. Local organizational intranets are presently the most reliable, secure and available network environments. Private clouds are also the most economical in the long term.

Public clouds are the most risky and disadvantageous for organizations (Hofmann and Woods, 2010). Organizations lose control over their valuable data, services and infrastructure. These essentials are outsourced to external providers. Organizations must compromise on numerous key issues, since services and information technology resources are owned by external entities. Valuable organizational data and services are exposed to significant security risks because they are hosted by external providers and accessed over internet and/or mobile networks. Internet and mobile networks are presently the most unreliable and insecure network environments. They are monitored by various entities. Thus, valuable organizational data is exposed. Unreliability of internet and mobile networks leads also to accessibility risks. If internet or mobile connection is not available, users cannot access critical data and services. Public cloud environments are the most expensive in the long term.

Hybrid clouds represent a combination of private and public clouds (Sotomayor et al., 2009). Organizations should maintain control over their critical data, services and infrastructure. Non-critical elements can be outsourced to external provides. Critical organizational data, services and infrastructure to access them are kept in-house. The critical services and resources are accessed over local intranets that provide secure and reliable connectivity. Residual non-critical data and services may be outsourced. They are located at infrastructures of external providers where they are exposed to significant risks. Accessibility of non-critical resources is via internet and mobile networks that are insecure and have low safety factors. Hybrid clouds provide opportunities to balance short term and long term costs.

Characteristics Of Hybrid Clouds

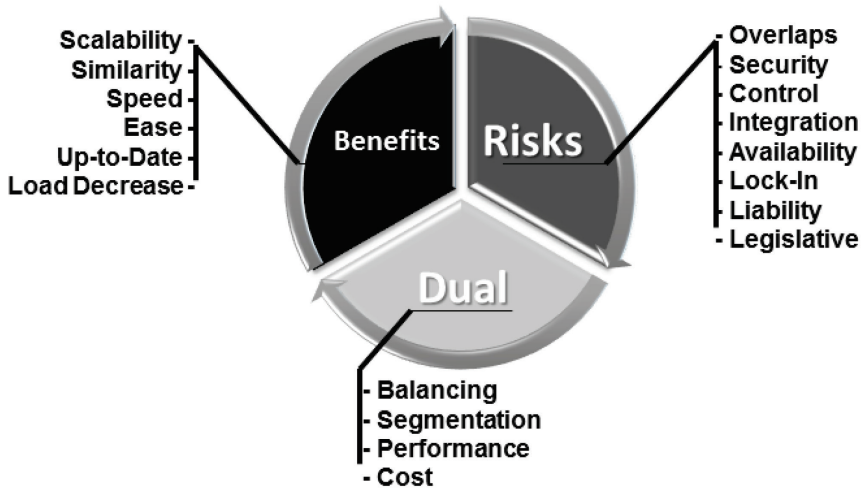
Hybrid cloud systems inherit various characteristics from both private and public clouds. Moreover, the unique combination of both cloud architectures presents some specific issues. Some specifics relate to links between both private and public cloud architectures, others arise from the resulting hybridization. Primary characteristics of hybrid cloud systems are listed in Figure 2. They are concisely described in the following subsections.

Benefits

Hybrid cloud-based systems have various benefits. Majority of benefits are inherited from its private cloud segment. Primary concerns for organizations and users are security and control of their valuable data and services (Anthes, 2010). While private cloud systems provide the most secure environments for organizational data and service, introduction of public cloud segments exposes organizations to significant security risks. Hence, the primary benefits in purely private cloud adoption scheme become potential risks in hybrid cloud configurations. Benefits of hybrid cloud systems relate to their structural features (scalability, similarity and load decrease) and temporal aspects (speed and up-to-date actualizations).

Scalability. Cloud systems are scalable. Information technology resources can be dynamically allocated on-demand. When demand increases, more resources are provided, and when demand decreases, resources are reduced. This permits efficient utilization of resources. Hardware and software resources can be scaled on-demand. Scalability is possible by employing virtualization and modularization technologies. These technologies allow dynamic management of available information technology resources.

Figure 2: Essential Characteristics of Hybrid Cloud Systems



Hybrid cloud systems feature essential benefits and risks. Furthermore, they possess characteristics that account for both potential risks as well as benefits—depending on proper assessment and implementation of hybrid cloud architecture.

Similarity. Adoption of cloud-based architectures is similar to outsourcing. Outsourcing experience provides viable higher-order perspective on cloud adoption. Managers with outsourcing experience and expertise should be competent to assess issues related to cloud adoption. Although there are differences between outsourcing and cloud adoption, information technology managers should be able to adapt fast. They should be capable of weighting risks and benefits of clouds with respect to their organization and users.

Speed. Cloud-based systems and services can be deployed fast. Most of the public clouds are specifically designed for fast deployment. Available private cloud systems are also rapidly deployable. There are ample ready-to-use packages suiting various needs of organizations and users. Information technologies and systems are modular. Modularity facilitates fast deployment and expansion.

Ease. Cloud-based systems are easily deployable. Contemporary technologies permit easy and fast deployment. Hardware, in majority of instances, is the same as or slightly different from the conventional server, cluster and modular systems. Analogously, software solutions for management of cloud-based systems are built for easy use and adaptation. Hence, the information technology managers with experience in modern server systems are able to adapt to new conditions with ease and speed.

Up-to-Date. Information technology solutions for cloud-based systems are kept up-to-date easily. In public cloud systems, software, hardware and related infrastructures are professionally managed and maintained at the side of providers. They are kept up-to-date by professional technicians. Private cloud solutions require in-house maintenance and management. Fortunately, majority of cloud-based solutions feature automatic update options. Thus, organizations and users are timely provided with the latest stable environments.

Load Decrease. Hybrid clouds enable decrease of various loads within organizations. Resource intensive services that are not among the core competencies of organizations can be moved to public clouds. This decreases load on private cloud systems. Analogously, large number of available information resources and data at organizational systems contribute to information overload. These can be managed effectively and dynamically by cloud-based systems.

Risks

Hybrid cloud environments present several significant risks. The main risks are inherent in the public cloud segment (Subashini and Kavitha, 2011; Lanois, 2010). Private clouds are the safest. However, incorporation of public clouds in hybrid cloud systems lowers the safety of the overall system. The major risks, inherent in public clouds, are security and loss of control. Proper control and management of valuable data and services are of the primary importance for organizations (Julisch and Hall, 2010; Hamlen et al., 2010). While private clouds allow full control of data and services by organizations, use of public clouds results in loss of control. Therefore, it is pertinent to assess which data and services are outsourced to external public cloud providers. Additional risks are availability of services, integration and legislative issues.

Overlaps. Data and services utilized by private and public clouds should be disjunct. Ideally, there should be no overlaps. Each cloud system should contain its own data and services. Utilization of private cloud systems exposes organizational data and services at substantial risk. Existence of overlaps increases the risk. For instance, if data is compromised in the public cloud, it affects also data in the private cloud; hence, the whole system is affected.

Security. Inclusion of public cloud segments results in security risks. Outsourcing organizational data and services to external providers exposes them to high risks. The external providers gain access to organizational data and services, and may compromise them—either intentionally or unintentionally. Additional risks relate to access of services and data in public clouds over internet and other insecure communication networks. These communication networks are monitored by various governmental and corporate organizations. Traffic is regularly intercepted and compromised despite the use of secure protocols and encryption. Several legislations, including the United States, even prohibit, limit or neutralize encryption standards and secure protocols.

Control. Control over valuable data and services is essential for organizations. It is therefore pertinent that organizations strive to maintain it. In private clouds, organizations have the complete control. However, in public cloud environments, the control is lost. External public cloud providers gain control over data and services. Organizations must compromise on notable aspects of their data and services and often follow regulations set up by public cloud providers. These may be in contradiction with internal organizational regulations.

Integration. Services provided by cloud-based systems should integrate well into existing information technology frameworks and workflows of organizations. Interfaces, data structures and communications should be compatible with the existing formats, data structures and communication protocols used by the organization. Incompatibilities result in various operational problems. Later-stage resolution of incompatibilities may be costly and time consuming. Cloud-based systems and providers should incorporate relevant integration services.

Availability. Availability underlines accessibility of services and resources. Services and resources should be accessible fast—whenever needed. Since cloud-based services are accessed over networks, reliability of networks plays significant role. If network connection is unreliable, services may become inaccessible. Local organizational networks are considerably more reliable and faster that global internet and mobile networks. Hence, public cloud services are less reliable and accessible than private cloud services. Therefore, the core services and resources requiring high availability should be in private clouds.

Lock-in. Ability to relocate organizational data, services and resources fast and easy is essential. However, lock-in is a business strategy of majority of public cloud providers. To start using their services is easy, but to transfer organizational data, services and resources from their platforms is not. Public

cloud providers erect artificial barriers for organizations and users. Moving away from their platforms becomes troublesome, time consuming and costly.

Liability. Public cloud providers protect themselves by legally distancing from possible liabilities. Organizational data, resources and services are exposed to significant risks at public cloud providers' platforms. Valuable organizational data may be damaged, compromised and exposed to undesirable entities. Their services may become inaccessible causing notable losses for organizations. Unfortunately, organizations and their members have only very limited or non-existent legal protection. Contractual terms of service of public cloud providers are formulated in such a way that they cannot be hold accountable and liable.

Legislations. Cloud-based systems and services are distributed. Distributed nature of cloud-based model provides numerous advantages, but inevitably brings up the issue of diverse legislations. Data centers of public cloud providers are physically located in various geographical locations. The choice of locations is influenced by several operational and legislative factors. Providers choose locations with legislations favorable for them, but not for organizations to which they provide services. These are often locations with inadequate or non-existent legislations for data protection, privacy, and other important issues. Hence, valuable organizational data and services may be on servers in locations with non-existent legal protection.

Dual Issues

Certain aspects of hybrid cloud systems are not clearly polarized. They cannot be straightforwardly characterized as risks or benefits. They can be either risks or benefits depending on implementation and/or deployment. Specifics of cloud system implementations determine their positive and negative values as well as their benefit and risk factors. Balancing and segmentation characteristics are unique features of hybrid cloud systems. Performance and cost are inherited features from private and public components. These characteristics are highlighted in the following paragraphs.

Balancing. Determining and maintaining a proper balance between private and public cloud systems is vital. Inappropriate division and utilization of individual cloud segments may lead to notable deficiencies and operating inefficiencies. Extensive public cloud segment provides significant exposure to risks. The major risk factors have been formerly described. It is important to minimize risks to manageable levels. Certain system designs and configurations may be more cost effective, but incorporate higher risks. It is not advisable to compromise on security of data and services—even in cases of higher initial costs. Security, control and reliability aspect should be prioritized.

Segmentation. Services and resources in hybrid cloud systems are divided among private and public components. Proper division of information technology resources, in addition to data and services handled by each cloud component, is important. There should be minimal overlaps between data and services (unless the overlapping aspects are desired for redundancy purposes). Critical organizational data and services should be always in private clouds. Division of data and services between private and public clouds results in fragmented control and customization. Extensive fragmentation is undesirable. Private clouds provide full control and can be customized to suit organizational needs.

Performance. Performance of cloud-based systems is dependent on available information technology resources. Organizations that can devote more resources to their information technologies should aim at maximizing their private cloud segment. Organizations with fewer resources may initially employ larger public cloud component, but should aim at expanding their private cloud systems and minimize exposure to external public cloud providers. Services and resources should have satisfactory performance allowing users to perform their tasks. They should also be scalable with growing user base and computing

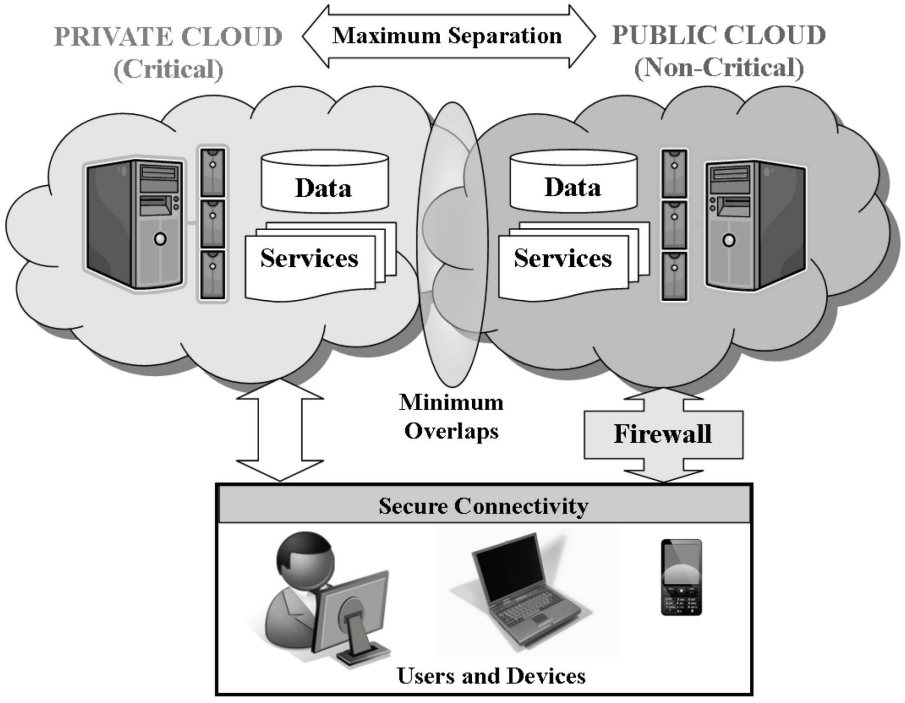
demands. Outsourcing residual services to external providers may help to free resources in private cloud and improve its performance for core services.

Costs. Costs in hybrid cloud systems are divided between private and public parts. Generally, private clouds are cost efficient in a long term, but may require higher initial costs. Public clouds are not cost efficient in a long term, but require lower initial costs. Hybrid cloud configurations enable greater flexibility in balancing short term and long terms costs. Organizations can reduce their initial costs and spread expenses more suitably over their planning periods. Since public cloud services frequently employ utility-style payment schemes (organizations pay only for the resources and services they used), costs may be easily estimated and effectively planned in both shorter and longer terms.

RESULTS: ACTIONABLE MANAGERIAL STRATEGIES FOR CLOUD HYBRIDIZATION

Necessary precursors to hybrid cloud system deployment are significant considerations and planning. While hybrid cloud systems may fit certain organizational needs, they may be unsuitable for others (McKinney, 2010). Large and medium size organizations should aim at implementation of private clouds from the beginning, or as early as possible. Information technology managers should cautiously weigh whether the incorporation of a public cloud dimension is worth the risks (Marston et al., 2011). There are numerous other aspects to consider. The essential actionable knowledge and strategic principles for viable hybridization of cloud systems are depicted in Figure 3.

Figure 3. Depiction of Strategic Cloud Hybridization Management Principles



Proper management strategies for adoption of hybrid cloud systems should aim at maximum separation and minimum overlaps of data and services at private and public clouds. The strategic considerations should target balancing security, control, legal protection and long term economic benefits for organizations.

The main advantage of hybrid clouds is the capability to balance inherent risks and benefits in its private and public segments. The major benefits originate from the private clouds. The public clouds bring the highest risks. A viable hybrid cloud adoption strategy aims at maximizing benefits, minimizing risks, and

efficiently maintaining suitable long-term balance. The primary focus should be on three essential points: maximizing separation between private and public cloud components in terms of data and services, minimizing overlaps among data and services, and enhancing segregate end-to-end secure connectivity for both clouds. These strategic management concepts are detailed in the following paragraphs.

Maximum Separation: Public cloud segment poses the greatest risks. Valuable organizational data and services are exposed to external entities and may be compromised. Thus, it is essential to maintain the maximum possible separation of data and services in the public and private clouds. Exposure to public clouds should be only for the data and services that are residual and non-core for efficient functioning of organizations. The core data and services should be in the private cloud in-house. The separation should be maintained preferably at both physical and logical levels (Loganayagi and Sujatha, 2011). Hardware and software infrastructures utilized for accessing data and services in private and public clouds should be segregated.

Minimum Overlaps: Total separation of public and private cloud systems may be difficult to achieve. If the complete separation is not achievable, it is advisable to minimize overlaps of data, services and infrastructures that are exposed to both public and private cloud systems. Overlaps elevate security and control risks primarily associated with external public cloud providers. Minimization of overlaps minimizes potential risks. Bridging systems between private and public clouds should be appropriately monitored for any data leakage, damage and exposure. Furthermore, the gateways to external public cloud systems should be suitably monitored as well.

End-to-End Secure Connectivity: Security is among the most important issues. The primary security risks are due to exposure to external public cloud providers. Services and resources hosted in the external public cloud systems are accessed over global internet or mobile communication networks. These networks are thoroughly monitored by the providers and several other entities. Traffic in these networks is routinely intercepted and analyzed. Any data exchanged between an organization and a public cloud provider is essentially exposed to a wide range of risks. Encrypted communication partially lowers the exposure level. A mistake made by organizations is that secure connectivity is provided only for the external traffic. Interception and compromisation may also happen internally. It is therefore pertinent to secure the complete communication path, that is, to employ secure end-to-end connectivity.

Cost Effectiveness: Organizations should aim at long-term cost effectiveness while balancing short-term costs. Private cloud systems are long term cost effective, but require higher initial costs. Public cloud systems may be cheaper in a short term, but become expensive in a long term. Present-day public cloud services are often economical for less than two years (Mann, 2011; Morton and Alford, 2009). Hence, the strategic target for information technology managers is to achieve full efficiency of private cloud systems within two years. Exposure to external public cloud services should be drastically minimized after two years.

DISCUSSION AND CONCLUSIONS

Elucidation of hybrid cloud systems revealed various pertinent strategic issues and considerations. Hybrid cloud systems comprise of private and public cloud components. Information technology resources and services in the private cloud segment are owned by the organization that utilizes them. Infrastructure, hardware and software are hosted inside the organization. Public cloud systems employ the opposite concept. External providers that own the underlying infrastructure, hardware and software provide services. Hence, the hybrid cloud systems utilize both internally and externally provided and owned resources and services.

Combination of internally and externally provided and owned resources and services presents both benefits and risks. Various risks and benefits are inherent in public and private segments. However, the unique combination of public and private cloud systems brings up specific challenges. The majority of inherent benefits arise from the private clouds. Conversely, the majority of inherent risks originate in the public clouds. The most important issues for organizations are security and control of data and services. While private clouds allow full control and better security, public clouds provide notably lower security and control of data and services. Major unique issues of hybrid cloud systems are fragmentation and overlaps of data and services between their public and private components. Information technology managers must carefully weigh both inherent and unique issues prior to adopting hybrid cloud architectures.

Suitable adoption of hybrid cloud systems should aim at balancing benefits and risks with respect to the local conditions of organizations. Hybrid clouds have a potential to balance inherent and unique risks and benefits. Balancing benefits and risks requires an appropriate strategy. A general strategy is to maximize benefits and minimize risks, while maintaining operational effectiveness of the hybrid cloud systems. This approach exposes managerial domains that require attention. Pertinent strategic targets are fourfold: maximum separation of private and public clouds, minimum data and service overlaps among cloud architectures, secure end-to-end connectivity and cost effectiveness. Maximum separation of data and services between private and public clouds lowers the risk of undesirable exposure and loss of control. Minimum data and service overlaps address both fragmentation and security issues. Secure end-to-end connectivity between users and services for both public and private clouds lowers unwanted exposure of valuable organizational data and services. Cost effectiveness leads to the issue of balancing short and long-term costs. Organizations should target long terms cost effectiveness of cloud systems. This means maximizing the efficiency of private clouds within two years while minimizing exposure to external public cloud providers.

Presented characteristic features of hybrid cloud systems highlighted selected important aspects. However, there are additional aspects that exceed the scope of this work. Information technology managers should be aware of the additional conditions (with respect to their organization) and incorporate them into the introduced strategic framework.

REFERENCES

Alvesson, M. (2004). *Knowledge Work and Knowledge-Intensive Firms.* Oxford University Press, Oxford.

Anthes, G. (2010). Security in the Cloud: Cloud Computing Offers Many Advantages, but Also Involves Security Risks. *Communications of ACM*, 53(11), 16-18.

Bright, P. (2011). Amazon's Lengthy Cloud Outage Shows the Danger of Complexity. *ArsTechnica*, http://arstechnica.com/business/news/2011/04/amazons-lengthy-cloud-outage-shows-the-danger-of-complexity.ars

Butler, T., Murphy, C. (2007). Understanding the Design of Information Technologies for Knowledge Management in Organizations: A Pragmatic Perspective. *Information Systems Journal*, 17(2), 143-163.

Clark, J. (2011). AWS Cloud Accidentally Deletes Customer Data. *ZDNet*, http://www.zdnet.co.uk/news/cloud/2011/08/10/aws-cloud-accidentally-deletes-customer-data-40093665/

Collins, H. (2000). *Corporate Portals: Revolutionizing Information Access to Increase Productivity and Drive the Bottom Line*. Amacom, New York.

Cubitt, S., Hassan, R., Volkmer, I. (2011). Does Cloud Computing Have a Silver Lining? *Media Culture and Society*, 33(1), 151-160.

Davenport, T. H. (2005). *Thinking for a Living - How to Get Better Performance and Results from Knowledge Workers*. Harvard Business School Press, Boston.

Doctorow, C. (2012). The Google-Kenya Ripoff. *BoingBoing*, http://boingboing.net/2012/01/13/google-fraudulently-solicits-f.html.

Frischbier, S., Petrov, I. (2010). Aspects of Data-Intensive Cloud Computing. *LNCS 6462*, Springer-Verlag, 57-77.

Géczy, P., Izumi, N., Hasida, K. (2012). Cloudsourcing: Managing Cloud Adoption. *Global Journal of Business Research*, 6(2), 57-70.

Georgantzas, N. C., Katsamakas, E. G. (2010). Performance Effects of Information Systems Integration: A System Dynamics Study in a Media Firm. *Business Process Management Journal*, 16(5), 822-846.

Goscinski, A., Brock, M. (2010). Toward Dynamic and Attribute Based Publication, Discovery and Selection for Cloud Computing. *Future Generation Computer Systems*, 26(7), 947-970.

Haeberlen, A. (2010). A Case for the Accountable Cloud. *ACM SIGOPS Operating Systems Review*, 44(2), 52-57.

Hamlen, K. Kantarcioglu, M. Khan, L. Thuraisingham, B. (2010). Security Issues for Cloud Computing. *International Journal of Information Security and Privacy*, 4(2), 36-48.

Hofmann, P., Woods, D. (2010). Cloud Computing: The Limits of Public Clouds for Business Applications. *IEEE Internet Computing*, 14(6), 90-95.

Howie, N. (2010). Computing on a Cloud. *Canadian Manager*, 35(1), 9-10.

Iyer, B., Henderson, J.C. (2010). Preparing for the Future: Understanding the Seven Capabilities of Cloud Computing. *MIS Quarterly Executive*, 9(2).

Julisch, K., Hall, M. (2010). Security and Control in the Cloud. *Information Security Journal*, 19(6), 299-309.

Kambil, A. (2009). A Head in the Clouds. *Journal of Business Strategy*, 30(4), 58-59.

Lanois, P. (2010). Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy? *Northwestern Journal of Technology and Intellectual Property*, 9(2), 29-49.

Linthicum, D. S. (2009). *Cloud Computing and SOA Convergence in Your Enterprise*. Addison-Wesley Professional, New York.

Loftus, T. (2012). 'Mortified' Google Apologizes to Kenyan Business. *The Wall Street Journal*. http://blogs.wsj.com/digits/2012/01/13/mortified-google-apologizes-to-kenyan-business/.

Loganayagi, B. Sujatha, S. (2011). Improving Cloud Security through Virtualization. *Communications in Computer and Information Science*, 204, 442-452.

MacAskill, E. (2010). WikiLeaks Website Pulled by Amazon After US Political Pressure. The Guardian, http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon, December 2, 2010.

Mann, A. (2011). The Cost Benefit Myth of the Public Cloud. Übergeek, http://pleasediscuss.com/andimann/20110504/the-cost-benefit-myth-of-the-public-cloud/

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A. (2011). Cloud Computing - The Business Perspective. *Decision Support Systems*, 51(1), 176-189.

McKinney, P. (2010). Is Cloud Computing for You? *Forbes*, 186(10), 56-57.

Mfonobong, N. (2012). Google Accused of Being Evil...In Kenya. *Forbes*, http://www.forbes.com/sites/mfonobongnsehe/2012/01/13/google-accused-of-being-evil-in-kenya/.

Morton, G., Alford, T. (2009). The Economics of Cloud Computing Analyzed. October 26, 2009. http://govcloud.ulitzer.com/node/1147473.

MSDN (2012). Google Bypassing User Privacy Settings. https://blogs.msdn.com/b/ie/archive/2012/02/20/google-bypassing-user-privacy-settings.aspx

Musil, S. (2011). Amazon Cloud Outage Downs Netflix, Quora. *CNet*, http://news.cnet.com/8301-1023_3-20089866-93/amazon-cloud-outage-downs-netflix-quora/

O'Connor, A. (2010). Amazon Removes WikiLeaks From Servers. The New York Times, http://www10.nytimes.com/2010/12/02/world/02amazon.html, December 2, 2010.

Oertel, N., Dibbern, J., Nochta, Z. (2010). Assessing the Potential of Ubiquitous Computing for Improving Business Process Performance. *Information Systems and e-Business Management*, 8(4), 415-438.

Orakwue, E. (2010). Private Clouds: Secure Managed Services. *Information Security Journal*, 19(6), 295-298.

Palanisamy, R., Verville, J., Bernadas, C., Taskin, N. (2010). An Empirical Study on the Influences on the Acquisition of Enterprise Software Decisions: A Practitioner's Perspective. *Journal of Enterprise Information Management*, 23(5), 610-639.

Papastathopoulou, P., Avlonitis, G. J., Panagopoulos, N. G. (2007). Intraorganizational Information and Communication Technology Diffusion: Implications for Industrial Sellers and Buyers, *Industrial Marketing Management*, 36(3), 322-336.

Privacy International (2007). A Race to the Bottom - Privacy Ranking of Internet Service Companies. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-553961

Rimal, B. P., Jukan, A., Katsaros, D., Goeleven, Y. (2011). Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach, *Journal of Grid Computing*, 9(1), 3-26.

Ringel-Bickelmaier, C., Ringel, M. (2010). Knowledge Management in International Organisations. *Journal of Knowledge Management*, 14(4), 524-539.

Rosen, M., Lublinsky, B., Smith, K. T., Balcer, M. J. (2008). *Applied SOA: Service-Oriented Architecture and Design Strategies*. Wiley, New York.

Sotomayor, B., Montero, R. S., Llorente, I. M., Foster, I. (2009). Virtual Infrastructure Management in Private and Hybrid Clouds. *IEEE Internet Computing*, 13(5), 14-23.

Sternstein, A. (2011). Service Interrupted: WikiLeaks Fiasco Reinforces Push to Set Security Standards for Cloud Services. *Government Executive*, 43(2), 13-14.

Subashini, S., Kavitha, V. (2011). A Survey of Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*, 34(1), 1-11.

Sullivan, D. (2004). *Proven Portals: Best Practices for Planning, Designing, and Developing Enterprise Portal*. Addison-Wesley, Boston.

ACKNOWLEDGEMENTS

The authors would like to thank the members of SITR group at the National Institute of Advanced Industrial Science and Technology (AIST) for their valuable discussions and comments.

BIOGRAPHY

Dr. Peter Géczy is a chief scientist at the National Institute of Advanced Industrial Science and Technology (AIST). He can be contacted at: AIST, 2-3-26 Aomi Koto-ku, Tokyo 135-0064, Japan.

Dr. Noriaki Izumi is a chief scientist at the National Institute of Advanced Industrial Science and Technology (AIST). He can be contacted at: AIST, 2-3-26 Aomi Koto-ku, Tokyo 135-0064, Japan.

Dr. Kôiti Hasida is a group leader at the National Institute of Advanced Industrial Science and Technology (AIST). He can be contacted at: AIST, 2-3-26 Aomi Koto-ku, Tokyo 135-0064, Japan.