CLOUDSOURCING: MANAGING CLOUD ADOPTION

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

Cloud computing adoption by organizations has been minor despite the initial optimism. The primary concerns obstructing adoption of cloud-based services are security, loss of control, and inadequate legislative. In a cloud-based model, information technology services are distributed and accessed over networks such as intranet or internet. Intranets are inside organizations and internet outside. The main concerns are inherently linked to employing services provided by other organizations and accessing them over internet. In such case, valuable organizational data and services are transferred to providers. The provider or other entities may compromise organizational data and services, thus posing significant security risks. By moving data and services to outside providers, organizations also loose substantial control over timely management and retention. Organizations must follow the rules set by the providers– which may not be well suited for them. The providers legally distance themselves from liabilities on important issues such as security, data loss and damage. There are also several other pertinent factors. Proper cloud computing adoption and utilization by organizations requires balanced approach. We elucidate various factors and highlight proper strategic concepts for effective cloud adoption management—benefiting both organizations and providers.

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

KEYWORDS: cloud computing, cloud providers, cloud-based systems, cloud services, web services, information technology management, knowledge management, risk management, actionable knowledge, knowledge-intensive organizations, knowledge workers.

INTRODUCTION

Cloud-based systems and services have been regarded as '*the next big thing*' by business communities, as well as technology and service providers—until WikiLeaks happened. The case of WikiLeaks plainly exposed intrinsic risks (Sternstein, 2011). What happened? WikiLeaks employed Amazon's cloud services for content and data hosting. Amazon, on a short notice, terminated its services to WikiLeaks and removed the content and data simply upon inquiry by US federal lawmakers (MacAskill, 2010; O'Connor, 2010). The shockwave strongly resonated with businesses. The lesson learned was clear: organizations cannot entrust their mission critical services and data to cloud providers.

Data and related information technologies are at the functional core of knowledge-intensive organizations. Organizations rely on a spectrum of information technologies supporting their operations (Alvesson, 2004). Information technology tools and services are indispensable for their efficient functioning (Ringel-Bickelmaier and Ringel, 2010). Knowledge workers depend on information technologies and data for completing their tasks. Information technology services are also enablers for achieving higher working and operating efficiencies (Davenport, 2005). Any impairment of organizational data or information technology tools and services translates to considerable losses for knowledge-intensive organizations. Hence, significant financial, physical and human resources are dedicated to management and innovation of organizational information systems and infrastructures.

Significant investments of organizations into information technologies attract cloud-based providers. They aim at providing information technology services to organizations for remuneration (Marston et al.,

2011). The essential idea behind the cloud-based business model is relatively simple. Organizations could outsource their information technology needs to cloud-based providers. Overall outsourcing costs should be lower than their information technology investments; hence, there are savings for organizations. Cloud-based providers supply services to multiple organizations, and employ the economy of scale. Thus, they can offer attractive pricing to customers and yet maintain reasonable margins (Kambil, 2009). On the surface, the cloud business model seems rational. However, there are several challenging issues.

This study highlights the pertinent issues and presents actionable knowledge for managers of information technologies. Managers should pay close attention to the presented points when adopting and implementing cloud computing and/or cloud-based services. We overview three essential variants of cloud computing models and concisely express their suitability for various implementations or adoptions. We explain their advantages and disadvantages, and provide managerial recommendations and consideration points. Understanding of the essential principles, as well as risks and benefits, enables knowledgeable decision-making and effective risk management.

The manuscript organization is as follows. The literature review section is followed by the 'Variants of Cloud-Based Models' section. It presents three main cloud computing models and concisely describes their characteristics. The next section, 'Categories of Cloud Services', provides a concise overview of three major categories of cloud services. Cloud computing models have positive and negative aspects. Concerning issues of cloud-based models are exposed in the section 'Cloud Related Concerns'. Beneficial aspects of cloud-based models are revealed in the section 'Cloud Related Benefits'. Organizations must carefully assess advantages and disadvantages according to their own conditions. Strategic recommendations for managers are highlighted in the section 'Actionable Managerial Recommendations'. The presentation finishes with a concise discussion and summary of the essential points in the section 'Conclusions'.

LITERATURE REVIEW

Cloud computing is not a technologically new paradigm (Howie, 2010). The core technologies incorporated in cloud computing model have been readily available. Why is it then that earlier day 'distributed computing' emerged today as 'cloud computing' (Cubitt et al., 2011)? To understand this re-emergence, it is useful to view adoption and deployment of information technologies in organizations in a greater perspective.

During earlier adoptions of information technologies by organizations, there has been a lack of coordinated longer-term strategy and planning (Butler and Murphy, 2007). Departments within the organization, and their branches, have been deploying information systems meeting their specific needs (Palanisamy et al., 2010). This has led to a number of installations having overlapping functionalities yet lacking interoperability (Papastathopoulou et al., 2007). As a result, management and maintenance costs of information technologies have risen sharply. To reduce rising costs, the necessity to economically coordinate, merge and manage distributed information technology resources has surfaced (Georgantzas and Katsamakas, 2010). Drastic reduction of information technologies and adoption of uniform platforms within organizations was not a solution. It would be costly due to significant reengineering and personnel retraining. A feasible solution to the problem emerged in a form of organizational portals (Sullivan, 2004; Collins, 2000). Portals provide a single-point access to distributed organizational resources (Oertel et al., 2010). The bridging technology between diversity of localized implementations and single unified access point has been the service-oriented architecture and design (Rosen et al., 2008). The service-oriented architectures permit accessing information technology resources over networks such as intranets and internets–within or outside of organizations. Thus, allowing organizations efficiently re-use the existing information technologies and related resources.

Distribution of resources and their accessibility over computer networks have been the central characteristics of cloud computing (Linthicum, 2009). Cloud computing model embraces distribution of information technology resources and their *on-demand* provision via networked environments (Iyer and Henderson, 2010). Resources can be distributed physically across geographical locations or logically across servers. They are accessible within organizations via intranets and outside of organizations via internet. Standardized protocols facilitate communication over both intranet and internet networks. This model allows economically efficient utilization of computing hardware, software, and web services (Morton and Alford, 2009).

Cloud-based model has both advantages and disadvantages. Cloud-based providers generally emphasize advantages, such as speed and ease of deployment, while they downplay or hide risks. Security, control and legislative issues are among significant risks (Anthes, 2010; Lanois, 2010). Organizations must account for these, and other risks (Subashini and Kavitha, 2011; Hamlen et al., 2010; Julisch and Hall, 2010). Adoption of cloud-based model should be managed and approached in a balanced manner (McKinney, 2010).

Variants of Cloud-Based Models

Cloud computing models have three common characteristics: distribution of resources, accessibility via computer or communication networks, and on-demand provision (Rimal et al., 2011). Information technology resources may be distributed across geographical locations, hardware and virtual environments. Geographical distribution refers to physical locations where infrastructure, hardware or services are located. Physical locations are chosen with respect to various factors; such as favorable legislation, utility costs and personnel availability. Hardware-level distribution refers to allocation of physical hardware resources to specific services. For instance, one service may utilize computing power of several servers. Virtual-level distribution relates to segmentation of services across virtual environments that run on single or multiple hardware.

Accessibility of distributed information technology resources and services is facilitated by computer and communication networks (Frischbier and Petrov, 2010; Haeberlen, 2010). Standardized protocols are used for accessing resources over both intranet and internet. Insecure connectivity may be used on intranets within an organization. Secure connectivity is preferable for accessing resources outside an organization—over internet and public communication channels.

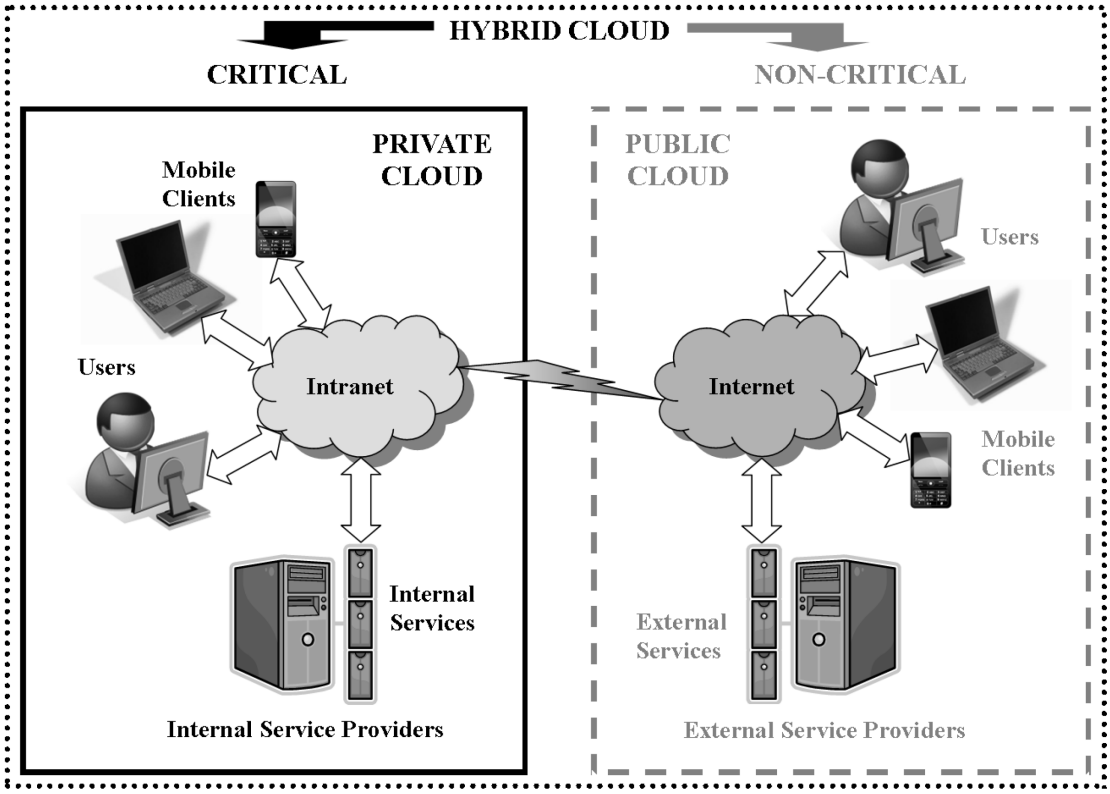
Resources in cloud computing systems are often provided on-demand (Goscinski and Brock, 2010). Both hardware and software resources can be dynamically allocated depending on varying needs of application services or users. Providers impose allocation limits with respect to their capabilities or contractual agreements. In-house cloud-based systems are closely tailored to the needs of organizations and their users. External providers are general-purpose oriented, since they serve various organizations and users with diverse demands. On-demand provisioning of resources permit flexible accounting. Organizations and users should pay only for the resources they used. This approach is beneficial in cases where there are significant fluctuations in use of resources.

There are three main models of cloud-based environments: private, public and hybrid. They are illustrated in Figure 1. All three models share the common features: resource distribution, accessibility via networks and on-demand provision. Distinctive characteristics relate to the ownership of provided information technology resources.

Private clouds refer to information technology environment where resources and services are owned by the organization that utilizes them (Orakwue, 2010). That is, all the infrastructure, hardware and services are in-house. The organization has its own information technology division that manages internal

infrastructure, hardware and software. Services are accessible within the organization via intranet. Access to information technology resources and services from outside the organization is optional. If the outside access is provided, it is usually via secure communication protocols. Services and resources are tailored the organizational needs and the organization has full control over them. This is the most secure model, but also the most expensive one. The organization must allocate financial and human resources to deployment, management and maintenance of utilized information technology resources and services. It requires greater initial costs and deployment time.

Figure 1: Illustration of Cloud-Based Models



Private cloud represents a model where information technology resources and services are contained within an organization and accessed via internal networks–such as intranet. In public cloud, services and resources are provided by external providers and accessed over internet. In hybrid cloud model, critical services and resources are provided internally and accessed via intranet, while non-critical ones are supplied by external providers and accessed over internet.

Public clouds relate to configuration where an organization does not own its core information technology resources and services and maintains only minimal setup. Information technology needs are outsourced (Hofmann and Woods, 2010). Outside providers own and provide services and resources required by the organization. They are not tailored to the needs of the organization and are general-purpose oriented, since the provider serves also other organizations. The organization does not have control over services and resources—the provider does. Services and resources are accessible over internet. Whether secure or insecure communication protocols are used is decided by the provider. This is the most insecure model, but the cheapest one. The organization may save the costs of deployment, management and maintenance of information technology resources and services.

Hybrid clouds pertain to a setup where an organization owns its core information technology resources and services. They are hosted and provided in-house. Non-critical services are outsourced to outside providers (Sotomayor et al., 2009). Critical resources and services are accessed internally via intranet,

while non-critical resources and services are accessed via internet. Critical services and resources are tailored to the organization's needs and the organization maintains full control over them. Provider has the control over non-critical services and resources. Hybrid cloud model represents a security-versus-cost compromise between private and public cloud models. The organization securely manages core resources and services, and saves costs by outsourcing non-core ones.

Categories of Cloud Services

Cloud computing services are broad. They range from hardware infrastructures, throughout software, to development platforms. Three major categories of cloud computing services are: infrastructure as a service, software as a service, and platform as a service.

Infrastructure as a Service (IaaS). Hardware and network infrastructures, together with related constituents, are provided as services. These may include complete computing hardware; such as computing servers or server clusters. Specific computing elements are targeted as well, such as Central Processing Unit (CPU) time of high-performance computing systems. Supercomputers are costly but fast. Thus, their CPU time can be provided as a service for computationally intensive applications and tasks. Data storage is another hardware related element. Data storage providers offer capacity for storing data and associated services such as backups. Bandwidth of high-speed networks is also utilized as an element of service; for instance, in video streaming for movie or television networks, in phone calls over networks, or in online video conferencing. The infrastructure and hardware services may be hosted in-house, or supplied by outside providers.

Software as a Service (SaaS). Functionalities of software systems are provided as on-demand services (SIIA, 2001). Large-scale software systems may be underutilized by individual divisions/users within an organization or costly. Hence, it may be more economical to share their functionalities. Spectrum of software services and related functionalities is broad. For instance, customer relation management systems, sales management systems, human resource management systems, content management systems, electronic commerce services, collaboration suits, office productivity suites, social networking services, e-mail services, etc. Benefits of SaaS adoptions are primarily associated with centralized management and maintenance of software. That is, security updates and patches, software upgrades and licenses are centrally managed. Users are provided with professionally managed and up-to-date software.

Platform as a Service (PaaS). Computing platforms and solutions are provided as services. Range of solutions in this domain is wide. They include facilities and tools for application design and development, testing, versioning, integration, deployment and hosting of applications, web service marshalling, security and persistence, state management, application instrumentation and developer community facilitation, etc. PaaS providers aim at enveloping the complete development lifecycle. Some aspects of application development are out of reach for individual or even organizational developers; for example, integration with third-party systems or large-scale testing. In such instances, PaaS providers have the ability to bridge the gap.

CLOUD RELATED CONCERNS

There are several significant concerns associated with cloud adoption. The majority of concerns are related to public clouds (Subashini and Kavitha, 2011; Lanois, 2010). Private clouds have the least number of issues. Three primary dimensions of concerns are outlined in Figure 2. They are concisely addressed in the following subsections.

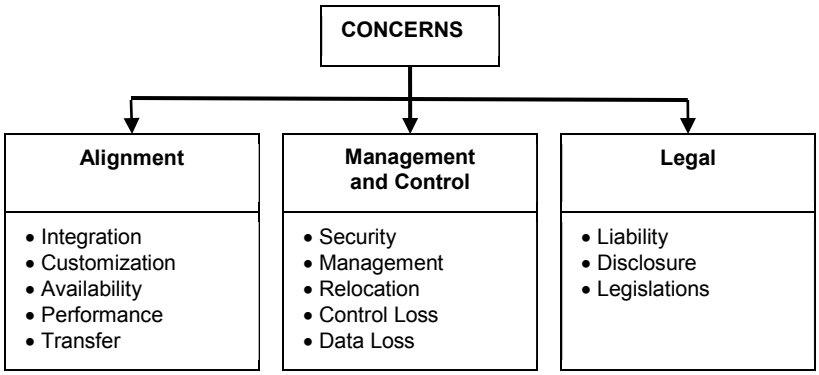
Alignment

It is important to align the organization's functional and operating model with the cloud-based model of utilization of information technology resources and services. Misalignments lead to decreased operating efficiency and losses for organizations. Following are several pertinent points for consideration.

Integration. Cloud-based services should easily integrate into information technology architecture of organization. They should be compatible with the existing formats, interfaces, and other structured data. If there are discrepancies, the integrating services should be provided.

Customization. Continual adjustments of services are important for meeting changing demands of users and organizations. Provided cloud-based services should be customizable at several levels to accommodate diverse needs. Without possibilities of customization, users and organizations may encounter substantial re-training and adjustment costs.

Figure 2: Three Essential Dimensions of Cloud Related Concerns



Three main dimensions of cloud related concerns are: alignment with existing operating model in organization, management and control of organizational data and services, and legal aspects.

Availability. Availability refers to readiness and accessibility of services. Cloud-based services are accessed via computer networks. Within organization, the access is provided via intranets, and outside organization via internet. It is important that high network reliability and readiness of services be provided. If the network is inaccessible, or services are not ready, users are unable to access critical services and data.

Performance. Scalability and performance of cloud-based services are closely related. Services should have satisfactory performance in order to accomplish the tasks users require. They should also be scalable to growing number of users. That is, performance of services should not decrease with growing user base. Several factors affect performance, however, the pertinent are network bandwidth, and computing resources allocated to services.

Transfer. Transferability of data and services should be easily manageable. It is necessary to consider transfers between intended cloud service providers as well as between providers and users. Organizations and users should avoid vendor lock-in. Complications during transfers between providers and backward to users could be costly and troublesome.

Management and Control

Management and control of data and services is one of the most important issues for organizations and users (Julisch and Hall, 2010; Hamlen et al., 2010). Public clouds pose the highest risk in terms of security and control. Private clouds enable full control of data and services as well as the greatest potential for security risk minimization. Following are the essential issues.

Security. Organization's data and services are among the most valuable assets. Moving your valuable data and services to outside providers poses essential security risks. The provider or other entities can compromise them. Accessing data and services over internet presents further risks. Internet transmissions propagate throughout various networks and are monitored and recorded by several third party organizations. Using secure communication protocols is crucial.

Management. Having potent managerial oversight over organization's data and utilized services is crucial. This should include data encryption, updates, deletes and backups. Data encryption is mandatory, in order to avoid possible compromization. When utilizing outside providers, it is important to properly manage actualizations between updates and backups. For instance, if sensitive data is deleted online, it remains on provider's servers and backups—where it can be compromised.

Relocation. Relocation of operations and secure move of organization's data back in-house or to different cloud provider should be fast and simple. Complications and delays in relocations and secure data moves may affect organization's operations and result in losses. Providers that do not allow secure, fast and simple relocations should be avoided.

Control Loss. Organizations and users should retain access control to their data and utilized services. Granular control of access privileges is desirable. In case of compromization, the control over data and services may be lost or transferred to other entities. Regaining the control should be fast and secure. Providers should maintain several layers of security.

Data Loss. Organization's data is a highly valuable asset. Data loss may have severe consequences. Despite reliabilities of backup systems, there is always a possibility of data loss or damage in cloud-based environments. Organizations and users should account for such possibilities and have adequate measures in place.

Legal

Legal aspects play important role in cloud computing. Relative novelty of cloud computing brings a number of legal challenges. The issues of liability, disclosure and legislative differences in various geographical regions are among the major ones to consider.

Liability. Cloud providers legally distance themselves from liabilities. Users of services offered by public cloud providers have limited or nonexistent legal protection. This presents significant challenges in important cases such as security compromization, data exposure, loss and damage. Nonexistent legal protection discourages adoption of services in public cloud environments.

Disclosure. Cloud providers are obligated to disclose data of organizations and users to certain government agencies and courts. This may happen even without notifying the affected organizations and users. Disclosure of sensitive economic data may harm organizations and negatively affect their competitiveness.

Legislations. Distributed nature of cloud computing model inevitably touches upon the issue of diverse legislations. Cloud-based services and data centers are distributed worldwide. When utilizing public

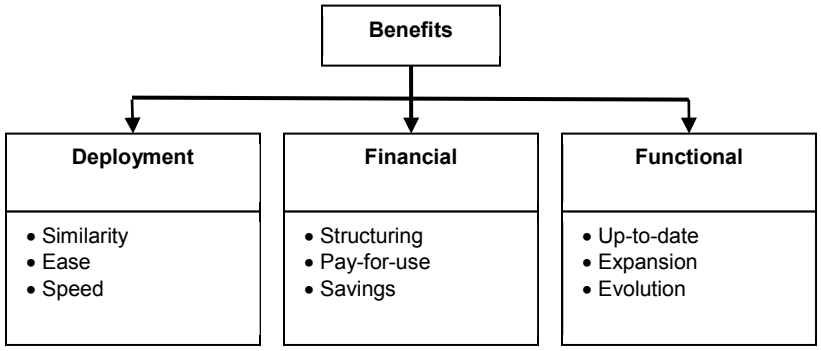
clouds, organization's valuable data may be distributed across geographical locations with inadequate or nonexistent legal protection and security.

CLOUD RELATED BENEFITS

There are benefits associated with cloud-based systems and services (Anthes, 2010). Organizations and users are primarily concerned about security and control. Security and control benefits are clearly associated with private cloud systems. The private clouds have also strong potential to avoid the most significant dangers. Employment of public cloud services significantly raises the security risks. One reason is the transmission of data over internet. Transmissions are monitored by several agencies and recorded by third parties. Thus, even if the organization uses encrypted communication protocols, third parties may intercept and compromise transmissions. Another reason is the loss of control over data and services on the side of public cloud providers.

Principal benefits of cloud-based systems are threefold: relative straightforwardness of deployment, financial flexibility and cost saving, and progressively managed functionality. Three benefit dimensions are depicted in Figure 3 and concisely described in the following subsections.

Figure 3: Three Fundamental Dimensions of Cloud Related Benefits



Three main dimensions of cloud related benefits are: deployment advantages, financial savings, and functional aspects.

Deployment

Deployment of cloud-based systems is becoming increasingly straightforward. Numerous advancements have been made on software level that facilitate virtualization and cloud adoption. All major operating system platforms provide high quality cloud solutions—both free and commercial. The main deployment process advantages are similarity to outsourcing, ease and speed.

Similarity. Deployment of cloud-based systems and services is similar to outsourcing. If organizations and their information technology managers have outsourcing experience and expertise, they are able to weight problems and benefits associated with cloud-based services. Information technology managers should be capable to ascertain which cloud-based model is the best suited for the needs of organization and its members.

Ease. On the technological side, deployment of both internal and external cloud-based services is relatively easy. This particularly holds in the case of outside providers. The providers specialize in cloud-based services. Hence, they have experience in easy adoption. However, this is generally valid for previously unused services. Transfer of existing services and data is more complex.

Speed. Deployment of cloud-based systems and services is relatively fast. There are numerous ready to use packages suiting various needs of organizations and users. Hardware and software solutions are modular. Modularity improves speed and ease of integration. Similarly, external cloud providers have a range of services available for immediate use.

Financial

Advantages of cloud-based systems in the financial domain are among the most pronounced. Cloud computing services have potential to decrease costs and increase flexibility of information technology investments in organizations. Major financial advantages include cost-structuring, payment for only utilized services and resources, and savings.

Structuring. Payments for cloud-based services may be segmented into several installments—depending on agreement with the provider (e.g. payments monthly, quarterly or semiannually). Structured payments for cloud services are beneficial for organizations that are unable to allocate the initial costs for private clouds. By employing external cloud services, they can spread the costs over longer periods. This also benefits short-term planning, since the near-future costs can be estimated more accurately.

Pay-for-Use. Cloud providers employ utility-style payment. Resources and services are segmented by providers into units according to various aspects; for instance, used data storage space, amount of processed data, or processing time. Users pay only for the resources and services they used. This permits scalability and estimates of costs with regard to amount of utilized resources and services.

Savings. Adopting cloud-based services may permit cost reductions. Organizations can reduce costs due to reductions of information technology personnel, costs of hardware and software infrastructures, and maintenance and management costs. Cloud computing model also allows better utilization of information technology resources.

Functional

Functional benefits of cloud-based services are linked to better-coordinated and centralized management. Although the services may be distributed, there is a dedicated team of information technology professionals managing them. Focused and dedicated information technology management brings up several functional benefits. Notable benefits include regular actualizations of services–in order to keep them up-to-date, expanding functionality and progressive evolution.

Up-to-Date. Software, hardware and infrastructure at the sites of cloud service providers are professionally managed and maintained. They are usually kept up-to-date. Required maintenance, updates and patches are professionally administered. Users are provided with the latest stable environments. This process is transparent to users, so they do not need to be concerned with such issues as patching the latest security holes or bug fixes.

Expansion. Cloud services are under continuous innovation by information technology professionals, in order to provide desired functionality. Cloud environments feature modular architectures. This permits expansion of functionality by implementing and deploying new modules. Cloud service providers can respond to needs of users relatively by deploying new modules.

Evolution. Progressive innovation and evolution of cloud-based environments is managed and executed by information technology professionals. They are well positioned to merge the latest technology advancements with the needs of users. Furthermore, they are capable of evolving cloud services according to progressive technology trends.

ACTIONABLE MANAGERIAL RECOMMENDATIONS

Significant considerations and planning should precede adoption and deployment of cloud-based services (McKinney, 2010). Managers should carefully weigh the associated risks and benefits (Marston et al., 2011). The previous sections highlighted the pertinent concerns and benefits. However, there are numerous other aspects to be considered by information technology managers and professionals (Haeberlen, 2010). Given the contemporary technological and legislative landscape, managers are advised to take into account the following actionable recommendations.

The best long-term strategy is to aim at the private clouds. Cloud computing services and infrastructure are kept in-house and provided internally. If there are excessive resources, or unused computing power, cloud related services could be provided to other organizations and users for adequate remuneration. Providing cloud services brings additional revenue to the organization. This is the model adopted by the largest providers. Private clouds have the best advantages in terms of security, control and availability. Valuable organization's data and services are all in-house. There is minimum exposure to outside entities; hence, there is a low risk of compromization by third parties. Implementation of appropriate in-house security measures is necessary. Furthermore, private clouds provide the greatest control over valuable data and services in the organization. Availability of services in private clouds is also significantly better. The access in private clouds is internal–via intranets. Intranets are notably more reliable than the present-day internet.

Hybrid clouds are the second best choice. In hybrid clouds, some services are hosted internally, while others are outsourced to external providers. Hybrid clouds allow balancing various aspects of cloud computing model and adjusting cloud adoption according to concerns and capabilities of organizations. Important issues are security, control and availability. It is essential to keep the mission critical services, data and infrastructure in-house. Non-critical services may be outsourced to external cloud providers. Hence, the organization shall maintain full control over its valuable services and data. There should be preserved strict separation between the core and the residual services and data. The separation should be preferably both physical and logical. That is, separate hardware and infrastructure is devoted to critical and non-critical services and data. Strict separation minimizes the risk of compromization by external entities. High availability of critical services and data should be provided by utilizing local intranets. Internet should be used only for accessing non-critical services and data, and secure communication protocols should be the standard.

Public clouds represent the least favourable alternative. In public cloud model, the organization utilizes external providers for both critical and non-critical services. It also stores organization's valuable data on provider's servers. Public clouds pose the highest risks and loss of control over organization's data and services. There is also significant risk of compromization by outside entities. The organizations employing public cloud services should have developed protocols addressing the issues of compromization, loss or damage to their data and services. Data should be kept in encrypted form at providers' servers and the organization should safeguard the encryption keys internally. Access to data and services should be via secure communication protocols. Legislative issues in public clouds play important role. Issues of liabilities and domiciles should be clearly stated. Data centres of providers may be located in regions with unfavourable legislations. Organizations should make sure that their data and services are hosted in regions with adequate legislative protection and enforceable rules.

CONCLUSIONS

Cloud computing does not institute a novel technological paradigm. It is a fusion of readily available technologies and enablers. Cloud-based services and technologies are associated with both benefits and risks. They should be approached with caution. The major risks are associated with public clouds.

Private clouds are the most beneficial. Information technology managers should carefully weigh advantages and disadvantages prior to adopting cloud computing model in their organizations.

The most important decision, after elucidating a number of factors, is the choice of cloud computing model. There are three main models: private, hybrid and public. Private clouds are in-house. The cloud infrastructure and services are hosted inside the organization and are owned by the organization. Public clouds signify the opposite of private clouds. The infrastructure and services are hosted and owned by external providers. Hybrid clouds feature the compromise between private and public models. Certain services are owned and provided within the organization, while others are owned and provided by external providers.

Understanding cloud computing risks and benefits is crucial. The greatest risks are security, loss of control, availability and legislative aspects. Security risks refer to the compromization of organization's data and services by outside entities. Loss of control is the inability to have exclusive control of data and services outside the organization. Availability underlines the readiness of services and data. It is largely affected by quality of connection between the access point and the service location. Internet connectivity is presently significantly less reliable than organizational intranets. Legislative aspects relate to liabilities and adequate legal protection of users. Notable benefits of cloud computing models are relative ease of deployment, cost savings and payments. Cloud computing services are designed for fast and easy deployment. By adopting cloud-based architectures, organizations can decrease costs related to staff, infrastructure, maintenance and management. On-demand services are aligned with utility-style payments—you pay for what you use.

Private clouds are the most beneficial in the long term. They feature the highest security, the greatest control and the best availability. However, private clouds may require higher initial costs. Public clouds are presently the most unfavorable. They pose the highest security risks, the lowest control and the greatest legislative gaps. Organizations should avoid reliance on public clouds. Hybrid clouds represent a compromise between risks and costs. Risks are minimized by keeping the critical data and services in-house—in private clouds. Costs are reduced by outsourcing non-critical services and data—to public cloud providers. Strict separation of critical and non-critical services and data should be preserved.

Hybrid clouds have promising future in diverse organizational environments. While large organizations have resources to implement private clouds, medium and small organizations may explore advantages of hybrid cloud systems. Hybrid clouds can balance risks and benefits. Unfortunately, there is a significant scarcity of hybrid cloud studies. Our future research will attempt to bridge this gap.

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.

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.

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.

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

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.

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.

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.

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

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.

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.

SIIA, (2001). Software as a Service: Strategic Backgrounder. *Software & Information Industry Association Report*, February 2001, http://www.siia.net/estore/pubs/SSB-01.pdf

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 laboratory 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 laboratory head 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.