Comparative Analysis of Private and Public Cloud Computing

Miss. Karin Adu
Student
Department of Information Technology
Sikkim Manipal University
Ghana, Accra
karinogh1009@gmail.com

Mr. Issah Bala Abdulai
ICT Tutor
Department of Mathematics and ICT
Kibi Presbyterian College of Education
Kibi, Ghana
isa_bala@yahoo.com

ABSTRACT: Cloud computing is commonly termed as the cloud. It provides the delivery of on-demand computing resources everything such as data centers, applications and Operation system platform over the Internet on a pay-for-use basis, Scale up or down quickly and easily to meet demand and All the IT resources you need with self-service access. In this Paper emphasis will be based on differentiating between private and public cloud computing with respect to security and cost since these drivers can prevent most organizations from adopting cloud computing.

KEYWORDS: Public cloud, Private cloud, Security issues, PaaS, IaaS and SaaS

I. INTRODUCTION

Cloud computing is gradually gaining acceptance in the business world and companies need to make cloud computing as part of their daily operations. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users.

Data center managers see the cloud as a way to reduce server acquisition and support costs, enabling them to focus more on actual business problems. Cloud computing is a model of information processing, storage, and delivery in which physical resources are provided to clients on demand and reduce the physical infrastructure requirement [3].

Cloud computing is a model for enabling convenient and on demand network access to a shared group of computing resources that can be rapidly released with minimal management effort or service provider interaction. Cloud Service model are useful in ensuring services such Software as a Service (SaaS), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) meet customer's needs[1].

When customers can access web applications and services over the internet it is termed as Public cloud.

Each individual customer has its own resources which are managed by a cloud Service providers. In private cloud, data centers of an organization are solely own by the organization and all technical issues are handled internally.

II. CLOUD SERVICE MODELS

There are three main Cloud service Models which can be accessed by a customer depending on the service required at a specific time for a particular need [18].

These services are outline below:

A. Software as a Service (SaaS):

It is the most advanced and complex cloud model. The software services provide functionalities that solve user problems, whether it's an individual or an employee of a company [7][8]. Some examples of solutions that are now offered under the SaaS model include: business intelligence, Web conference, e-mail, office automation suites and sales force automation.

B. Platform as a Service (PaaS):

It is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones without the cost and complexity of buying and managing the underlying software/hardware [8][9].

C. Infrastructure as a Service (IaaS):

It provides the processing environment (servers, storage, load balancers, firewalls)[7]. These services can be implemented through different technologies, virtualization being the most common one, but there are implementations that use grid technologies or clusters [8][9]. An abstraction of an execution environment that can be made dynamically available to authorized clients by using well-defined protocols. Abstraction of a physical host machine, Hypervisor intercepts and emulates instructions from VMs, and allows management of VMs, VMWare, Xen, among others.

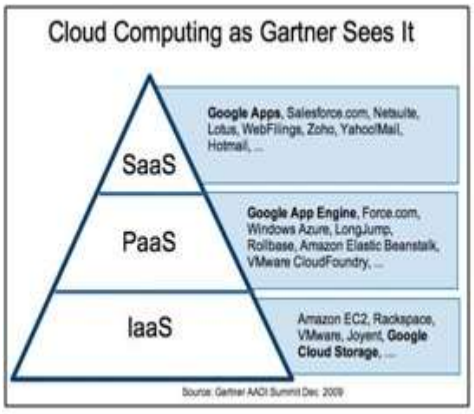

Figure 1: Cloud Service Models

D. Cloud deployment models

There are three primary ways in which cloud services can be deployed.

- Private Cloud Computing
- Public Cloud Computing
- Hybrid Cloud Computing

1. Private Cloud

Services and Infrastructure are hosted internally by authorized users [20]. It is primarily a data center deployed on the customer's premises. Here the customer owns all applications, firewalls, server infrastructure, operating systems and deployment site [5]. There is total control over data, applications, access controls and security [11]. A company can install, configure and operate the infrastructure to suit its requirement and demand. Hence mission critical systems and other deployed application are done in house with optimum security [14].

2. Public Cloud

Customers can access web applications and services over the internet. Each individual customer has its own resources which are provided by cloud service provider [20]. These providers facilitate multiple customers from multiple data centers, manage all the security measures and provide hardware and infrastructure for the cloud customers to operate [16].

This helps to reduce customer risk and cost by replacing their enterprise infrastructure. The cloud service provider is responsible for technical deployments, applications and operating systems. It is hosted in a remote location and security, access control and data privacy are all handled by the Cloud Service Provider.

3. Hybrid Cloud

It comprises of both public and private cloud computing with optimum security by keeping each aspect of a business in the most efficient environment possible. The flaws here are that proper track needs to be kept on different security platforms and ensure that all aspects of your business can communicate with each other. Hybrid Cloud architecture is the ideal combination that requires on premises resources and off site server based cloud infrastructure.

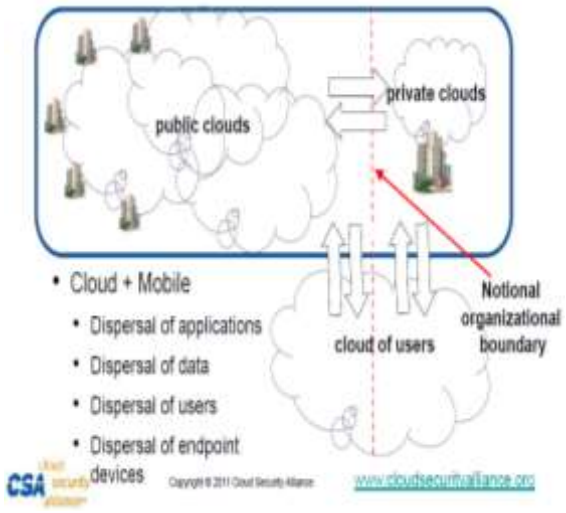

Figure 2: Cloud Security Alliance

E. Security Issues in cloud

The main hurdle in the fast adoption of cloud is the security concerns of the customers. Security issue has played the most important role in hindering Cloud computing acceptance [15].

F. Private Cloud Security and Cost Adoption

In the private cloud mode, there a distinct and secure cloud based environment in which only the specified client can operate. It provides computing power as a service within a virtualized environment using an underlying pool of physical computing resource. Hence it has more privacy and data control compared with the public cloud and is own as a data center on premise [14] [15].

Private cloud services draw their resource from a distinct pool of physical computers but these may be hosted internally or externally and may be accessed across private leased lines or secure encrypted connections via public networks.

1. **Higher security and privacy**: public clouds services can implement a certain level of security but private clouds - using techniques such as distinct pools of resources with access restricted to connections made from behind one organisation's firewall, dedicated leased lines and/or on-site internal hosting - can ensure that operations are kept out of the reach of prying eyes[13].

2. **Cost and energy efficiency:** implementing a private cloud model can improve the allocation of resources within an organisation by ensuring that the availability of resources to individual departments/business functions can directly and

flexibly respond to their demand [**19]**. Therefore, although they are not as cost effective as a public cloud services due to smaller economies of scale and increased management costs, they do make more efficient use of the computing resource than traditional LAN.

3. **Cloud bursting:** some providers may offer the opportunity to employ cloud bursting, within a private cloud offering, in the event of spikes in demand [13]. This service allows the provider to switch certain non-sensitive functions to a public cloud to free up more space in the private cloud for the sensitive functions that require it. Private clouds can even be integrated with public cloud services to form hybrid clouds where non-sensitive functions are always allocated to the public cloud to maximise the efficiencies on offer.

4. **Improved reliability:** even where resources (servers, networks etc.) are hosted internally, the creation of virtualised operating environments means that the network is more resilient to individual failures across the physical infrastructure [1]. Virtual partitions can, for example, pull their resource from the remaining unaffected servers. In addition, where the cloud is hosted with a third party, the organisation can still benefit from the physical security afforded to infrastructure hosted within data centres.

G. Public Cloud Security and Cost Adoption

The most recognisable model of cloud computing to many consumers is the public cloud model, under which cloud services are provided in a virtualised environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet[10] [18]. To some extent they canbe defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organisation has access. Public clouds, however, provide services to multiple clients using the same shared infrastructure.

1. **Ultimate scalability:** cloud resources are available on demand from the public clouds' vast pools of resource so that the applications that run on them can respond seamlessly to fluctuations in activity.

2. **Cost effective:** public clouds bring together greater levels of resource and so can benefit from the largest economies of scale [16]. The centralised operation and management of the underlying resources is shared across all of the subsequent cloud services whilst components, such as servers, require less bespoke configuration. Some mass market propositions can even be free to the client, relying on advertising for their revenue.

3. **Utility style costing:** public cloud services often employ a pay-as-you-go charging model whereby the consumer will be able to access the resource they need, when they need it, and then only pay for what they use; therefore avoiding wasted capacity [1].

4. **Reliability:** The sheer number of servers and networks involved in creating a public cloud and the redundancy configurations mean that should one physical component fail, the cloud service would still run unaffected on the remaining components [6]. In some cases, where clouds draw resource from multiple data centres, an entire data centre could go offline and individual cloud services would suffer no ill effect. There is, in other words, no single point of failure which would make a public cloud service vulnerable.

5. **Flexibility:** there are a myriad of IaaS, PaaS and SaaS services available on the market which follow the public cloud model and that are ready to be accessed as a service from any internet enabled device [18]. These services can fulfil most computing requirements and can deliver their benefits to private and enterprise clients alike. Businesses can even integrate their public cloud services with private clouds, where they need to perform sensitive business functions, to create hybrid clouds.

6. **Location independence:** the availability of public cloud services through an internet connection ensures that the services are available wherever the client is located [12]. This provides invaluable opportunities to enterprise such as remote access to IT infrastructure (in case of emergencies etc) or online document collaboration from multiple locations.

III. RESEARCH REVIEW/METHODOLOGY

According to survey carried out by Dzone, the adoption of Private and Public Clouds is growing at a fast pace for 2013.The vast majority of organizations have now deployed cloud computing (82%). The deployment of private versus public cloud is relatively close with 69% implementing private clouds and 61% implementing public clouds. And organizations are getting more advanced in their cloud deployments with more implementing both private and public clouds over just one or the other.

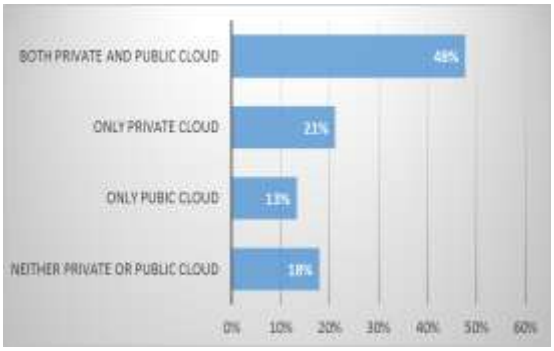

Figure 3: Security concerns for both Private and Public Cloud

Cloud Adoption by Business Size. The size of the organization impacts cloud deployment. We defined small- and medium-sized businesses (SMB) as businesses with under 1000 employees and enterprise as businesses with over 1000 employees.

Enterprises are more likely to Deploy Private Clouds: Almost all enterprises have deployed (84%) or have plans to deploy (additional 12%) a private cloud. Only 4% of enterprises do not have any plans to deploy a private cloud. Compare this to SMBs in which only half (50%) have deployed a private cloud. Another 18% of SMBs plan to deploy a private cloud, but almost a third (32%) have no plans to deploy this cloud type. Public Cloud Deployment More Even Across Organizations: SMBs are slightly more likely to have deployed public clouds than enterprises (66% vs 59%). But SMBs are also a bit more likely to not have plans to deploy public clouds at all (23% vs 20%).

Areas of Concern	Private Cloud	Public Cloud
Elasticity & Scalability	71%	88%
Self-service provisioning	66%	88%
Resource pooling	57%	63%
Programmable/API access	40%	61%
Metered Usage/billing	40%	61%

Table 1: Responses for Private and Public Cloud (2013)

These results illustrate that SMB organizations have been amongst the first to jump to the public cloud – given that it is the easier route to business agility (all you need is a credit card to get going). With many enterprises needed to contend with the "sunk costs" of existing datacenters and with many of the cloud providers building out their enterprise feature set in 2013, enterprise preference for private cloud makes sense but expect this to slowly balance out in coming years.

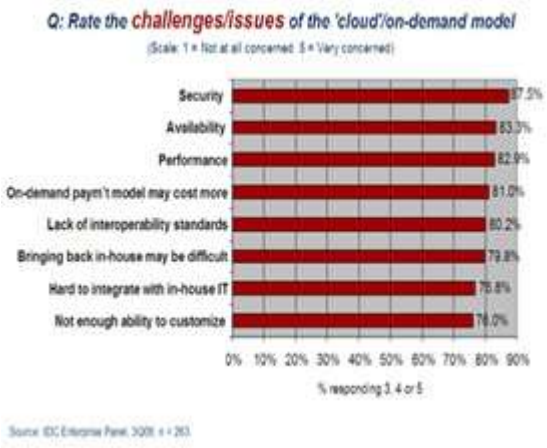

Figure 4: Challenges/issues of the Cloud/on-demand model

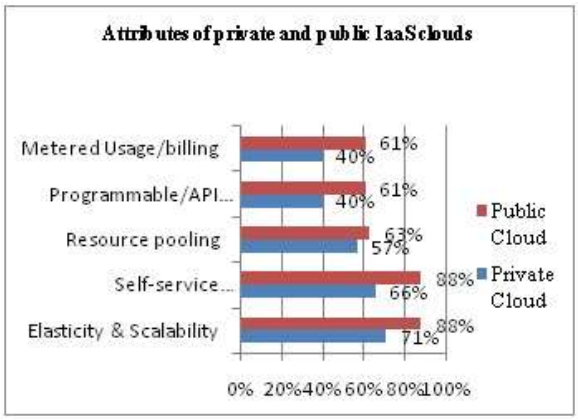

Figure 5: Attributes of private and public IaaS clouds

IV. DISCUSSIONS AND CONCLUSION

The public cloud and private clouds are not necessarily at odds with one another: although some companies may choose to implement one or the other exclusively, most companies in a position to choose one or the other can benefit from a mixture of both. Although not every in-house IT infrastructure can honestly be called a private cloud, there is some grey area, and the semantics are something of a peripheral issue.

In some case, certainly a private cloud may be a clear winner over the public cloud, and in other cases, vice versa. But this business decision need not be an all-or-nothing matter: in a contest between public and private clouds, hybrid clouds may dominate. Developing a strategic plan for virtualization will evolve into private or public computing, including your future virtualization architecture. Private cloud computing is a major investment. It requires technical expertise and constant monitoring to enable that all deployments are fully functional. It is more secured and can be implemented by larger companies and institution. Public Cloud may have privacy and security but it is

cost effective and needs less technical know how to handle it.

V. FUTURE WORKS

Further research on hybrid deployment models with will have to be done in order to improve upon security and cost effectiveness to create the platform for more business and institutions, small and medium as well as large enterprises to move into the cloud. This paper concludes that most enterprises will rather adopt to both Private and Public cloud to create a balance in terms of availability, security and cost.

VI. ACKNOWLEDGMENTS

My sincere thanks goes to the IT Faculty Head, Mr. Kamal Hiran for his constant support and guidance through the preparation of this paper.

VII. REFERENCES

[1] A Platform Computing Whitepaper.(2010)..Enterprise Cloud Computing: Transforming IT Platform Computing, pp 6.

[2] Arnold, S. (2009, Jul.). *Cloud computing and the issue of privacy*: KM World, pp14-22.

[3] Bala, I., & Henderson, J. C. (2010). Preparing for the Future: Understanding the Seven Capabilities of Cloud Computing.*MIS Quarterly Executive, 9* (2).117—131. ISSN 1540-1960.

[4] Brodkin., J. (2008, Jun.). *Gartner: Seven cloud-computing security risks*: Infoworld.

[5] Cloud Security Alliance.(2010). CSA.

[6] Danish, J. & Zaki, H. (2011). Security issues in cloud computing and counter measures. *International Journal of Engineering Science and Technology, 3* (4), 2672-2676. Issn : 0975-5462.

[7] ELC Technologies. (2010). Cloud Computing: *What You Should Know.* ELC Technologies.

[8] Geng, L., David, F., Jinzy, Z., & Glenn, D. (2009). Cloud computing: IT as Service :*IEEE computer society IT Professional*, Vol. 11, pp.10-13.

[9] Gens, F. (2009, Feb.). New IDC IT Cloud Services Survey: *Top Benefits and Challenges.*IDC eXchange.

[10] Grobauer, B., Walloschek, T., & Stocker, E.(2011). Understanding Cloud Computing Vulnerabilities. Security & Privacy: IEEE, Vol 9, pp 50.

[11] Hiran, K. K., Doshi, R. & Rathi, R.(2014, Feb). Security & Privacy Issues of Cloud & Grid Computing Networks. International Journal on Computational Sciences & Applications,4(1), 83-91.

[12] Hiran, K.K., & Doshi, R.(2014, Aug). The Proliferation of Smart Devices on Mobile Cloud Computing. LAMBERT:Academic Publishing.

[13] Mell, P., & Grance, T.(2009). Effectively and Securely: Using the cloud computing Paradigm. Boulder: NIST.

[14] Minqi, Z., Rong, Z., Wei, X., Weining, Q., & Aoying, Z. (2010).Security and Privacy in Cloud Computing: A Survey. Sixth international conference on Semantics Knowledge and Grid (SKG), pp 105.

[15] Morsy, M. A., Grundy, J. & Müller, I.(2010). An Analysis of the Cloud Computing Security Problem. *In PROC APSEC 2010*. Cloud Workshop. 2010.

[16] Ramgovind, S. M., Eloff, M., & Smith, E. (2010).The Management of Security in Cloud Computing. *In PROC 2010 IEEE International Conference on Cloud Computing 2010:*IEEE.

[17] Sahu, B.L., &Tiwari R.(2012). Journal of Advanced Research in Computer Science and Software Engineering 2(9) 33-37.

[18] Subashini, S. & Kavitha, V. (2010). A survey on security issues in service delivery models of cloud computing. Network ComputApplication. doi:10.1016/j.jnca.2010.07.006..

[19] Timmermans, J., & Ikonen, V.(2010). The Ethics of Cloud Computing. A Conceptual Review. 2nd IEEE International Conference on Cloud Computing Technology and Science.

[20] Vizard, M.(2013). Public Versus Private Cloud Distinction Starts to Blur [14] Tom bittman, The Spectrum of Private to Public Cloud Services.