Nottingham University Business School

"Cloud Computing"

Individual Report

Main Report: "The Use Of Big Data In Pharmaceutical Clinical Development"

Module Title: Individual Report for MBA Management Group Project

Submission Due Date: 13/09/2013

Academic Year: 2012/2013

Word Count: 5387 (Excluding table of contents, references)

Copy 1

Submitted By:

Gayatri Devi Rajasagi (4176787)

Table of Contents

List Of Figures And Tables

Figures:

Tables:

1. Introduction

The objective of this report is to explore cloud computing in depth i.e. its characteristics, model offerings and security issues etc. and how it could help Perceptive Informatics to provide better and faster IT solutions to its wide customer base.

Perceptive Informatics is a leading eClinical solutions provider who helps its customers to accelerate their drug development process through innovation. It offers its customers flexible software-as-a-service (SaaS) applications, which enables them to maximize their benefits of clinical trial technology (Perceptive.com, 2013).

Information Technology (IT) has been an ever changing and the fastest growing industry since its evolution. Most of the industries are relying on IT to enhance their performance and increase their revenue. One of the reasons for this dependence on IT is its high, reliable, data processing and storing capabilities. In the age of globalisation, enterprises require their data to be available in multiple geographical locations at the same time. However storing such huge amounts of data requires huge servers and applications for processing thus increasing the cost of the operations. Is there away to have this data present in multiple locations but at a reduced cost? Its known that necessity is a mother of all invention; and this necessity for data availability has lead to a new data sharing process known as cloud computing.

2. Cloud Computing

The term cloud computing (CC) was coined in the early year's of 2000. CC is to be known as an offspring of utility computing, distributed computing, virtualisation, grid computing etc. The reason it is called 'Cloud' is because of the availability of software, platform and infrastructure on the same network and service. (Che, J. et. al.(2011)).

In the budding days of CC it was anticipated to be one of the most promising business concepts for many enterprises, and is now seen as one of the fasted growing segments of the IT industry. Post recession companies are seeking to gain fast access to the top applications while drastically reducing their costs, by exploring the available offerings in cloud (Popović & Hocenski (2010)).

2.1. Definition of Cloud Computing

Over the years academia and enterprises have been defining cloud using various terms; the most commonly adopted definition in the industry for cloud is from he National Institute of Standards and Technology (NIST), which defines CC as:

"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p.2).

Mell & Grance (2011) state that CC is a made of three service models, 4 deployment models, and constitutes of five main characteristics.

2.2. Characteristics of Cloud Computing

According to the widely accepted definition from NIST, the five main characteristics of CC are:

1. **On Demand Self Service** - At any point of time the customer is able to obtain the required computing resources such as network access, CPU,

additional storage space etc. without any need of interacting with the provider thus making it convenient to operate.

2. **Broad Network Access -** As the services are provided over the Internet, data loaded on the cloud is easily accessible by the customer over any device that supports the usage of Internet. Such facility helps in easy and faster access, thus helping business to take decisions quicker and reducing the operation time.

3. **Resource Pooling –** The provider of cloud uses a multi-tenant model where all the resources such as data centres, servers and virtual machines. Through this model the provider assigns each customer with their relative servers and data centres thus providing customer independence, at the same time the customer has no control as to where the data is being stored and in what manner. Although while taking up cloud the customer has control over the choice of geographical area respective data centre he requires.

4. **Rapid Elasticity –** Enterprises that process data in high volumes are benefited from cloud as storage capacity is unlimited. At the same time Cloud Service Providers (CSPs) have the control to provide and revise the storage capacity for each client, by this storage space is efficiently allocated to various clients and thus providing cost benefits as the space used by the customer is charged.

5. **Measured Service –** By using metering capability these systems automatically optimize resource allocation. Thus providing the storage, bandwidth, and processing to the active users. Usage is easily monitored and thus maintaining transparency between the customer and provider of the services utilized. Along with the above there re other characteristics associated with cloud (Zhang et. al. (2010)).

6. **Multi-Tenancy –** CSPs of various cloud services are able to store their information on the same data centre. This allows sharing the performance and management issues of the cloud environment, where each layer responsibilities are pre-defined.

7. **Service Driven –** CC operates on a service driven model thus importance is given to strong service management. CSPs are responsible to

adhere to service level agreement (SLAs) setup while taking up the respective contract.

8. **Utility Based Pricing –** Last but not the least is its utility pricing model. Cloud computing operates on a pay-as-you go model also known as pay – per – use. The pricing mechanism could vary from service to service. For example, a SaaS provider would rent a virtual machine from an IaaS provider on a per-day basis. While a SaaS provider that provides on-demand clinical solutions to pharmas may charge its customers based on the number of trials it serves. This model relatively reduces the operating cost of the enterprises, as customers are charged on a per-use basis. Conversely, it does introduce difficulties such as controlling the cost involved in operations.

The above summarise the features of cloud computing that are proving to be advantageous to enterprises at negotiable costs.

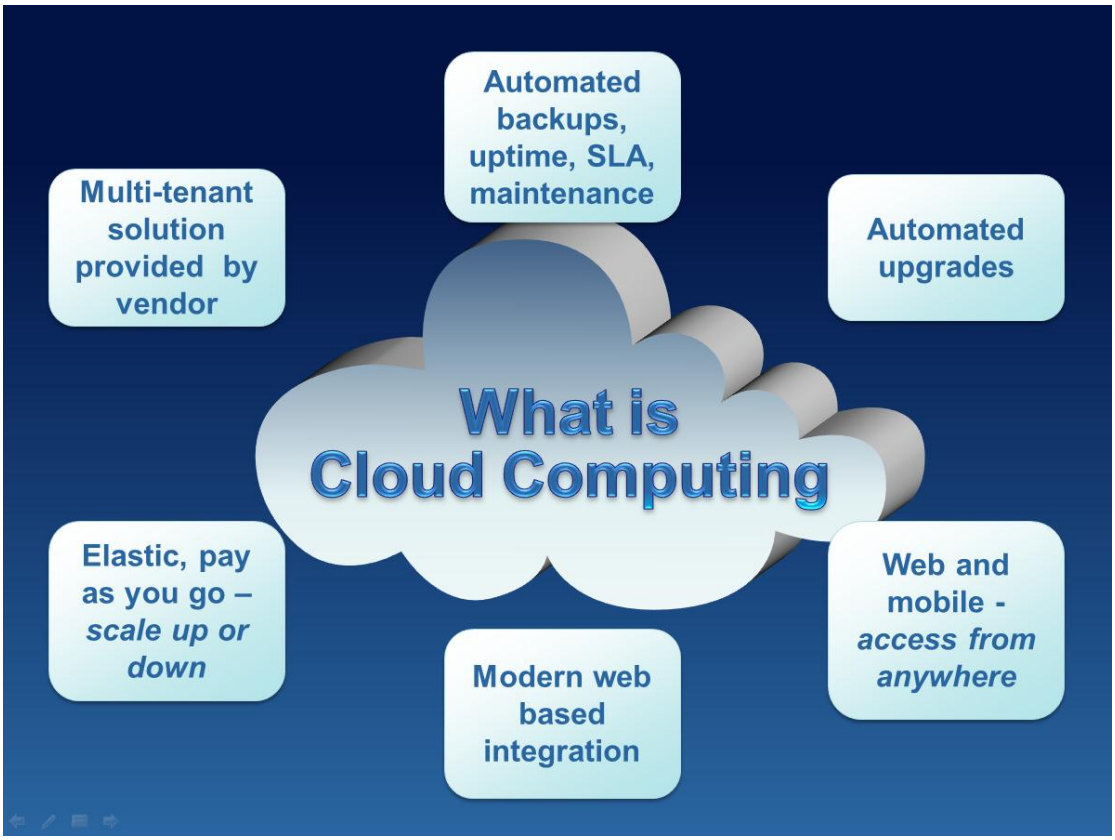


Figure 1. Cloud computing in a Nutshell (Abouttmc.com, 2012)

2.3. Benefits of Cloud Computing

As seen in the previous section, some features of cloud such as cost savings, elasticity, load balancing etc. are highly beneficial. Cloud computing is being used by various enterprises such Google, Facebook, Amazon and so on. Some of the unstated benefits observed by these companies are listed below (McKendrick, J. (2013)):

1. **Flexibility To Get Into New Business:** With the availability of on demand cloud resources where new setups can be up and running in matter of few hours, entrepreneurs and enterprises are able to access real time information at any given time and place. Convenient and safe access to bulk data allows aids to faster innovation and decision-making process. As the cloud works on pay – per – use model it reduces the cost involved in accessing the data. Shifts in the business focus can be achieved at a higher speed.
2. **Easier Mergers And Acquisitions:** Moving data from one company to the other is not only time consuming but also involves huge investment. With the availability of cloud systems and their easy access companies can now share data quickly and merge data systems as per required. For example telecom companies that operate on data need their operations and data processing to be up and running, lack of data transfer after a merger or acquisition can lead to major outages and down times leading to dissatisfied customers and a loss in business. Cloud is hence proving useful for and proving to aid smoother mergers and acquisitions.
3. **Replicate Business Processes:** As information from various sources is shared and is accessible from the cloud this enhances data sharing process. Enterprises can now easily access and implement best practices, which are tested and proven to be useful. For example if there are new methods implemented for a clinical research and proves to be successful then companies can share this information in real time and implement the same for projects in pipeline.
4. **Better Utilisation Of Resources:** With the implementation of cloud, companies can not only utilise their infrastructure resources in a better manner but also reduce their human resources involved in storing and processing data. Without the availability of cloud, companies need to

monitor processes for anticipating the need to increase or decrease the space. Cloud reduces the monitoring required significantly and thus also enhancing better resource utilisation and reducing costs at the same time.

5. **Segue Into Cloud Business:** With the availability of tools such as virtual machines (VM – These machines provide virtual access to various systems and servers, at the system are independently used by the company like any other physical machine. This reduces the infrastructure cost to deploy physical machines and maintain the same) companies are now able to build or rent a private cloud, which is not only accessible to internal users but could also be accessed outside the firewall with authenticity. The availability of compatible third party services is an additional benefit to the companies.

Amazon, Google, Microsoft and many more companies are investing billions of dollars into cloud computing to create large-scale systems, which comprise thousands of computers. The benefits of cloud are anticipated to increase at a large scale with more usage.

2.4. Cloud Service Models

As stated earlier the cloud operates on a service model where hardware and software are provided as services as per requirements, thus allowing enterprises to choose between the various service offerings as stated below (Kuyoro et. al., (2011)):

1. **Infrastructure as a Service (IaaS):** Is a single tenant service offering by the CSP that provides a virtualised infrastructure to its customers, thus allowing them to develop their on applications. This virtualised infrastructure doesn't only consist of VM but also storage space. With the availability of IaaS, companies can now build and run their own applications at a reduced cost, as the investment on establishing and maintaining physical machines and data centres is reduced drastically. At the same time the security provided in the IaaS is only at the infrastructure level, and companies are required to carter to security issues such as trusting a VM image, inter communication and access to the applications.
2. **Platform as a Service (PaaS):** PaaS sits on top of IaaS, and consists of a set of software and development tools that are available on the

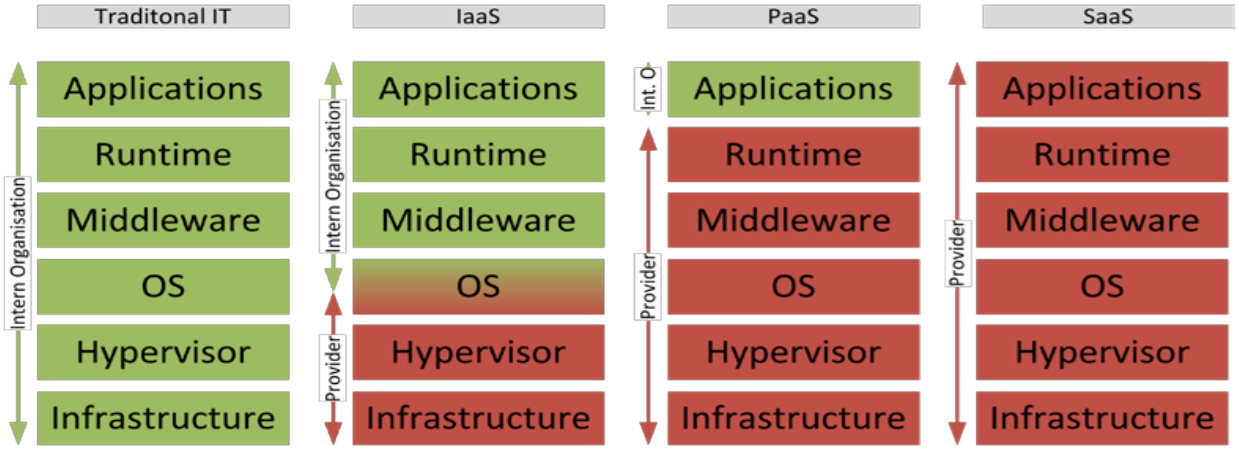
provider's servers. This developer environment helps the developers to build their applications without interfering with the service operations at the infrastructure layer. This service offers a complete software lifecycle development tool from the point of designing to software to maintaining it after being delivered. Companies using the Paas invest more on the operations rather than on capital investment. Similar to the IaaS, even though the underlying infrastructure is provided and managed by the CSP, companies need to build strong security systems in order to safe guard their applications and prevent any malicious attacks.

3. **Software as a Service (SaaS):** Is a software distribution model, in which the CSP provides pre developed software applications to its customers that are easily accessible over the Internet. SaaS is increasingly being adopted by many industries, as the provider has up to date applications and are customised easily as per customer requirement. It is often associated with the pay–as-you-use model. Due to the increasing efficiency of broadband performance and ability to access through various devices around the world, this model is able to serve the customers with excellent quality software, speed and security at a lower cost. Companies are able to use the software applications without worrying about complexities related to managing, supporting, obtaining licensing and last but not the least high investments. The SaaS is designed to work on multi tenancy model where multiple customers are using the software as independent users and thus helping them to achieve economies of scale. As applications are used over the Internet various Internet communities and third parties are working on providing high security to these applications.

Even though cloud provides IaaS, PaaS and SaaS at three different levels the boundaries for these various levels are still to be defined. Hence leading to interoperability issues between the clouds available today, and providing relatively less incentives for the providers of Cloud to invest in designing and providing new interfaces. With more usage of clouds and development of sophisticated applications as well as services the cloud industry would mature, and thus providing incentives to companies to develop better clouds, and increase interoperability.

Below is a pictorial view of the service model where Green indicates the level owned and operated by the company where as red is run and operated by the cloud service provider.

Figure 2. Cloud Service Models (Brunschwiler et. al., 2008)



Depending on the SLA the CSP takes charge of the services he provides and the level of access to be provided to the customers for the other layers (Brunschwiler et. al., 2008).

1. **Applications**: These are the front-end applications that are used by business.
2. **Runtime**: This states the environment in which the customer applications would be running on along with the prerequisites of running the application.
3. **Middleware**: This layer is the communication link between the various layers and the operating systems.
4. **Operating System**: It provides the hardware resources required to perform the computing needed.
5. **Hypervisor**: This layer is key in cloud as it provides the virtualized layer to the operating system thus providing the vm and other virtual infrastructure.
6. **Infrastructure**: This is the bottom and the main layer for each of the applications as it provides the physical systems such as the CPU, servers, storage units, networks, and other physical units needed.

2.4.1 Pros And Cons Of The Cloud Service Models

(Adapted from Brunschwiler et. al., 2008).

1. Infrastructure as a Service:

Advantages:

- System is highly scalable based on real time requirement
- Data Storage is redundant
- Data used and stored are physically separated
- Zero maintenance for the infrastructure
- Zero's down capital expenditure and only operational expenditure is incurred.
- Customer pays according to the use.

Disadvantages:

- Physical location of the data is not transparent.
- Storage and usage depends on the available infrastructure.
- Data processing is not isolated.
- Misconfiguration can lead to unauthorized access.
- Security of the system is challenged.

2. Platform as a Service:

Advantages:

- Less administration involved as infrastructure is outsourced.
- Development team can access systems from any geographic location.
- Zero maintenance for the tools required for developing the software.
- Zero's down capital expenditure and only operational expenditure is incurred.
- Customer pays according to the use.

Disadvantages:

- Systems could be inflexible
- Companies might be dependent on a single vendor due to lack of interoperability and portability.
- Additional cost is required for attaining different environments.

3. Software as a Service:

Advantages:

- All the applications are developed and used under the multi tenancy model.
- Projects are initiated and delivered quicker.
- There is no dependence on location.
- Zero maintenance to run the business functionalities.
- Zero's down capital expenditure and only operational expenditure is incurred.
- Customer pays according to the use.

Disadvantages:

- Cannot be accessed without Internet.
- Companies might be dependent on a single vendor due to lack of interoperability and portability thus causing vendor lock-in.
- Software applications are standardised and thus reducing adaptation to a large extent.
- System is highly vulnerable and thus requires additional securities in order to avoid malicious attacks.

2.5. Cloud Deployment Models

Cloud computing currently operates on four deployment models often known as the private, public, hybrid and computing model. Network, software, infrastructure are provided with a scale up and scale down features depending on the requirement needs of the customer (Mell & Grance , (2011), Dillon, T. et. al. (2010)).

These models have been developed in order to serve various requirements of the industries. For example in the banking industry or the defence system of a country would cannot share their information on a public cloud due to data sensitivity issues where as Google and Amazon and other big companies benefit more through the public cloud as more information is shared would enhance the work system and quality of data stored.

Below is the pictorial representation of the cloud computing definition given by NIST.

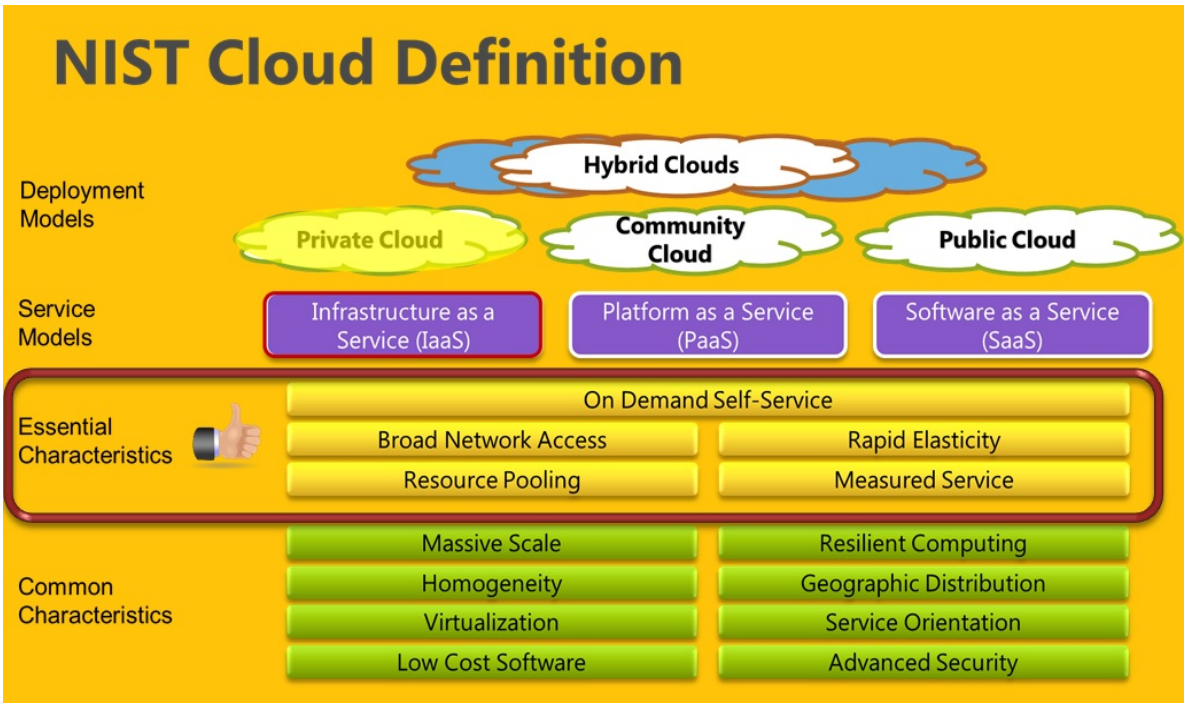


Figure 3. Cloud Deployment Model (Joyner, J. (2011))

1. **Private Cloud:** A private cloud is created to cater the needs of a single organisation and this cloud is either maintained by the owner company or outsourced to a third party, irrespective of the location i.e. either on premises or off. It is also known as internal clouds and provides a maximum degree of control over its performance, reliability and security. This helps to optimise the utilisation of the various in-house resources of the organisation. Due to the high sensitivity of the data involved in some organisations, security and trust are of prime concerns, hence companies prefer private over a public cloud. The need to have access and control over critical company activities is another reason why companies lean towards private cloud.
2. **Public Cloud:** Currently it is the most popular cloud in use. One of the key reasons behind its popularity is easy accessibility and availability. Although customers use their data and applications independently, the system is managed and controlled by the cloud service provider. Multiple users on the same system are achieved using the multi tenancy model. However the customer doesn't have any information on how and where the data is stored but can control the geographical

location. Google mail, amazon and apple are one of the examples of public cloud where, general public can add, update and store their information but have no access to its physical location. Currently this cloud is phasing challenges with respect to security and data integrity.

3. **Hybrid Cloud:** As the name suggests, it's a combination of two or more clouds often a private and a public cloud, which operate as different units but at the same time are put together with standard technology allowing them to be interoperable and also allowing application portability. Enterprises use this cloud to enhance their resource utilisation and core competencies by moving out their minor business functions to the public cloud while have complete control over their primary activities on premise using the private cloud. This model was developed in order to address the limitations of the individual clouds. This is achieved by running part of the infrastructure on a private cloud to achieve the security issues where as the rest is operated over a public cloud thus offering high flexibility. The hybrid cloud also provides on demand expansion and contraction of the services as required. One of the challenges with hybrid cloud is identifying and configuring the split between the private and public cloud.
4. **Community Cloud:** Many enterprises come together jointly to share the infrastructure, policies, networks etc. forming a community often known as community cloud. This cloud helps the community to achieve economic scalability and sharing data under stated policies. This cloud could be outsourced to a third party or could be set up in one of the organisations premises. This allows easy access and sharing data within set firewalls in large group of companies.
5. **Virtual Private Cloud (VPC)** (Zheng et al (2010)): Amazon Web Services has developed another alternate solution to address the issues in the above clouds. It runs above the public clouds. The main difference is that a VPC powers virtual private network (VPN) technology, allowing CSPs to design their own topology and security settings for the clouds. VPC is essentially a complete solution, as it not

only virtualizes servers and applications, but also the network underlying in it.

All the above stated clouds operate on a pay per use model thus allowing customers to use infrastructure and software at a reduced cost without compromising on the efficiency.

3. Cloud Safety

Even though the IT industry has been very promising over the decades, the safety and security issues that come along cannot be ignored. Security of the information is as important as cost reduction for an enterprise. Enterprises have been producing and analysing data for years together and have built their business on the same hence the safety of this transactional data is of prime importance. For example, the pharmaceutical industry, clinical data has been stored and maintained for decades.

According to a recent survey conducted by International Data Corporation (IDC) on the challenges of adopting cloud computing; one of the major concerns of top professionals has been with respect to the security and data integrity of cloud (Gens, F., (2009))

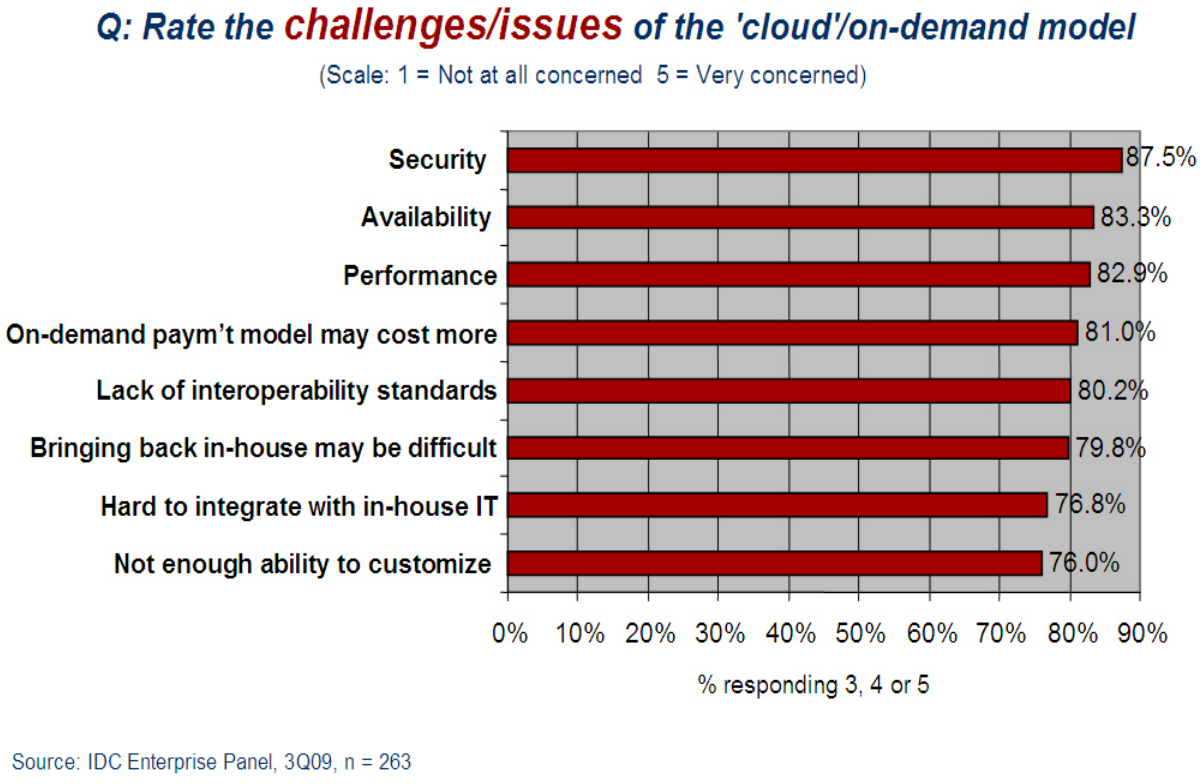


Figure 4. Cloud Deployment Model Gens, F., (2009)

Even with all the benefits of clouds and a negotiable price why is it a tough decision for enterprises to operate using the cloud? The below section explores the vulnerabilities and security concerns associated with cloud

computing.

3.1 Vulnerabilities In Cloud Computing

(Grobauer et. al., (2011))

Ever since cloud computing has gained popularity, it has been challenged for its security by various blogs, technological media, and academia. The biggest roadblock highlighted for the success of cloud computing is the issues related to security. Cloud computing has been challenged for risks, threat and vulnerability. ISO 27005 defines risk as **"The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization,"** (27000.org, (2008)). Vulnerability is a possible cause for risk.

Open Group's taxonomy defines vulnerability as **"The probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force".**

As cloud operates highly on Internet, it is easily exposed to hacking and malicious attackers. As most of the services are provided on virtualized machines, even virtualization is highly vulnerable to virtual escape; here details can be captured easily once they get access to the machine. Cryptographic mechanism used in cloud can be easily broken and hence exposing data.

Cloud requires management interface to access it on demand self-service, any unauthorized access to this management interface could lead to potential threats. Traditional systems have various administrators but for the cloud it would be a common management access thus increasing its vulnerability. With information accessible over Internet, the system is exposed to Internet protocols that can be attacked by unwanted users. As it works on pooled resources that are allocated according to use, user data vulnerability can occur as the space once used by a user would be allocated to the other when required. As the cloud follows a pay per use model, there could be billing vulnerabilities, as the metering is present in a layer, which could be evaded.

Vulnerabilities affecting the standard security control would also be affecting the cloud implementation know as control challenges. Some of the control challenges are with respect to network controls, which are not available due to the virtualized network in use. In the virtualized network it is difficult to differentiate a normal scan and an attacker scan into the system. In the virtualized network, traffic on a physical network would be affecting the virtual network for example having three virtual networks on a system; all the three would be affected if the main environment has network traffic. As stated in vulnerabilities, due to the interdependency of layers, even risks pass through the layers. Below tables summarize the security requirements and threats of these layers:

Table 1. User-specific security requirements (Zissis, D. & Lekkas, D. (2012)).

User-specific security requirements.

Level	Service level	Users	Security requirements	Threats
Application level	Software as a Service (SaS)	End client applies to a person or organization who subscribes to a service offered by a cloud provider and is accountable for its use	• Privacy in multitenant environment • Data protection from exposure (remnants) • Access control • Communication protection • Software security • Service availability	• Interception • Modification of data at rest and in transit • Data interruption (deletion) • Privacy breach • Impersonation • Session hijacking • Traffic flow analysis • Exposure in network
Virtual level	Platform as a Service (PaS) Infrastructure as a Service (IaS)	Developer–moderator applies to a person or organization that deploys software on a cloud infrastructure	• Access control • Application security • Data security, (data in transit, data at rest, remanence) • Cloud management control security • Secure images • Virtual cloud protection • Communication security	• Programming flaws • Software modification • Software interruption (deletion) • Impersonation • Session hijacking • Traffic flow analysis • Exposure in network • Defacement • Connection flooding • DDOS • Impersonation • Disrupting communications
Physical level	Physical datacenter	Owner applies to a person or organization that owns the infrastructure upon which clouds are deployed	• Legal not abusive use of cloud computing • Hardware security • Hardware reliability • Network protection • Network resources protection	• Network attacks • Connection flooding • DDOS • Hardware interruption • Hardware theft • Hardware modification • Misuse of infrastructure • Natural disasters

There are no standard security metrics currently available for cloud computing thus making it difficult to monitor the clouds. Without the development and implementation of these standard security metrics, controls for security check, audit, and accountability would be more difficult to implement.

3.2 Security Issues in Cloud Computing

We have spoken about the threat to growth for cloud is its security concerns. Current users and researchers have highlighted some of these concerns (Popović & Hocenski (2010)):

1. As resources are shared among companies through cloud, the physical security of the infrastructure is reduced due to lack of control.
2. Risk of violation of data sharing law can occur as different governments have different laws.
3. Vendor dependability is high.
4. Control of encryption and decryption is reduced.
5. As a common standard to ensure data integrity doesn't exist, data transfer, storage and retrieval in a safe environment can be a challenge.
6. Generating and maintaining security logs in a large cloud environment separately for each customer could be a challenge.
7. Companies could face legal implications if their data is floated in public. For example credit card details, or clinical trial data.
8. Data access is also a major concern. At any moment if the data subjects want to stop sharing their information, how would CSP ensure it has been removed from all systems?
9. Retention policy of clouds needs to be well defined in order to assure data is not missing in the future.
10. How can data destruction be assured by the CSP once a request has been place to delete the data?
11. Due to lack of legal standards, system and service auditing and monitoring is a challenge.
12. As the systems are maintained by the CSP, assurance of privacy breach notification is a challenge.

Brodkin had identified Gartner: Seven security issues in cloud computing which need to be addressed to benefit from the enterprise. Customers need to demand transparency of the systems and also avoid vendors who refuse to share their security methods. The security risks highlighted by him are (Gartner, J. B. (2008):

1. **Privileged User Access:** Processing of sensitive data outside the enterprise does involve inherent risks, as you lose control of the systems. Hence it is important to gain knowledge on the resources working on your data and also privileged administrator access.
2. **Regulatory Compliance:** It is important that customer's adhere to compliance while choosing vendors as they hold the primary responsible for the security and integrity of their data. It's thus the customer's responsibility to engage third party audits and monitoring.
3. **Data Location:** In cloud computing, customers do no have access to the physical location, hence its important to have data storage restrictions laid before hand for example, specific geographic location format etc.
4. **Data Segregation:** Multiple enterprises' data is stored on the same system with use of virtualized segregation. Encryption is the method used to differentiate the data but it's important to understand how the CSP does the same.
5. **Recovery:** While managing huge data there are high chances of losing data due to a disaster. Hence it's important for the customer to get assurance of data recovery and the time involved for the same.
6. **Investigative Report:** Due to multiple logins and data movement in the cloud, it is difficult to analyze the log the user activity. Thus it is important to avoid any damage it is important to get contractual agreement on the timely investigation of the data stored and access reports.
7. **Long Term Viability:** In the fast changing industry, it is possible for the cloud provider to merge with another provider or even breakdown, this could possibly lead to loss of data and operation interruption. Hence the CSP should state the back up plans in advance and also the formats the customer would receive the same. Also considerations of the financial aspect should be made if a new cloud is required.

3.3 Security Strategies in Cloud Computing

Construction: To avoid or reduce the security issues while operating on cloud, it is important to migrate data onto a system that assures security and reliability. One procedure is to state them in the contract in form of Service Level Agreements (SLA). Some helpful approaches are stated below (Che, J.et. al., (2011)):

1. **Traditional Security Practice Mechanism**

   International information security standards such as ISO27001 should be followed to secure the physical facilities, networks etc. Thus assuring the physical systems used for cloud are secure.

2. **Virtualization Security Risks Assessment**

   Security level of various virtualization technology resolutions and suite products need to be assessed for high security and only the best one should be chosen to reduce the security risks brought by virtualization.

3. **Development Outsourcing Risk Control**

   Constructing s huge cloud by a single enterprise is darning and thus work is outsourced, at the same time this introduces security issues. Strict control measures should be taken to assure the quality level and security requirement of the system developed.

4. **Portability and Interoperability**

   Due to unacceptable increase in the cost at contract renewal time, or business operations ceasing by service providers or decrease in the quality would require migration of data from one service provider to the other. Hence portability and interoperability should be considered before hand as a part of the risk management and security assurance for a given cloud program.

Operations: Similar measures can be taken in the operations to reduce security risks (Che et. al., (2011)):

1. **Business Continuity Assurance**
   Service providers should update the disaster recovery plans and also provide status updates on the functioning of the physical systems to the customers. A real time back up should be assured in case of any breakdown.
2. **Attack Proactive Alerting**
   As the cloud operates on large and multiple networks, at this stage it is inevitable to avoid security issues. Thus CSP should have systems to monitor the cloud 365 days 24* 7 and update the customer on any malicious intrusion.
3. **Data Leak Prevention**
   CSP and customer should configure strong system access such that there is no unauthorised access into the system. Also care should be taken during data transfer, so that the information is not hacked.
4. **Security Accident Notification & Response**
   In order to evaluate any potential damage occurred due to a security breach, CSP should alert the customer immediately after the occurrence. Standard security incident management plans should be updated and audited time to time.
5. **Security Accident Audits**
   The root cause of each security hazard should be analysed and preventive measures should be implemented to avoid a reoccurrence. Due to the increasing threat to sensitive data, governments and legal systems are trying to implements strong auditing systems to protect the data. Auditing should be a two way process where the customer and the CSP can check the systems on either sides, this reduces the possibility of over ridding information.

These are the possible measures that a company can take before an after migrating to the cloud to avoid the occurrence of security hazards.

4. Cloud As An Offering From PI

PI's goal is to help its customers perform better on their clinical trials by providing IT solutions with the latest technology. Clients would be benefited with a new product offering of cloud as they would be able to access their data over the Internet as and when required along with the MyTrials application.

PI would benefit financially by offering cloud to their clients as cloud can be operated at a negotiable cost. As seen in the previous sections one of the most beneficial models for PI would be to operate on the multi-tenancy model, as it allows processing multiple client data, with the use of virtualization thus helping to achieve economies of scale. One of the primary concerns for the pharmaceutical client's is the safety of their data, and the challenge using the cloud is safety of data. Even though with the existing challenges of cloud big pharmas like J&J are working on brining the pharmaceutical companies to share their practices and base data on cloud, so that the industry can benefit on a whole. PI could initiate similar offering where companies can opt for the hybrid model where generic information can be logged on a public cloud and at the same time clients have their specific activity data operating on their private cloud.

Cloud is an attractive product offering as it can be combined and offered along with Mytrials to the clients as a SaaS.

5. Conclusion

Cloud computing is a developing technology that aims to enhance managing and operating services over the Internet. PI would have a strong product offering and benefit financially as investment in moving to cloud is negligible as compared to setting up a new data center or network. PI would benefit in long term as cloud computing has a tremendous opportunity to grow and outperform.

6. References

Abouttmc.com, (2012)., " What is Cloud Computing?", Downloaded from http://abouttmc.com/microsoftdynamicsgp-netsuite-vs-microsoftdynamicsnav/netsuite/what-is-cloud-computing/. as at 18 August 2013

27000.org (2008)., " Introduction To ISO 27005 (ISO27005)", Downloaded from http://www.27000.org/iso-27005.htm. as at 22 august 2013.

Brodkin, J. (2008)., "Gartner: Seven cloud-computing security risks." , Downloaded from http://www.networkworld.com/news/2008/070208-cloud.html. As at 10 August 2013.

Brunschwiler, T. et. al, (2008).,: Cloud Computing." *Communications of the ACM*. Vol. 51 (7), pp.9 - 11

Che, J. et. al. (2011)., "Study on the security models and strategies of cloud computing",. *SciVerse ScienceDirect*. Vol.23 pp.586 – 593

Dillon, T. et. al., (2010), :Cloud computing: Issues and challenges." In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pp. 27-33

Diamond, P. F (2011).," Cloud Computing Augments Clinical Trial Process.", Downloaded from http://www.genengnews.com/insight-and-intelligenceand153/cloud-computing-augments-clinical-trial-process/77899424/. As at 12 August 2013

Gens F. (2009)., "New IDC IT Cloud Services Survey: Top Benefits and Challenges." Downloaded from http://blogs.idc.com/ie/?p=730., as at 15 August 2013.

Grobauer, B. et. al. (2010)., "Understanding Cloud Computing Vulnerabilities.", *IEEE Security and Privacy*. Vol.99, pp.50 – 57

Joyner, J. (2011).,"How cloudy is your cloud? The NIST offers a cloud standard.", Downloaded from http://www.techrepublic.com/blog/data-center/how-cloudy-is-your-cloud-the-nist-offers-a-cloud-standard/. As at 1 August 2013.

Kuyoro S. O., Ibikunle F. & Awodele O., (2011).," Cloud Computing Security Issues and Challenges.", *International Journal of Computer Networks (IJCN)*. Vol. 3(5), pp.247 - 255

McKendrick, J. (2013). , "5 Benefits Of Cloud Computing You Aren't Likely To See In A Sales Brochure.", Downloaded from http://www.forbes.com/sites/joemckendrick/2013/07/21/5-benefits-of-cloud-computing-you-arent-likely-to-see-in-a-sales-brochure/. As at 24 July 2013

Mell, P., Grance, T., (2011)., "The NIST Definition of Cloud Computing", *NIST Special Publication*., pp.1 - 7

Perceptive.com (2013) *Home Page*. Downloaded from http://www.perceptive.com as at 20 June 2013

Popović, K. & Hocenski,Z., (2010).,"Cloud computing security issues and challenges", *MIPRO*, pp.24 – 28

Zhang et. al. (2010) " Cloud computing: state-of-the-art and research challenges.", *The Brazilian Computer Society*., pp.7 - 18

Zissis, D., & Lekka, D., (2012).," Addressing cloud computing security issues". *Future Generation Computer Systems.,* Vol. 28 (3), pp.583-592