Cloud computing: security issues and challenges

Business, Industries

Cloud Computing: Security Issues and Challenges Name: Course: Date: Cloud Computing: Security Issues and Challenges Introduction Cloud computing is a new phenomenon that raises Information Technology (IT) to higher level that seeks to provide more scalable as well as flexible and powerful computing processes. Cloud computing seeks to provide services such as data storage and capacity as well as providing the clients with an opportunity to use software that would otherwise be expensive since they can pay as they use from the cloud provider (Limoncelli, Hogan & Chalup, 2007). It allows information technology services to be provided over the internet and encompassing services that include social networking as well as other interpersonal services.

It provides clients with a chance to increase their IT capacity as well as processing power without having to invest in new technology or infrastructure. Rather, a client only has to pay for the services (Knorr, & Gruman, 2013). Benefits of cloud computing are many such as flexibility that comes with the on-demand, its mobility as well as scalability that also comes with cost saving. This benefits of cloud computing have seen many companies adopt it since it saves some costs as well as the need for training workers to serve in the IT sector within the company. It has seen the growth of cloud computing grow tremendously over the last few years since 2008 when it become a promising concept within the business world. However, several issues and challenges surround cloud computing especially considering that several companies or firms could be storing their data in the same hardware.

As more and more companies continue to store their valued information in the cloud, security issues and challenges have come up especially concerning how safe the cloud-computing environment is. Although its growth is continuing and likely to continue, this has deterred several potential clients from adopting it due to the risks associated (Limoncelli, Hogan & Chalup, 2007). The challenges facing cloud computing include security, issues, performance, availability, portability or hardness in with integrating it with in-house IT and migrating from one provider to another, hardness in bringing it back to in-house IT, on demand costing services where some are worried it would cost more, and regulatory requirements. Although it is posed with several challenges, the most important or the one that has posed a bigger issue has been the security issue according to a survey conducted (Kuroyo, Ibuunle & Awodele, 2011). This paper looks at the issues surrounding cloud computing security as well as the other challenges identified. Security Issues Security issue is one of the challenges facing cloud computing.

However, several studies have shown that security is the main issue hindering the acceptance of cloud computing amongst many potential clients. The main issue with security has to do with trusting a third party to store your data as well as provide you with services over the internet. Companies have to trust their sensitive information to other parties, whom they might not know whether they temper with it. Using cloud computing is same as giving one’s information to another person for keeping. This has posed a serious threat to the users who feel that their information could be mishandled. The main issues within security include security in transfer of

data, secure software, and separation of data and access control of the users (Limoncelli, Hogan & Chalup, 2007). Further, hackers as well can use the loud services to design or make botnet considering that clouds provide a reliable infrastructure service at an economically favorable price. Transfer of data Organizations have to transfer their data to the cloud via the internet, which has a lot of traffic in it.

All of the data transferred when migrating as well as during services has to be within the internet. This raises a concern since one cannot be very sure about the security of the channels used. One has so ensure that data is transferred through channels with the right URL to avoid corruption from other internet malware. It is necessary to encrypt data always in order to secure the data. Therefore, a company has to use authenticated as well as encrypted data through standard protocols within the industry such as the Internet Protocol Security, (IPSec) that is specifically designed for protection of data over the internet traffic.

Having to trust confidential data to transverse over the internet raises issues since it is not a sure guarantee that it will not be tempered. Sensitive information for companies becomes a target to attackers over the internet, thus posing the main risk. Even though measures may be taken to ensure security, it is not always a guarantee that it will secure all the threats from attackers. Within transfer of data over the internet as well as provision of some of the services raises yet other issues. One of them is increased exposure to network. Before cloud computing, network exposure still existed.

However, cloud computing increases its risk. Accessing company resources directly over the internet presents greater risks that could be protected when companies have their own firewalls and security services within their own infrastructure. In the cloud computing, a company’s information is always in transverse over the internet, meaning it is compartmentalized with an internet connection to the rest of the world. With all the information in transit over the internet most of the times, more risks are realized since it can easily be attacked as opposed to when it is internally stored and away from internet traffic. The other risk posed by having most of the services such as software as a service and applications as a service is the increased exposure of applications. Previously, companies owned their own software and application that they operated within the organization. Cloud computing on the other hand provides applications as a service to the clients where they can use it over the internet. This cuts costs associated with having to buy the applications as well as licenses for most of the software.

However, using these services over the internet all the time raises yet another risk. Internet as good as it is has issues of security and attackers. Over the internet, applications can easily be attacked as opposed to offline applications. Most of the SaaS software is mostly built by third parties. Further, their APIs use the Representational State Transfer that lacks a predefined security method (vBox, 2011). Therefore, before moving ones resources to the cloud there are several security issues to consider such as the security systems used by the provider infrastructure used.

One has to be aware of the software interfaces used by the provider in order to access whether they are compatible. This further enables the organization to know whether the APIs and interfaces are reliable and strong enough since weak interfaces are prone to more security issues that are concerned with accountability, integrity and availability. Data Separation Before cloud computing became a popular notion within the information technology industry, organizations used to store their data in private serves and infrastructure such as hardware. Since they were stored internally within the organization, it was clearly separated from other organizations physically. Therefore, each organization stored its data separately from the other organizations since each had its infrastructure.

This is in exact contrast of cloud computing since organizations can share the same cloud, meaning the data is stored within the same infrastructure. Additionally, organizations had their own software and application that were separate from each other (Sorrels, 2010). One characteristic of cloud computing is that infrastructure is shared among several clients in many cases being several companies that could be competing. Therefore, unlike before where each organization stored its data separately from other organizations, it could be found in the same hardware where it is managed by a third party. Thus, an issue of separation is raised since errors could occur where information is mismanaged. Therefore, cloud providers need to ensure that data for each company of client is stored separately from the others.

This requires that clouds providers use hypervisor software that is used for creating virtual containers within the hardware of the provider where each client will have their own virtual container. However, it has been noted that attacks are coming up within the last few years, which is mainly focusing on the shared IT within the cloud. Data Storage Although this has been mentioned within the other security issues, it s considered yet another issue within cloud computing security. One issue that rose is the fact that data is stored in the same infrastructure used by other organizations. On the other hand, one can never know who has access to such data and who controls its transverse over the internet. Thirdly, one never knows the location of the infrastructure used by the cloud. Possibly, another country may not have the same security issues over the access to information.

For instance, such data access is not protected from non-users or other clients. One could never know whether unauthorized people have access to such information considering the organization does not have control over the infrastructure. User access control In the previous systems where organizations had their own infrastructure as well as applications and software, control of these resources was within their control. Cloud computing on the other hand puts the cloud providers under control of the company’s resources. This makes it hard for an organization to file for an investigation in case there is a problem with their resources or data. If anything goes wrong, it could be hard not only to sue the cloud, but also to locate the cloud infrastructure since one might not know where it is located.

In cloud computing, a company does not have access to the infrastructure where the data is stored as well as services are provided from. This way, a firm will only have access to their resources as the provider avails them as services. This poses yet another security issues considering that when a problem occurs, the firm will not have control. The cloud provider may take time before finding the underlying cause of the solution considering that the firm has to notify the cloud. This increases the response time as opposed to having one’s infrastructure where response can be immediately. Additionally, the company will not have the control to solve the problem considering the infrastructure is not within the control of the firm. Additionally, considering that one sues shared software, when any risk arises within the cloud it affects other firms as well since they have no way of controlling such an issue as well as due to the sharing of infrastructure.

Other Challenges Other challenges facing cloud computing are such as costing issues and billing or charging, interoperability, what should be migrated, reliability and the availability, performance and costs of bandwidth as well as the difficulties associated with migrating back to in-house information technology. Costing and Billing Issues Cloud computing is known to reduce the costs associated with running the information technology infrastructure internally or within the company. However, it raises the cost of other things such as costs associated with data communication and connection. With cloud computing, one has to constantly use the internet to access the services.

Internet connectivity does not come free. Therefore, companies will have to spend more money on transferring of the company’s data to the cloud as well as from the cloud. Additionally, the cost per unit of data or computing resources is likely to go higher. This is especially so when using a hybrid model there the company’s data is distributed to several public or even private clouds. Moreover, on-demand services are only valuable for services requiring intensive CPU usage (Kuroyo, Ibuunle & Awodele, 2011).

Therefore, cost saving associated with cloud computing only make sense when the cost of bandwidth is lower than the cost saved from having the infrastructure within the company or in-house. On the other hand, when it comes to billing of charging clients, it becomes hard considering the on-demand services. Assessment and budgeting of on-demand services is hard unless the cloud providers develop software as well as comparable benchmarks.

This is often made difficult by the elastic resource pools as opposed to the regular centers where costs are calculated based on consumption within static computing. Another issue that makes billing hard is the complexities associate with providing Software as a Service (SaaS) to the clients that offers multiple tenancies. The costs of developing software as a service are quite substantial and involve several factors that include, re-designing as well as development of software that previously was for single tenancy, providing new features to such software in order to allow customization, security and performance for the clients’ access. Subsequently, this requires the providers to weigh between the trade-offs from providing multiple

tenancy and the costs saved from reduction of overheads realized amortization as well as the reduction in number of licenses for software. With all this to consider, a model for costing is needed that would take into consideration all the factors.

Interoperability Issue Currently, companies or clients suing cloud computing do not have an option of migrating from one provider to another of accessing several clouds simultaneously. Additionally, it is a hard task to move data into the cloud as well as to integrate it with the in-house information technology services. This is because each cloud has a unique way in which the clients and other user can interact with cloud. This brings about the vendor lock-in where the providers limits the clients and users from choosing between the alternative providers that can offer simultaneous providing optimization of the resources within different levels in a company. Vendor lock-in happens in three ways, platform lock-in where the vendor uses one of the several possible platforms that include MVWare and Xen.

Thus migrating from one platform to another different platform becomes a complicated process. The other lock-in is data lock-in where data ownership is not yet defined upon moving data into the cloud. This makes it even difficult to move data from one vendor to another vendor.

Finally, the other lock-in is tools lock-in where the vendor could use tools that are not compatible with different virtual and physical infrastructure; it would be very difficult to manage data in other infrastructures. Such lock-ins provide rather a difficult time in seeking to achieve interoperability within cloud computing. More so is that the API of the clouds pose yet another

difficulty for integration of the cloud services to the company’s own systems. Interoperability seeks to achieve seamless integration of systems where there is easy access as well as interaction of data within the cloud and across as well and between the local applications within the company. With the different kinds of infrastructure and tools, seamless integration of data between the clouds and the companies become complicated. Interoperability is important since it allows easy migrating of data from the company to the cloud as well in the opposite direction.

More so, it allows the seamless flow of data between clouds. Interoperability has several advantages such as allowing optimization of the company’s operations such as when they need outsourcing some of their operations that could have different data within different clouds (AMCHAM, 2012). Further, it becomes hard for companies to use data stored in other clouds or even use software that is provided by one cloud in another. This makes it even harder considering the company would need to integrate some of this information. Although this is one of the big problems, it is arising now and could affect many. It is therefore important that vendor develop standardization that would enhance interoperability (Zissis & Lekkas, 2012). If the company or firm owning the cloud is bought out or faces issues, the clients suffer a major blow considering moving out or migrating to another cloud will be quit complicated. Reliability and availability Cloud computing is still a relatively new phenomenon and lacks enough players within the market as well as lack of regulations from government.

This makes it hard for monitoring and assessment of the clouds. There are no plans for supervision or regulation, which makes potential clients refrain from adopting it. When providing information technology to several organizations, a cloud could face problems such as too much traffic that slows it down. For instance, Carson (2011) sites that one time she needed to use the blogger but could not since it was down. She further cites that the blog was out for about 20 hours. This is quite a significant amount of time if the company needed the services. Customers requiring accessing some of the services from their company or even companies needing to use some of the application would have to halt their services until this outage is solved (Sabahi, 2011). In the usual IT resources within the company, it would take a shorter time to solve such issues since they are within the company.

Unlike the usual models, clouds require more time as well as intensified personnel to solve such issues. With such an issue likely to happen, it contributes to lack of acceptance to many potential clients especially for firms dealing with bigger loads of data to provide services such as online services companies. Some of the cloud providers have an agreement with the clients on the amount of time the services are likely to be running without outages or hiccups, most cite a 99. 9%service delivery time (Carson, 2011). This is the Service Level Agreement (SLA), where the provider to the SaaS agrees with the clients the time this service will be up running smoothly. Some of the outages are because of necessary maintenance or scheduled downtime and unscheduled ones when the cloud has problems.

When such problems occur, they pose a problem to not only one organization, but also all those organizations within the cloud (Carson, 2011). With such downtime and issues likely to halt services, the reliability of the cloud computing is reduced. However, this only seems quite a problem because it happens to many organizations and publicly as well especially for public clouds. Such downtime or outages are also seen with the in-house infrastructure where systems fail and it halts operations. The only difference is that this will affect several people and come out to the public unlike the in-house where such outages can be hidden or just known to the organization.

This publicity puts the hiccups of cloud computing at the lime light while as well putting the benefits in the same place. Although it has been reliable and available more than 90% of the time, many are still reluctant to adopt the cloud computing. Conclusion Although cloud computing has security issues and challenges, the benefits are good and outweigh the setbacks. The fact is that these setbacks or security issues and challenges are also present within the in-house systems. The only problem is that organizations have to share infrastructure, which in fact provides a cost cutting advantage and having to use the services over the internet that poses the security issues. Otherwise, the benefit of cloud computing are worth the risk considering most of the risks are also available within the in-house systems. Additionally, considering it is a new system, cloud providers are most likely to design software that increases security level while improving the reliability and customization as well as interoperability as the new phenomenon continues to evolve. Therefore, the security issues and challenges should not be an excuse for potential clients to refrain from enjoying its benefits.

References AMCHAM. (2012). Cloud Computing: Issues and Challenges. Retrieved from http://www.

ey. com/LU/en/Newsroom/PR-activities/Articles/article_2012_february_cloud-computing Beckham, J. (2011). The Top 5 Security Risks of Cloud Computing. Retrieved from http://blogs.

cisco. com/smallbusiness/the-top-5-security-risks-of-cloud-computing/Carson, L. (2011). The Downtime Dilemma: Reliability in the Cloud. Retrieved from http://blog. softwareadvice. com/articles/crm/reliability-in-the-cloud-1060611/ Knorr, E. & Gruman, G.

(2013). What cloud computing really means. Retrieved from http://www.

infoworld. com/d/cloud-computing/what-cloud-computing-really-means-031 Kuroyo, S. O.

, Ibikunle, F., & Awodele O. (2011). Cloud Computing Security Issues and challenges. International Journal of computer Networks, 3 (5): 247-255. Limoncelli, T., Hogan, C. & Chalup, S.

(2007). The Practice of System and Network Administration. New York, N. Y: Pearson Education. Sabahi F. (2011). Cloud Computing Reliability, Availability and Serviceability (RAS): Issues and Challenges.

International Journal on Advances in ICT for Emerging Regions 2011 04 (02): 12 – 23 Sorrels, J. (2010). Securing the Cloud: Separation and Isolation is Key. Retrieved from http://www. securityweek. com/securing-cloud-separation-and-isolation-key vBox.

(2011). Cloud Computing – Managing risk within the cloud (cont’d). retrieved from http://thevbox. net/2011/06/02/cloud-computing-%E2%80%93-managing-risk-within-the-cloud-cont%E2%80%99d-lockbox/Zissis, D.

& Lekkas D. (2012). Addressing Cloud Computing Issues. Future Generation Computer Systems, 28 (3): 583-592.