Computer Science and Information Technology 2(5): 232-237, 2014
DOI: 10.13189/csit.2014.020502
http://www.hrpub.org

Towards a Good Cloud Computing Provider other than Choosing through Data Security and Privacy Capability Factor

Duncan Waga[1,*], Kefa Rabah[2]

[1]Jaramogi Oginga Odinga University of Science and Technology, Kenya
[2]Kabarak University, Kenya
*Corresponding Author: wagadun@gmail.com

Abstract Cloud computing (CC) is the assumed miracle solution for establishments who are keen on cost effective automation and is brought to a users door step through cloud computer service providers. There are many areas where a user should consider when selecting a vendor for a cloud services solution, from the vendor's infrastructure and computing architecture framework to the jurisdiction within which the solution resides. In as much as its uptake is sky rocketing, there is a major challenge in selecting a provider who fits the bill. Most practitioners falsely believe that as long as a data security and privacy is mitigated then all is well. There are many other factors that users should confirm with the provider of their ability before any contract is signed of which this paper discusses. Issues to do with Intellectual property, jurisdiction, and portability of content are mentioned. Disappointed users with failed projects who end up with court cases are also included in the paper.

Keywords Cloud Computing, Cost Effective Automation, Cloud Providers, Cloud Vendors, Data Security And Privacy, Jurisdiction, Intellectual Property, Portability

1. Introduction

Cloud computing, a new concept in distributed computing after the web2.0 is causing serious ripples in the virtualization arena. New entrants are streaming into it en masse with only one concern of data privacy and security. As long as my data is safe then I don't care about other factors kind of attitude is common with users who are coming in as new entrants. Ion et al argue in their article of **"**Home is safer than the cloud: privacy concerns for consumer cloud storage" stating that Several studies ranked security and privacy to be major areas of concern and impediments of cloud adoption for companies, but none have looked into end-users' attitudes and practices.

This study will discuss many salient factors that cloud users should confirm before settling on particular vendors. Practitioners run a risk of engaging vendors before doing a thorough investigation of their capacity to deliver in line with other factors like intellectual property where client resources cease to be theirs when they cross jurisdictions and where relocation of resources to other platforms cause incompatibilities.

CC and its inter relationships between the geography of cloud computing resources, its users, its providers, and governments (Jaeger et al) is very significant since the basis of resource centralization is in other facets of disparate clusters of data centers across the world with possible loss of control due to policies and legislation.

Jon Brodkin of Network World, Gartner says that customers ask tough questions of the risks associated with their data before they can adopt and they go as far as engaging other neutral firms to help them trust a given provider. This only happens to a few customers who have the awareness else most of them simply look at the data security assurance factor. He goes further to explain that Cloud computing has "unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing. Many vendors are often not in a position to answer client concerns like security and transparency hence should be shunned claims Jon.

Ang Li in his article of comparing cloud providers bases his argument that CC practitioners don't have the capacity to select the best provider and advices usage of his tool, cloud CMP. This tool has the capability of comparing service provider's capacities and suggests the most appropriate one. Such a tool would be very useful since most users don't have much technical knowledge and are only interested in a working cloud. The main objective of this study is to outline the factors which should be considered before a CC provider is selected.

Despite CC being a rather new area with little research

having taken place, there are a number of literatures from manufacturers and academics available. A review of these produced a lot of ideas that made up this paper. This article would go a long way in proving initial authentic knowledge on how to select providers which is important precursor to CC uptake.

2.1. Justification

CC is known to house essential digital resources of users and its security, privacy and location should have some guarantee hence the essentiality to vet providers who are able to effectively deliver CC. The absence of CC vendor federation means there are no proper standards for guidance to new entrants and every vendor runs his business merely to reap maximum profits and not maximum service. Resources are handled differently in various jurisdictions which can also lead to serious repercussions. Cost differences should not be ignored too. Some providers are known to sub contract other vendors to specially manage some of their client's resources without revealing in the SLAs. There are cases where a sub contracted vendor has had issues which necessitated data loss and disputes have ended in courts as shown in this paper.

2.2. Literature Review

Durkee et al argues that today's price-focused cloud-computing market, which is moving rapidly toward perfect competition, presents challenges to the end customer in purchasing services that will meet their needs. This first-generation cloud offering, essentially Cloud 1.0, requires the end customer to understand the trade-offs that the service provider has made in order to offer computing at such a low price. Luqun Li et al (2009) formulated a framework that analyzed the effect of job scheduling and QOS offered to the end users and demonstrated that job scheduling system can not only guarantee the QoS requirements of the users' jobs, but also can make the maximum profits for the cloud computing service providers. Chakraborty et al (2010) worked on Information Assurance practices by cloud providers and showed how it differs based on a cloud vendor's service offering, amount of online traffic, and company size. Mowbray et al (2009) considered the legal aspects of factors affecting cloud computing and also predicted that some disputes will end up in court. Patel et al (2009) emphasized the significance of SLAs to manager consumers and providers of CC and further asserted that continuous monitoring on Quality of service (QOS) attributes is necessary to enforce SLAs. Foley (2008) argues that many policy questions will continue to be issues even after the data center is constructed. The largest challenges to existing providers will likely be tied to issues of security and privacy of the users.

In spite of these issues of law and policy, few attempts have been made to address the thorny legal issues raised by cloud computing (Jaeger, *et al.*, 2008). The failure to create policies that adequately balance the needs of cloud providers, cloud users, and jurisdictions could have sizeable consequences on where the data centers of the future are located. Simply put, without good policy, one jurisdiction — no matter what the other advantages of the location may be — will lose cloud providers and their data centers to other jurisdictions, asserts Jaeger. Of course, the fact that a cloud consists of many data centers in many different jurisdictions, there may be very practical limits on jurisdiction shopping. Perhaps the most intriguing unanswered policy questions about cloud computing is whether a cloud will be considered to legally be in one designated location (and therefore beholden to the laws, policies, and regulations of one place) or in every location that has a data center that is part of the cloud.

Jurisdiction shopping and the provision of incentives to locate in certain jurisdictions raise several major concerns for users of cloud computing. For example, if certain jurisdictions are too eager for the economic benefits of data centers, they may give away too many legal protections of users and content, granting a great deal of control to the providers. Conversely, providers may be wooed by economic incentives from jurisdictions that have a negative legal environment in terms of data and user protection, giving the government a great deal of power over the provider, users, and content. Even when providers suggest unique responses to such jurisdictional concerns, there are still major potential problems. Though it is being presented as a solution to issues of energy and environmental conservation, the Google Navy can also been seen as a response to these complex jurisdictional issues. At the most basic level, data centers on ships in international waters would not have to pay property taxes. More significantly, it also raises major questions about the legal jurisdiction of such seafaring data centers. Could a National Security Letter be enforced against a server in a boat in the middle of the Pacific Ocean? The Google Navy may indicate that existing jurisdictional issues are so unappealing to cloud providers that they are looking to the sea for relief.

Table 1 outlines the different cloud types found in the cloud market and their respective applications.

As such, individual and corporate user rights and protections, provider interests, and government duties must be extremely carefully considered and balanced as cloud computing edges closer to ubiquity. While jurisdictional concerns will not likely lead to a mass discontinuation of use of cloud services, the way data centers are established under law in the near future will have long–term ramifications for users, providers, and governments, as well as for the control of the Internet itself. As per the scope of this paper, it is clear that there are many factors affecting the smooth operation of CC and users must be aware.

Table 1. Cloud cateories

DEPLOYEMENT MODELS	DESCRIPTION	EXAMPLES
PUBLIC	Public clouds are not restricted to any particular customers or organizations. They provide services to the public all over the world without any limitations. But they are not as secure as private clouds.	• Amazon Elastic , • Google App Engine, • Blue Cloud by IBM and • Azure services Platform by Windows
PRIVATE	Private clouds provide services to the customers of the particular organizations for the sake of security and confidentiality of their personal data. The fact is that whether these private clouds are owned and controlled by customers but they are built and installed by the third parties.	• VMware • Microsoft • Amazon EC2 • Eucalyptus
HYBRID	Hybrid clouds are the combination of both public and private clouds. The organizations and other people can take benefits of both public and private cloud by using hybrid clouds. Like some of the companies set their own private clouds and they take services from it but if they need some services from public cloud also then this facility comes under hybrid clouds only.	• CTERA • Red hat open hybrid cloud

Table 2. Cloud types

MODELS	SERVICES AVAILABLE	USED BY	WHY USE IT	EXAMPLES
SAAS	Email, office automation, website testing, wiki, virtual desktop blog, CRM	Business users	To complete business tacks	Salesforce.com, Animoto, Oracle on demand, Windows Office Live
PAAS	Service, application tests, development, integration and deployment	Developers and deployers	Create or deploy applications and services for users	Google Application Engine, Microsoft Azure, Coghead, Force.com, Yahoo Developer Network
IAAS	Create platforms for services and application test, development integration and deployment	System manager	Create platform for service and application test, development integration and deployment	Amazon EC2, Simple Storage Service(S3), Gogrid

3. Methodology

A lot of literature searches were conducted and many articles cited in the reference were considered and their themes comparatively analyzed in the discussion section of this paper. We also did a lot of talking to people, focus groups, personal interviews, telephone surveys, mail surveys, email surveys, and internet surveys. A few of the articles are mentioned above.

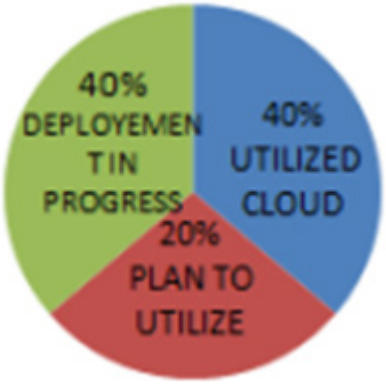

Figure 2. Cloud distribution

4. General Regulations

The other major set of factors affecting the location of cloud computing data centers revolve around jurisdictional issues. The laws, policies, and regulations of a particular jurisdiction can have a significant impact on the cloud provider and the cloud user. Governments through law, policy, and regulation can either stifle or promote the development of cloud computing within a particular jurisdiction. There are many law and policy problems raised by cloud computing that could become problematic for cloud providers and cloud users (Jaeger, *et al.*, 2008). For users, these issues and expectations include:

Access

Users will expect to be able to access and use the cloud where and when they wish without hindrance from the cloud provider or third parties.

Reliability

Users will expect the cloud to be a reliable resource, especially if a cloud provider takes over the task of running "mission–critical" applications (Jaeger, *et al.*, 2008; Armbrust, *et al.*, 2009).

Security

Users will expect that the cloud provider will prevent unauthorized access to both data and code, and that sensitive data will remain secure (Jaeger, *et al.*, 2008).

Data confidentiality and privacy

Users will expect that the cloud provider, other third parties, and governments will not monitor their activities, except when cloud providers selectively monitor usage for quality control purposes (Armbrust, *et al.*, 2009).

Liability

Users will expect clear delineation of liability if serious problems occur.

Intellectual property

Users and third party content providers will expect that their intellectual property rights will be upheld (Jaeger, *et al.*, 2008).

Ownership of data

Users will expect to be able to regulate and control the information that is created and modified using those services (Jaeger, *et al.*, 2008; Armbrust, *et al.*, 2009).

Fungibility

Users will expect that data and resources stored in one aspect of the cloud can be easily moved or transferred to another similar service with little or no effort, *i.e.*, a high expectation of data portability.

Auditability

Users, particularly corporate, will expect that providers will comply with regulations or at least be able to provide them the ability to be audited per regulation requirements (Armbrust, *et al.*, 2009). The failure to address these issues can cause resistance to a service among users. Lingering mistrust and fear of governmental snooping is already having a negative backlash on certain Google services that sort vast amounts of user information (Avery, 2008). And while all of these issues clearly are also of concern to cloud providers, they will also evaluate a jurisdiction based on factors such as:

Legal jurisdiction

In cases involving the cloud provider, where will the cases be adjudicated? How favorable is that jurisdiction to the cloud provider's interests?

Government intervention

How intrusive can the government be under the law or under accepted local practices?

Costs of doing business

How high is the financial burden of taxes, insurance, and regulations (safety, environmental, industrial, etc.)? Is there sufficient work force available? How favorable is the business climate? Goiri et al in his article of Characterizing Cloud Federation for Enhancing Providers' Profit argues that customers who are turned away from some providers due to their limitations may benefit immensely if cloud providers formed a federation such that they run a common platform which can be borrowed at will depending on the clients wish. This is so true since it will provide a one stop CC solution provider. Gartner of Network world discusses other issues that must be cleared before adoption like qualifications of policy makers, architects, coders and operators; risk-control processes and technical mechanisms- and the level of testing that's been done to verify that service and control processes are functioning as intended, and that vendors can identify unanticipated vulnerabilities.

5. Client to Vendor Questions

Regulatory compliance

Usually it is normal that Service providers go through external audit processes as a government based regulation mechanism. CC providers are no exception else they lose the public entrustment.

Data location

Cloud computing exhibits location transparency and clients seldom realize the particular locations where their resources reside. A provider must contractually agree to ensure clients resources in various jurisdictions are secure and still meet the contractual agreements they make with their clients.

Data segregation

Resources in the cloud in the same platform should not mix with other customers'. Vendors must convince clients of effective technologies like encryption that separates data from other peoples resources and must also own up to accidents caused by these technologies.

Recovery

Due to the disparity of locations of data storage in CC chances of system disruptions and possible loss are higher. Providers who don't have a multi site replication capacity and fast, effective complete restoration is not worth going for.

Investigative support

Launching of investigations in a CC environment is usually a nightmare on due to the changing set of hosts and data centers. Good vendors are those willing to have contractual commitment to support investigations and evidence of their experience in that line.

Long-term viability

In cases where providers close shop or cease operations are there arrangements to ensure clients data retrieval and access is facilitated. In individual jurisdictions, the approaches to cloud policy will vary greatly, depending on the priorities of the location. Some jurisdictions have recently created or expanded tax breaks to encourage the construction of data centers — one of the key reasons many data centers are being constructed in Iowa is the hefty tax breaks given to data centers (Foley, 2008). On a larger scale, entire nations may provide tax breaks to companies like IBM and Google to provide incentive for construction of data centers outside the United States. Jurisdictions, however, must weigh the advantages of having data centers with the sizeable environmental impacts. Figure 4 indicates the status at which cloud computing is at in the market

6. Litigation on Breeches

Cases relevant to cloud computing arise in a variety of areas of law, as cloud computing is a type of business activity distinct from a unique legal area. Like any area of business activity, particularly those involving computers and digital distribution, cloud-computing-related transactions have and will generate a variety of potential cases (Mark H. Wittow). There are numerous cases of litigation as mentioned below:

The St. Louis-based grocery chain Schnuck Markets has claimed that a potential class action lawsuit filed against it in an Illinois state court over a recent data breach really belongs in federal court because of the case's scope and damages involved. In a motion for removal filed earlier this month, Schnucks noted that the damages claimed by the plaintiff in the case easily exceeded the $5 million threshold for a federal case. The number of people that are alleged to have suffered financial injury from the breach and the fact that they are from multiple states also make the case a federal one, the company alleged in its motion.

Cartoon Network v. CSC Holdings, also known as the Cablevision case, addressed cloud-based digital television services, specifically whether a television cable service's operation of a remote storage digital video recorder (RS-DVR) system and the related serving of content constituted copyright infringement.

In Arista Records, LLC v. Usenet.com, Inc., 7 the District Court for the Southern District of New York granted summary judgment to plaintiff record companies 8 on claims for (1) direct copyright infringement of the exclusive right of distribution under 17 U.S.C. § 106(3); (2) inducement of infringement; (3) contributory infringement; and (4) vicarious infringement by Usenet.com, Inc. (UCI). UCI created an online bulletin board system on which subscribers posted files and downloaded files posted by others for storage on their personal computers. While technically different in format conversions, UCI's service created an experience like peer-to-peer file-sharing networks, including Napster. UCI offered access to its service based on monthly fees and agreement to UCI's terms of use (TOU). One TOU prohibited the unauthorized upload of copyrighted content. The record companies objected to UCI's activities as the unauthorized distribution of copyrighted works.

7. Discussion

Durkee et al (2009) in his article, didn't talk about Information assurance(IA) i.e The aspect of IA that assures that no one other than those specifically authorized have access to the data, and that the data (not just the service) will be available when needed. The data must also be transportable between cloud providers, which offer an added level of IA. When a company is evaluating "moving to the cloud", this is often overlooked. These factors are mentioned elsewhere in this paper. Luqun Li et al (2009) referred to job scheduling to be directly related to QOS to the end users. However factors such as user etiquettes can also affect QOS even if the provider has perfect job scheduling systems. Mowbray et al (2009) predictions have come to pass that some disputes will end up in court as mentioned somewhere in this paper. Patel et al (2009) didn't mention other major factors that go hand in hand with SLAs like jurisdiction as challenges affecting ranking of providers.

A number of attempts are already being made to avoid the reach of such laws. The Canadian government has a policy forbidding public–sector IT projects from using U.S.–based

hosting services to avoid U.S. laws like the USA PATRIOT Act (Thompson, 2008). Further, neutral countries are being viewed as ideal locations for data centers by some companies in order to prevent the data from being reachable by the United States government (*Economist*, 2008a). For example, SWIFT, an international banking organization, is looking to be a data center in Switzerland for this very reason (*Economist*, 2008c). However, these types of approaches are of limited benefit in attempting to avoid law enforcements entanglements. The laws of any nation where a data center is located will apply, and many nations do not have nearly the civil rights safeguards that the United States does (Thompson, 2008). Placing data centers in other countries may ultimately result in more legal complications for providers and users.

In spite of these issues of law and policy, few attempts have been made to address the thorny legal issues raised by cloud computing (Jaeger, *et al.*, 2008). The failure to create policies that adequately balance the needs of cloud providers, cloud users, and jurisdictions could have sizeable consequences on where the data centers of the future are located. Simply put, without good policy, one jurisdiction — no matter what the other advantages of the location may be — will lose cloud providers and their data centers to other jurisdictions. Of course, the fact that a cloud consists of many data centers in many different jurisdictions, there may be very practical limits on jurisdiction shopping. Perhaps the most intriguing unanswered policy questions about cloud computing is whether a cloud will be considered to legally be in one designated location (and therefore beholden to the laws, policies, and regulations of one place) or in every location that has a data center that is part of the cloud.

Jurisdictions may be eager to get more financial benefits hence institute many protections of users and content, hence much control to the providers as opposed to providers being attracted by areas that have negative legal environment in terms of data and user protection, giving the government a great deal of power over the provider, users, and content. Even when providers suggest unique responses to such jurisdictional concerns, there are still major potential problems.

Google Navy though a plus towards environmental conservation can also been seen as a response to these complex jurisdictional issues. Datacenters in the ships pose challenging jurisdictional and security provider concerns. Providers would wish to find a regulation less jurisdiction to operate, whether it is possible remains imaginative.

8. Conclusions

The above cases of CC projects that failed and possibly ended as courts cases for arbitration was mainly due to entrant's non consideration of most of the factors providers should mitigate before engagements. Jaeger et all supports this idea in terms of different jurisdictions considering contracts differently. Zhang et all reiterates in his paper of Realization of open cloud computing federation based on mobile agent that only the application of a mobile federation that is not answerable to rigid local jurisdictions is the solution to this problem. Amazon and Google are already championing tax rebates to clouds which are able to meet all the demands. We can therefore state that before engaging a cloud provider; confirm their stand as regards information assurance and jurisdiction challenges. As more vendors emerge with more complex technologies new challenges follow suit hence more of a continuous research is needed in this area.

REFERENCES

[1] http://www.computerworld.com/s/article/9239534/Schnucks_wants_federal_court_to_handle_data_breach_lawsuit JULY 02, 2008 Gartner: Seven cloud-computing security risks

[2] Cloud computing is picking up traction with businesses, but before you jump into the cloud, you should know the unique security risks it entails By Jon Brodkin | Network World

[3] Characterizing Cloud Federation for Enhancing Providers' Profit by Goiri et al

[4] The computer and internet lawyer, aspen publishers volume 28 January 2011

[5] Home is safer than the cloud!: privacy concerns for consumer cloud storage Ion et al

[6] Realization of open cloud computing federation based on mobile agent zhang et all

[7] http://www.mimecast.com/Documents/Whitepapers/WP_Osborne-Clark_Cloud-computing-vendor-selection.pdf

[8] Why Cloud Computing Will Never Be Free by Dave Durkee, ENKI

[9] An Optimistic Differentiated Service Job Scheduling System for Cloud Computing Service Users and Providers by Luqun Li

[10] The Information Assurance Practices of Cloud Computing Vendors Chakraborty, et al (2010)

[11] The Fog over the Grimpen Mire: Cloud Computing and the Law Mowbray et al(2009)

[12] Service Level Agreement in Cloud Computing patel et al (2009)

[13] Cloud Computing Services – A comparison BY Torris Harris

[14] Legal and Quasi-Legal Issues in Cloud Computing Contracts *By Steve McDonald, General Counsel, Rhode Island School of Design*

[15] Data Protection Jurisdiction and Cloud Computing Queen Mary University of London, School of Law Legal Studies Research Paper No 84/2011

[16] Kimmy Department of Computer Science and Engineering CT Institute Of Engg. & Technology Jalandhar, Punjab, India kim_00b4178@yahoo.com