

LAW 447B TERM PAPER

Cloud Computing: Facts, Security & Legal Challenges

MINAMUR CHOWDHURY

Student # 67709055

Instructor: Professor Mark Yang

University of British Columbia

December 18, 2009

CONTENT

CHAPTER – 1: CLOUD COMPUTING - FACTS

INTRODUCTION	3
HISTORY	4
AN EMERGING BUSINESS MODEL	5
The Economics of Cloud Computing		
Platform as a Service (PaaS)		
Software as a Service (AaaS)		
Benefits		

CHAPTER – 2: CLOUD COMPUTING - LEGAL FACTS, CHALLENGES AND A POSSIBLE SOLUTION

SECURITY CHALLENGES	11
LEGAL CHALLENGES	14
Protection of Privacy		
Enforcement of Intellectual Property Rights		
Jurisdiction		
Service Level Agreements		
RECOMMENDATIONS AND A POSSIBLE SOLUTION	16
Overview - Addressing the Security Needs		
Overview - Addressing the Legal Needs		
A Possible Solution for Service Level Agreements		
CONCLUSION	21
BIBLIOGRAPHY	22

CHAPTER - 1

CLOUD COMPUTING - FACTS

INTRODUCTION

The Cloud is a metaphor for the Internet network diagram. Cloud computing is not a new technology but a new concept that encapsulates a platform of applications. The concept runs on the Internet thereby providing applications to end users without the need of physically installing software or implementing complex infrastructure. Cloud computing can be divided into several categories: Infrastructure as a Service, Platform as a Service, and Software as a Service. Cloud computing services are emerging technologies that provide both businesses and individuals many benefits such as lowered costs and ease of accessibility but have also come with issues such as legal and security risks. Despite that, analysts say Cloud computing represents a sea change in the way computing is done in corporations. Merrill Lynch (banking and wealth management division of Bank of America) estimates that within the next five years, the annual global market for Cloud computing will surge to \$95 billion. In a May 2008 report, Merrill Lynch estimated that 12% of the worldwide software market would go to the Cloud in that period. Those vendors that can adjust their product lines to meet the needs of large Cloud computing providers stand to profit.

HISTORY

The name Cloud computing was inspired by the Cloud symbol that's often used to represent the Internet in flow charts and diagrams. The underlying concept of Cloud computing dates back to 1960 when John McCarthy (an American computer scientist) opined that, "computation may someday be organized as a public utility." In 1997, the first academic definition was provided by Ramnath K. Chellappa who called it *a computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits*. In 1999, Salesforce.com applied many technologies developed by companies such as Google and Yahoo! to its own business applications. In the early 2000s, Microsoft extended the concept of SaaS through the development of web services. IBM detailed these concepts in 2001 in the Autonomic Computing Manifesto. Amazon played a key role in the development of Cloud computing by modernizing their data centers after the dot-com bubble. They started providing access to their systems through Amazon Web Services on a utility computing basis in 2005. In 2007, Google, IBM, and a number of universities embarked on a large-scale Cloud computing research project. And, by mid-2008, Gartner Inc, the world's leading IT research & advisory company saw an opportunity for Cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them."

AN EMERGING BUSINESS MODEL

There is a high flexibility that comes with implementing infrastructure as a service. A company can increase or decrease how much space it rents on the Cloud as its utilization pattern varies. During peak periods, such as release dates, the companies can rent more bandwidth to accommodate the demand and then lower it during the low usage periods. Finally, the implementation of IaaS gives companies access to enormous computational power. The latest data center built by IBM is the size of 11 football field! Clients are granted access to all the computational power available inside the data center.

The Economics of Cloud Computing

Recent studies conducted by IBM shows, only 3% of energy consumed by a data center is used for computation; therefore IBM has implemented energy efficient policies to successfully apply the economies of scale principle to increase server utilization and decrease energy costs by up to 40%. This is increasingly important as the energy costs continue to rise and hardware costs drop. Finally, moving the infrastructure to the Cloud allows companies to drastically downsize their IT departments and focus their resources on running their core business.

Platform as a Service (PaaS)

Platform as a Service offers users the ability to go through the entire lifecycle of building an application on the Cloud. This means individuals can design, develop, test, deploy and support custom applications whenever and wherever they want. Companies nowadays are reluctant to spend enormous amounts of money on technology, especially if it is not their core

business. Many employees are also unfamiliar with programming so a dedicated IT team is needed whenever custom applications are to be created or else the job is outsourced to another company. Platform as a service allows for simple application creation that minimizes costs and decreases the need to depend on other companies.

Platform as a Service can be very beneficial to a business. One of the benefits of PaaS is that helps business users minimize operational costs. PaaS follows the pay-as-you-go model of software, as service so there is no need for large up-front investment since companies only pay for what they need. It allows for a centralized information management so there is access to the information anywhere, anytime through the Internet. Teams consisting of members from around the world can work together on software development projects as everything is done on the web. Productivity is increased because of these factors. PaaS is being offered by both the software giants such as Google and Microsoft and also by companies dedicated to Cloud computing services. Some such companies include Force.com, Bungee, and Rollbase. Rollbase is an example of a platform as a service company developed specifically for business users. The platform allows business users to create sophisticated applications in a short period of time. The online platform allows for a point and click, drag and drop type programming that almost anyone can understand to build and deliver custom web-based business applications. Businesses no longer need to employ large IT departments to create complicated programs. People who are not trained can easily create applications online in an Internet browser in traditional programming methods.

Software as a Service (AaaS)

Software as a service is a model of software deployment whereby a provider licenses an application to customers for use as a service on demand. The services are provided through the internet where as the actual data and IT infrastructure resides with a host. Some examples of companies offering SaaS are Salesforce, IBM and SAP. Software as a service encompasses all business applications delivered as an on-demand service via a secure internet connection and a web browser.

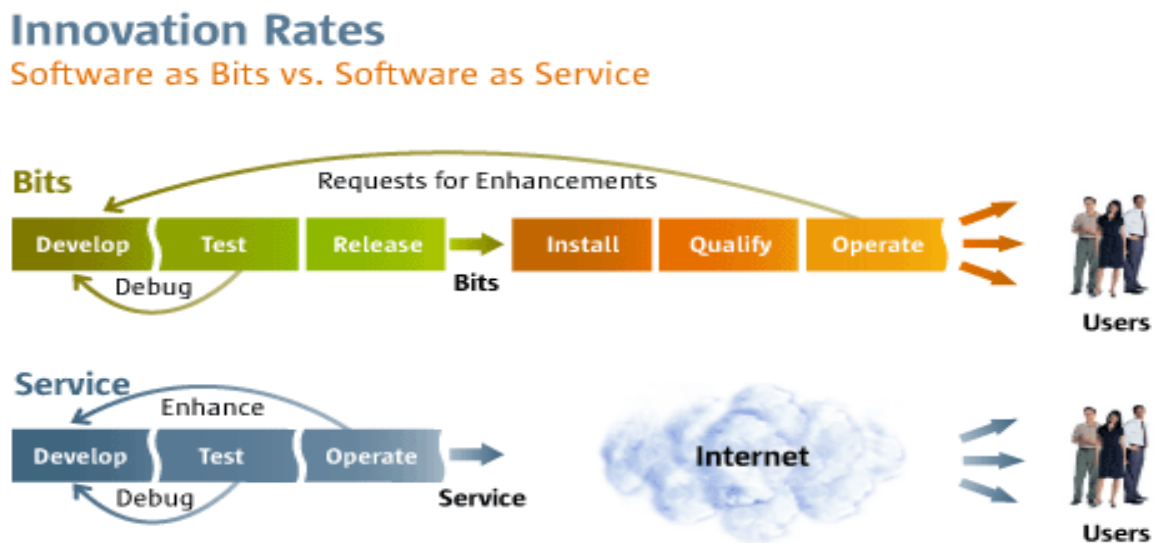


Figure – Innovation Rates: Software as Bits vs. Software as Service

Benefits

Benefits of software as a service include flexibility, cost reduction, integration and accessibility. Since all applications are web-based, information of a user's choice may be accessed anytime, anywhere in the world with a simple connection to the network. For example,

Google services such as Gmail and Google Docs are accessible on any Internet browser. Since everything is integrated and centralized, there is greater accessibility to the data. When a user inputs data into an application, this information is processed and saved directly onto the Cloud. This information can then be retrieved through different means as long as there is proper authorization. In other words, a user has the flexibility to choose where and when he or she wants to access the data again. The data can also be easily shared with others as through proper authorization assignments.

Another benefit of software as a service is that a business no longer has to worry about upgrades. Traditionally, software goes through planning, development, testing and then is released to the public, but with Cloud computing technology, upgrades and enhancements are done in the Cloud by the service providers. This allows for flexibility in developing business applications without the hassle. Since the software is in the Cloud, service providers can upgrade the software in the Cloud and end users can benefit from it with immediate effect, thus, saving time and money.

The major competitive advantage of software as a service application such as Google Docs is cost reduction. Most SaaS solutions have a pay-as-you-go pricing model instead of a large up-front investment. Such pricing models allow end users to pay only for what they use thus freeing up resources such as time and money for other more important (core) business activities. For example, Salesforce charges anywhere from US\$5 to US\$250 per month per user for its services. Implementation of Cloud computing will reduce the investment cost in server hardware and software licensing. This then frees resources that can be used elsewhere in the firm. It is also a low cost method for businesses to acquire rights to use software as needed versus mass licensing of all applications, which can be very costly.

According to [Forrester Research](#), the notable benefits of Cloud Computing are:

1. Improving time-to-application deployment. Cloud platforms give clients the option of developing and deploying new applications on existing infrastructure as quickly as desired. Traditional platforms can take up to three or four months to procure, install, and configure, stalling the application deployment process.
2. Aligning IT budgets with application demand. How many Web applications does an organization deploy without exactly knowing how popular they'll be or how much capacity you'll need to accommodate that popularity? Many of the early Cloud adopters host customer- and public-facing Web applications with Cloud providers for this reason. They can pay just for the resources they use, hour by hour.
3. Providing a 'safety valve' for peaks in demand for data centre capacity. Cloud computing is also good for handling episodic spikes in demand for computing, storage, and network resources. Rather than provision for the expected peak of the holiday shopping season, retailers can push the additional demand into a Cloud environment. Big batch jobs also fit this model.
4. Delivering applications without raising budget. Cloud computing gives clients the ability to deliver new applications without having to buy gear, curbing the firm's capital expenditures. Application development and delivery can all be handled using operating expenses only.
5. Sharing without putting the data centre at risk. Many of the early adopters of Cloud computing are looking for an inexpensive and easily accessible way to share information. Medical researchers are an example. Cloud lets these organizations host data on public Clouds rather than having to punch new holes in their organization's firewall to make it available to external parties.

CHAPTER - 2

CLOUD COMPUTING - LEGAL FACTS, CHALLENGES AND A POSSIBLE SOLUTION

The Cloud spans many borders and "may be the ultimate form of globalization." As a result, it becomes subject to complex geopolitical issues and providers are pressed to satisfy countless regulatory environments in order to deliver service to a global market. Concerns arise about security and privacy from individual through governmental levels (e.g., the USA PATRIOT Act, the use of national security letters, and the Electronic Communications Privacy Act's Stored Communications Act).

The major public Cloud providers keep performance assurances and warranties to a minimum and essentially offer their products only on an "as is" basis drawn from the consumer services where they started. Many also retain the right to suspend their services at any time in the event of any unanticipated downtime or unavailability. Even where a breach occurs most public Cloud providers require broad exclusions of liability. There is a major disconnect between the confident claims of availability and resilience which Cloud providers make for their services and their hesitance to accept risk.

Additionally, many Cloud providers seek indemnities against any claim which is made against them as a result of any information, data or electronic material that a customer places into its Cloud which causes it to breach a third party's intellectual property rights. Some other common indemnities include those protecting suppliers against losses suffered from a customer breach of the services agreement or failures to secure their passwords or permitting unauthorized

access to the service. As Cloud computing, by its design, transcends national borders, it complicates compliance with the various flavors of data protection legislation and ensuring the security of the data that is placed in the Cloud.

In Europe, data protection law requires that the party which decides the purposes for which any personal data is held or processed and the manner in which it is held or processed (the "data controller") has sole responsibility for safeguarding the data. The UK Data Protection Act 1998 includes obligations on data controllers to include certain specific provisions in written contracts with data processors. The law requires data controllers to ensure that personal data is processed with "appropriate technical and organizational measures" in place to prevent unauthorized or unlawful processing or accidental loss, destruction or damage. The standard approach in many Cloud providers' terms of service is to exclude liability for security of any data and provide that the customer retains full responsibility for data safety, contrary to the principles of the UK legislation. However, perhaps more significantly, the resources used in the Cloud may be located in unknown (and unknowable) jurisdictions, so compliance cannot be assessed by the user.

SECURITY CHALLENGES

Security, which is an important issue to businesses, is also a large aspect of IaaS. In a study performed by IBM, 33% of companies responded that they would leave and terminate their relationship if they were notified that a security breach had occurred. Understandably, large companies such as IBM invest heavily in guarding their data centers against breaches. Data centers are heavily guarded by security staff to prevent physical attacks and also by sophisticated

security software to prevent malicious hacker attacks. IaaS providers offer fine grain access to files; therefore customers can grant file access rights to only authorized individuals.

Loss of control over sensitive data being processed outside the enterprise brings with it an inherent level of risk because outsourced services bypass a company's physical, logical and personnel controls. Another risk is the lack of security standardization that applies for IT security and compliance that govern most business interactions. Unknown data location is yet another risk as Cloud providers may choose to store and process data in a location that is unfamiliar or is in an unfriendly jurisdiction. This may make it difficult to investigate if there are inappropriate or illegal activities involving user data. Risks also may include perils related to availability, long-term viability, data integrity and proper Failover technology. In Summary, first and foremost risk is the threat to the data privacy. Interestingly most risks are somewhat associated with this data privacy issue. Details of possible problems involving Cloud Computing is discussed below (based on [Forrester Research](#)).

1. Multi-tenancy may clash with security, privacy, and compliance requirements

Services that employ multi-tenant architectures are the most cost-efficient Cloud services. In these products, the data and processes of many clients run side by side, so to speak, raising obvious concerns about data protection and privacy, as well as process compliance. Vendors handle these risks in different ways, none of which are yet well understood.

2. Subscriber fee economics may not produce cost savings

Does Cloud computing save money? The answer depends on what consumers use Cloud computing for and the alternatives compare it with. Eliminating the need to buy, configure, and

manage a lot of hardware for each major new application certainly can produce cost savings. But those savings may be surpassed by the cost of the Cloud provider's subscription fees.

Furthermore, a company may not see dramatic decrease on software license costs. When it comes to saving labor costs, the economics of Cloud computing works favorably only by modeling specific scenarios in details.

3. Vendor lock-ins

There are no Cloud computing standards to promote data and code portability.

Infrastructure-as-a-service providers like Amazon have low lock-in, but platform and application providers like Salesforce.com have high lock-in. In these environments, you can get your data out to run somewhere else, but your code will run in only one place – the vendor's environment. For interoperability, the Web Services Standards apply, but many rely on the less standard Representational State Transfer (REST) pattern.

4. Reliability and control may be reduced

When a client signs up with a Cloud provider, in effect the client delegates responsibility for a portion of his application's reliability to that vendor. In most cases, the client will have a very limited amount of control over the systems factors that influence that vendor's reliability.

5. Integration of Cloud apps will also be difficult and expensive

Applications running on Cloud platforms will not be self-contained forever. Cloud applications will face many of the same requirements for integration with other applications, user interfaces, services, and databases as conventional applications. Application integration is

expensive, period. The additional security and reliability risks posed by Cloud platforms will add to the potential expense of application integration.

6. Application pattern, model, and framework options will be limited

Lastly, if Cloud computing economies of scale are based on standardized workloads, it follows that you'll find limits on the custom applications you can build and deploy on Cloud computing platforms. The risk is that you'll invest in skills but find yourself achieving only a limited payoff from your investment.

LEGAL CHALLENGES

Protection of Privacy

There have been concerns as to whether personal information about Canadians stored outside Canada may be accessed by law enforcement bodies, particularly under anti-terrorism legislation such as the USA PATRIOT Act. Cloud users' data is not stored on their own servers, but rather is accessed through the Internet from devices such as laptops or mobile phones. Surveys find that 90% of Clouds computing users say that they would be very concerned if the company at which their data were stored sold it to another party. 80% say they would be very concerned if companies used their photos in marketing campaigns. 68% of users say they would be very concerned if companies who provided Cloud computing services analyzed their information in order to display relevant ads.

Another concern in this area is that a user is no longer in control of his or her personal information, an aspect that breaks the concept of "informational self-determination," an

internationally accepted privacy principle that forms the basis of data protection laws worldwide. This raises questions such as: Who owns and controls data in Cloud? Is it or should it be a shared responsibility? Who should be accountable or liable in case of misuse?

Enforcement of Intellectual Property Rights

This gives rise to concerns regarding whether rights holders will be in a position to enforce their intellectual property rights when computing resources are used for the unauthorized distribution of video, music or other content. With regards to the issue of cross-border transfers of data, no clear policies are in place to enforce laws to safeguard IP rights or protect confidentiality of users' personal information. Cloud computing complicates pinpointing the location of the infringing activity; therefore it is difficult to determine and enforce existing laws. There are a lack of effective policies at the international and national levels that provide legal certainty to Cloud computing companies and their users.

Jurisdiction

There is the broader issue regarding which courts have the jurisdiction to deal with any wrongful activity such as the posting of defamatory content on storage devices located in one jurisdiction, whereas the affected parties are located in another jurisdiction. Jurisdiction varies from one country to another and its scope relies upon the traditional legal system and its approach by the local courts and tribunals. With Cloud computing, many new questions appear. One such question may be: "What laws should apply and which authorities and courts are legalized to launch an investigation, prosecute the crime and perpetrators?"

Service Level Agreements

Service Level Agreement (SLA) is one of the major issue among other risks associated with Cloud computing. As businesses rapidly move toward SaaS and start to manage the hosting of their systems on the Cloud, a generation of new service providers and products is entering the IT industry. Cloud service providers and customers need to agree on contractual service levels, such as the quality of service, content, functionality and service guarantees. They also need to agree on what is covered and provided in a terms service level agreement. How the services are measured and reported and how often there are back ups are also something that needs to be discussed and agreed upon. As more and more companies are looking to use the general Internet, where once they would have used a private WAN. One of the primary issues is the bandwidth. While, in some cases, bandwidth availability and price is an issue; in others, the quality of the available bandwidth could major issue.

RECOMMENDATIONS AND A POSSIBLE SOLUTION

Overview - Addressing the Security Needs

Security setups in Cloud computing are similar to the security setups in traditional IT environment. However, the business models, the operational models, and the technologies used to enable Cloud services, Cloud computing present different kind of risks (especially involving legal issues) to an organization than traditional IT solutions. In effect, Cloud computing is about losing control while maintaining accountability even if the Cloud responsibilities falls upon one or more out sourced parties. Basically, controls are implemented at the people and process levels, such as separation of duties and change management, respectively. In short, the Cloud business models are expected to be in context with their relevant security controls and legal concerns. A set of

Security Guidance is outlined in Cloud Computing V2.1 (2009), prepared by the Cloud Security Alliance indicates that in order to address the possible Cloud computing risks, users must depend on four major issues, they are: (a.) types of assets, resources, and information being managed, (b.) who manages them and how, (c.) which controls are selected and how they are integrated and (d.) compliance issues.

Furthermore, organizations and individuals intending to deal with Cloud computing must avoid the following potential loopholes:

1. The notion of how Cloud services are deployed is often used interchangeably with where they are provided, which can lead to confusion. For example, public or private Clouds may be described as external or internal Clouds, which may or may not be accurate in all situations.
2. The manner in which Cloud services are consumed is often described relative to the location of an organization's management or security perimeter (usually defined by the presence of a firewall). While it is important to understand where security boundaries lie in terms of Cloud computing, the notion of a well-demarcated perimeter is an anachronistic concept.
3. The re-perimeterization and the erosion of trust boundaries already happening in the enterprise is amplified and accelerated by Cloud computing. Ubiquitous connectivity, the amorphous nature of information interchange, and the ineffectiveness of traditional static security controls which cannot deal with the dynamic nature of Cloud services, all require new thinking with regard to Cloud computing. The Jericho Forum has produced a considerable amount of material on the re-perimeterization of enterprise networks, including many case studies. The deployment and consumption modalities of Cloud should be thought of not only within the context of 'internal' vs. 'external' as they relate to the physical location of assets, resources, and information; but also by whom they are being consumed by; and who is responsible for their governance, security, and compliance with policies and standards.

Overview - Addressing the Legal Needs

Cloud Computing creates new challenges in understanding how laws apply to a wide variety of information management scenarios. As discussed earlier in this paper, when dealing with legal issues involving Cloud Computing requires consideration of functional, jurisdictional, and contractual dimensions. The functional dimension involves determining which functions and services in Cloud Computing have legal implications for participants and stakeholders. The jurisdictional dimension involves the way in which governments administer laws and regulations impacting Cloud Computing services, the stakeholders, and the data assets involved. The contractual dimension involves the contract structures, terms and conditions, and enforcement mechanisms through which stakeholders in Cloud Computing environments must address and manage the legal and security issues. The following recommendations are advised:

- Customers and Cloud providers must have a mutual understanding of each other's roles and responsibilities related to electronic disclosures, such activities as litigation hold, discovery searches, who provides expert testimony, etc.
- Cloud providers are advised to assure their information security systems are responsive to customer requirements to preserve data as authentic and reliable, including both primary and secondary information such as metadata and log files.
- Data in the custody of Cloud service providers must receive equivalent guardianship as in the hands of their original owner or custodian.
- Plan for both expected and unexpected termination of the relationship in the contract negotiations, and for an orderly return or secure disposal of assets.

- Pre-contract due diligence, contract term negotiation, post-contract monitoring, and contract termination, and the transition of data custodianship are components of the duty of care required of a Cloud services client.
- Knowing where the Cloud service provider will host the data is a prerequisite to implementing the required measures to ensure compliance with local laws that restrict the cross-border flow of data.
- As the custodian of the personal data of its employees or clients, and of the company's other intellectual property assets, a company that uses Cloud Computing services should ensure that it retains ownership of its data in its original and authenticable format.
- Numerous security issues, such as suspected data breaches, must be addressed in specific provisions of the service agreement that clarify the respective commitments of the Cloud service provider and the client.
- The Cloud service provider and the client should have a unified process for responding to subpoenas, service of process, and other legal requests.
- The Cloud services agreement must allow the Cloud services client or designated third party to monitor the service provider's performance and test for vulnerabilities in the system.
- The parties to a Cloud services agreement should ensure that the agreement anticipates problems relating to recovery of the client's data after their contractual relationship terminates.

(Source: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009)

A Possible Solution for Service Level Agreements

It is obvious that business enterprises need trustworthy Service Level Agreements (SLA) in order to address any legal challenges arises out of the SLA legal loopholes. Businesses today need sufficient assurance and confidence to qualify and engage with all service providers in ways that are in alignment with organizational risk tolerances. They will need the flexibility to use Cloud services for business needs of varying levels of legal challenges. Therefore, it is essential for businesses to seek for “Cloud Legal and Security Protection Agencies” that would be specializing in “**Cloud Service Risk Management Mechanisms**” in case of potential legal issues and provide services as third parties or act as Outsourced SLA Risk Management Team in order to shift the consequence of service related risks with full ownerships. These risk management agencies could be commercial entities in nature. These agencies could be beneficial to various insurance companies and they could form business relationships to help assure users that the adoption of Cloud computing provides best practices without impeding the business operations. The (proposed) SLA Risk Management companies may also be extend or engaged themselves in several other key Cloud issues as a value added services, such as governance, other law related challenges such as IP implementations, conflicts involving multiple jurisdictions, issues related to protection of privacy, network security, audit, application security, storage, cryptography, virtualization. This approach makes way for a robust authoritative mechanism in order to take ownerships of potential legal challenges and security risks for both parties, the Cloud providers as well as Cloud users. However, Cloud users are the one who may find themselves fallen into a Cloud trap and feel vulnerable when they face legal challenges arising from the Cloud services and therefore, likely to be in need for third party legal and security protections.

CONCLUSION

The future of the Cloud involves computing with virtual representations without the physical presence of hardware or software. For example, programmers can use a web-based platform to design their applications of business users can operate their businesses with easy to customize online software. There are many benefits from switching over to Cloud computing. One benefit is that capital expenditure costs are lowered as new systems and maintenance costs are reduced through a pay-as-you-go methodology. Developers are alleviated of their worries regarding interoperability or data portability. As Cloud computing becomes more popular, questions regarding legal issues start to arise so effective polices are needed on both the international and local level. Cloud computing is an emerging field that has been embraced by both small and large businesses. It has a lot of potential to revolutionize businesses today.

However, the future of Cloud computing is not all that sunny, if fact it could be very Cloudy unless possible security and legal risks are dealt with and a successful business model is established. There are potentially tough security and legal risks tasks associated with Cloud computing which mainly revolve around the questions of compliance, support SLA, global performance, availability of bandwidth, misuse of client data, IP infringement, transparency, location of client data and most of all the question jurisdiction in case of legal disputes. Businesses today demand assurance and confidence to deal with any service provider, the question of risk tolerances is a major issue, they also need the flexibility to use services for their business needs of varying levels of legal challenges. In order to address the service level agreement issues, Cloud service users can turn to a third party legal and security risk management agency. A risk management agency could be engaged in all other key Cloud challenges such as governance, most other legal challenges including IP implementations, conflicts involving multiple jurisdictions, issues related to protection of privacy, network security, audit, application security, storage, cryptography, and

virtualization. This will give birth to a robust authoritative mechanism in order to take potential legal challenges and security risks away from both Cloud providers and Cloud users alike.

BIBLIOGRAPHY

<http://www.forrester.com/rb/research>

http://news.cnet.com/8301-10784_3-9889947-7.html

<http://knowledge.wpcarey.asu.edu/article.cfm?articleid=1614>

<http://www.cs.ucy.ac.cy/~gpallis/publications/journals/editorial.pdf>

<http://www.gartner.com/it/page.jsp?id=707508>

http://www.google.com/apps/intl/en/business/collaboration.html#utm_medium=et&utm_source=docs-en-hcnav&utm_campaign=crossnav

<http://www.ibm.com/ibm/green/index.shtml>

<http://www.infoworld.com/d/Cloud-computing/what-Cloud-computing-really-means-031>

http://www.nytimes.com/2007/11/15/technology/15blue.html?_r=1

<http://www.redcanary.ca/view/Cloud-computing>

<http://www.rollbase.com>

<http://www.salesforce.com>

<http://www.Cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>