Judicial Frameworks and Privacy Issues of Cloud Computing

Riyaz A Jamadar[1], **Pritesh A Patil**[2]

AISSMS IOIT, Pune-01, India

Abstract: ***Cloud Computing a leading and getting widely adopted technology in industry, unveils some unprecedented challenges to security of company's resources such as capital and knowledge based assets. Hither to no much attention has been paid by the governments and there is neither any universal standard adopted, nor any breakthrough to take up these challenges. Traditional contracts and licensing agreements may not provide adequate legal resources and remedies normally associated with the layers of protection for corporations. Intellectual Property, Foreign Direct Investments (FDI) and corporate governance issues have to be fully explored and practiced in domestic and international markets. So this paper discusses the need of establishment of Law and judicial framework of policies to the services embedding cloud computing technology, besides this it also addresses legal issues and existing policies adopted by different countries.***

Keywords: Cloud Computing, Cloud Security, Judicial policies, regulatory control

1. Introduction

Cloud computing is rapidly becoming an integral part of how we communicate with one another, buy music, share photos, conduct business, pay our bills, shop, and bank. Many of the activities that once occurred solely in the physical world, including communications with one another, are increasingly moving to the digital world. What was once a letter to a friend is now a Facebook message; a call to a loved one is now a Skype chat; a private meeting with a business partner is now a video conference call. In short, the cloud is revolutionizing not only how we compute, but also how we live. So, creating a judicial framework that would require companies to provide baseline protections for personal information while also taking steps to enhance users' control over their own data.

This has been elaborately discussed in this paper, which is organized in six sections. The first Section provides an overview of cloud computing and its Architecture. The Second section addresses various kinds of security threats and privacy issues titled as Security of Resources at Stake.

The third section of this paper elaborates judicial frameworks of policies adopted different countries. Fourth Section Discusses How insufficient are SLAs to protect and secure data in the Cloud. Finally the fifth section draws some important conclusions and the Sixth section lists all the references.

2. An Overview of Cloud Computing & It's Architecture

With the rapid development of processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful and more ubiquitously available than ever before. This technological trend has enabled the realization of a new computing model called cloud computing, in which resources (e.g., CPU and storage) are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion. In a cloud computing environment, the traditional role of service provider is divided into two:

The *infrastructure providers* who manage cloud platforms and lease resources according to a usage-based pricing model, and, the *service providers*, who rent resources from one or many infrastructure providers to serve the end users. The emergence of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the past few years, where large companies such as Google, Amazon and Microsoft strive to provide more powerful, reliable and cost-efficient cloud platforms, and business enterprises seek to reshape their business models to gain benefit from this new paradigm. Indeed, cloud computing provides several compelling features that make it attractive to business owners, as shown below.

No up-front investment: Cloud computing uses a pay-as you go pricing model. A service provider does not need to invest in the infrastructure to start gaining benefit from cloud computing. It simply rents resources from the cloud according to its own needs and pay for the usage.

Lowering operating cost: Resources in a cloud environment can be rapidly allocated and de-allocated on demand. Hence, a service provider no longer needs to provision capacities according to the peak load. This provides huge savings since resources can be released to save on operating costs when service demand is low.

Highly scalable: Infrastructure providers pool large amount of resources from data centers and make them easily accessible. A service provider can easily expand its service to large scales in order to handle rapid increase in service demands (e.g., flash-crowd effect). Generally speaking, the architecture of a cloud computing environment can be divided into 4 layers: the hardware/datacenter layer, the infrastructure layer, the platform layer and the application layer, as shown in Fig. 1.

As Cloud Computing technology has become more cost-efficient through the architectural changes and modifications of the above-discussed composite of varying models and their applications, there is a growing concern about another quickly developing area that has matched the speed of Cloud Computing and that is the amount of risk or uncertainty inherently embedding itself in the layers of protection that have, up to this point in time, provided sufficient risk assessment and management controls and industry standards for on-site computing models.

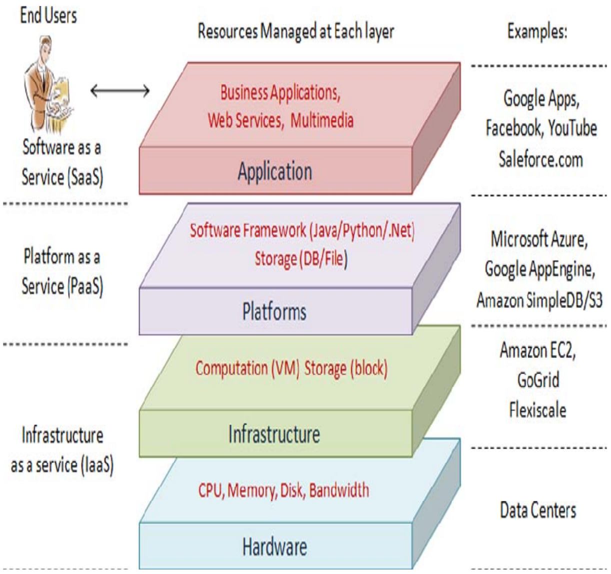
End Users
Resources Managed at Each layer
Examples:
Business Applications, Web Services, Multimedia
Application
Google Apps, Facebook, YouTube Saleforce.com
Software as a Service (SaaS)
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Microsoft Azure, Google AppEngine, Amazon SimpleDB/S3
Platform as a Service (PaaS)
Computation (VM) Storage (block)
Infrastructure
Amazon EC2, GoGrid Flexiscale
Infrastructure as a service (IaaS)
CPU, Memory, Disk, Bandwidth
Hardware
Data Centers

Figure 1: The Architecture of Cloud Computing Environment

3. How Security of Resources at Stake

Although the jurisprudence of Internet privacy is in its infancy, the current body of case law sheds light on how the Fourth Amendment and federal statutes apply to the cloud. When applying the Fourth Amendment, it appears that courts have not distinguished between traditional forms of Internet communication and cloud-based communication; the same rules apply to each. However, when applying the Stored Communications Act, cloud computing such as web-based e-mails or messaging through social network sites has not received the robust privacy protections accorded to traditional e-mail services.

Inherent within this service-based industry are multiple layers of low- to high-risk areas in connection with clouding types, such as Software as a Service, Platform as a Service, and Infrastructure as a Service. In response to this demand curve, numerous small- to large-scale providers and ancillary third-party contractors and subcontractors have created a myriad of pay-as-you-go services in public, private and community clouds, with varying levels of expertise and resources and with varying levels of risk. Subsequently, as with any emerging technology and business model, there are few industry-wide solutions to cloud computing risks.

Moreover on the issue of regulatory compliance, Gartner establishes that customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Gartner goes on to say that industry best practices require traditional service providers to undergo external audits and security certifications, cautioning customers to veer away from providers who refuse to provide this level of industry standardization and security scrutiny.

4. Information Policies Adopted in the United States

To compound the complexity of these security issues, there is growing concern about a uniform information policy in the United States, with application to the emerging cloud computing technologies. Information policy in the United States, simply put, is continuing to fall further and further behind in policies related to new technology developments and how these developments are being employed. This gap between policy and technology has been noted, as has the increasing speed and distance of the gap as the United States continues to make laws retroactively and based on a pre-electronic mentality [1]. Jaeger, Lin, and Grimes argue that to ensure the growth and adoption of cloud computing, it will be necessary to find technological and policy solutions for ensuring privacy and assuring information security [2].

Despite the advantages of this clouding model, Youseff and De Silva [3] recognize that deployment issues such as security and availability of the cloud applications are major issues that do not have an industry-wide solution yet. They further state that the leniency of SLAs may prolong a solution to these extant problems due to the compos ability of the clouding layered environment. Current security approaches include using Public Key Infrastructure (PKI) and X.509 SSL certificates as a methodology for authentication and authorization in the cloud.

Youseff and De Silva opine that due to the absence of cloud computing standards, such issues as cloud security, data privacy and ownership policies will continue to be major concerns as a result of different approaches and services provided by each cloud provider.

The gaps between policies and technological realities are becoming so significant in some cases that arguments can be made that information policies may have to be completely re-thought [9]. This situation is further confounded by the number of policy decisions left to the marketplace in the United States that are more heavily regulated through policy in other nations [1].

In highlighting the case for a uniform and national information policy regime, Cloud Computing not only affects SAS-70 and Sarbanes-Oxley (SOX) compliance, but also Gramm- Leach-Bliley (GLBA), Payment Card Industry Data Security Standards (PSI DSS), and the Health Insurance Portability and Accountability Act (HIPAA). Compliance with such regulations and standards requires varying degrees of security, and the data will likely need to be handled differently [5].

An examination of the SAS-70 SOX compliance control objectives reveals the importance of managing risk by ensuring that third-party processors place internal controls in their framework to ensure due diligence for audits and industry and regulatory compliance.

To understand the layers of federal legislation and regulations applying to information policy and internet use, the Federal Information Security Management Act ("FISMA"), 42 U.S.C. § 3541 *et seq*., a United States federal law enacted in 2002 as Title III of the EGovernment Act of 2002, provides a uniform regime to address the levels of risk that may arise from domestic and international sources.

The act basically recognizes the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA has brought attention within the federal government to cyber-security and explicitly emphasized a "risk-based policy for cost-effective security." FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act.

In FY 2008, federal agencies spent $6.2 billion securing the government's total information technology investment of approximately $68 billion or about 9.2 percent of the total information technology portfolio (Federal Information). One of the problems besetting the international community and WTO members is a set of different jurisdictional frameworks that offer varying levels of risk protection.

The protection of personally identifiable information provides such an example—there are enormous differences between the minimal regulation of the United States and the intricate protection structures of the European Union [11].

5. Service Level Agreements and Terms of Use

SLAs govern upstream and downstream users in a clouding/on-demand model, and therefore, users can negotiate terms and conditions on such important issues as perpetual licensing arrangements, civil and criminal liability, fundamental breaches, data usage, proprietary scalability, and M&A protection and trailing liabilities, among others [12].

Nolan advises clients, on negotiations with regard to the bargaining power between cloud providers and end-users, that contracts may be standard forms or individually negotiated, which is the preferred method of liability protection because the parties can tailor the terms and conditions appropriate to the level and degree of contractual obligations and performance .

As a practical consideration, small- to medium-sized businesses may not have the kind of leveraging power to enter into substantive negotiations, due to scale, size and resources that larger-scale enterprises, such as MNCs, will typically possess in traditional contract negotiations and this economic reality may affect a small- to medium-sized company's ability to protect against risk in a clouding environment. As to the global marketplace and the ramifications of clouding providers providing services in international markets, clouding users must understand the importance of various treaties and foreign government laws and regulatory regimes in considering what mix of IT and C-level strategies will work in the areas of risk assessment and management. Due to the emerging technology clouding markets, governments of both developed and developing countries are still responding to this SOA model by augmenting existing information and security policy(s) to include the SOA and quality of service (QoS) issues, resulting in a reactive, heterogonous framework of policies.

Under the World Trade Organization (WTO), existing tariffs are reduced and the agreement extends General Agreement on Tariffs and Trade (GATT) to new areas, including service industries. The WTO expects countries to upgrade their intellectual property (IP) laws to protect patents and copyrights and to guard against the piracy of items such as computer software and videotapes. International licenses and contracts are recognized by and given protection under the Convention on the International Sale of Goods ("CISG"). The CISG applies to contracts for the commercial sale of goods (consumer sale for personal, family, or household use are excluded) between parties whose businesses are located in different nations. If a commercial seller or buyer in the U.S., for example, contracts for the sale of goods with a company located in another country that has also adopted the CISG, the convention and not the UCC applies to the transaction [4].

As yet another example of the inherent difficulty of policing trade and security issues in a clouding environment, there arises a troubling set of questions about the scope and reach of the CISG's coverage of SLAs across multijurisdictional lines, which includes the implications of what rules of law apply and in which forums and venues such disputes can be resolved. These issues, as suggested earlier, may have to be ultimately resolved through litigation and its appeal cycles before a final determination on the allocation of risk(s) can be made and before a bright line test(s) on these issues can be drawn. The importance of regional alliances to comparative advantage also needs to be considered in these risk assessments, as there are numerous alliances that, in some cases, have restricted trade solely to their member states, affecting the clouding community's ability to protect against levels of risks present in such jurisdictions.

The North Carolina Bar Association recently crafted a proposed Formal Ethics Opinion in connection with the propriety of using a practice management program (e.g., Clio) in the practice of law. Under the Rules of Professional Conduct ("RPC"), a law firm may use such a cloud computing program provided that steps are taken to minimize risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including file information, from risk of loss. The proposed rules were crafted in cooperation with and oversight from the ABA Legal Technology Resource Center, whose leadership provided guidance and counsel on the merits of cloud computing.

6. Conclusion

From the above fully fledged discussion, it could be concluded that cloud computing is an emerging technology and a flexible and economical business model in which inherent layers of risk exist throughout the value chain.

The industry-wide adoption and utilization of industry certifications and security measures remove some of the risk by implementing internal controls and ensuring password and encryption measures; however, due to the lack of uniformity present in the terms and conditions of provider contracts and Service Level Agreements, as discussed, consumers may be exposed to layers of risk depending on how much risk of loss is assumed by the providers, subcontracting third-party vendors, and other parties included in the liability chain. As shown, governments have not provided a uniform and homogenous information policy regime in which private industry is given clear guidance as to multijurisdictional risk, cyber-terrorism risk, outage risks, and M&A risks.

The traditional system of contractual protection afforded service industries, such as financial, technological, and healthcare industries, may be exposed to high levels of risk by entering into Terms of Use agreements and Service Level Agreements in which providers hold the upper-hand on assumption of liability and risk of loss, as defined in negotiations and final calls. In this environment, SMEs may be at a disadvantage due to lessened leverage and power to negotiate, in comparison to larger enterprises, such as MNCs, whose ability to negotiate more favorable terms and conditions is predicated on more scalable resources and more layered protections against the levels of risk in cloud computing technology.

So an organization must conduct a thorough and diligent risk assessment of the potential threats of low to high risk inherent in cloud computing environments, and must ensure that all management and operational strategies and initiatives incorporate an optimal mix of cost-efficient processes, policies, and controls to militate against these risks.

References

[1] Braman, S. (2006). Change of state: Information, policy, and power. Cambridge, MA: MIT Press. :

[2] Jaeger, P.T., Lin, J., and Grimes, J. (2008). Cloud Computing and Information Policy: Computing in a Policy Cloud? Journal of Information and Politics, 5(3): 269-283.

[3] Youseff, L., Butrico, M. and Da Silva, D. toward a Unified Ontology of Cloud Computing. Retrieved from:

[4] http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf.

[5] Reed, O.L., Shedd, P., et al. The Legal and Regulatory Environment of Business, 15th Edition (2010 McGraw-Hill-Irwin). http://www.buyya.com/papers/hpcc2008_keynote_cloudcomputing.pdf.

[6] Cherry, Bakaert & Holland L.L.P. The Impact of Cloud Computing on SAS-70 Compliance Issues, 2010. (2010). Retrieved on September 13, 2010 from http://www.cbh.com/index.asp.

[7] Federal Communications Commission (2009). Broadband plan Executive Summary. Retrieved from http://www.raunfoss.fcc.gov/edocs_public/index.do?document=296858.

[8] Johndavid Kerr Harris-Stowe State University Kwok Teng University of West Alabama

[9] Cloud computing: legal and privacy issues, Journal of Legal Issues and Cases in Business pp 1-11

[10] Khajeh-Hosseini, A., Sommerville, I. and Sriram, I. Research Challenges for Enterprise Cloud Computing. Retrieved from http://arxiv.org/abs/1001.3257.

[11] Travis, H. (2006). Building universal digital libraries: An agenda for copyright reform. Pepperdine Law Review, 33, 761-833.

[12] Cherry, Bakaert & Holland L.L.P. The Impact of Cloud Computing on SAS-70 Compliance Issues, 2010. (2010). Retrieved from http://www.cbh.com/index.asp.

[13] Sunosky, J.T. (2000). Privacy online: A primer on the European Union's Directive and the United States' Safe Harbor privacy principles. Currents: International Trade Law Journal, 9, 80-88.

[14] Spinola, Maria. An Essential Guide to Possibilities and Risks of Cloud Computing. http://www.mariaspinola.com/whitepapers/Updates_White_Paper_An_Essential_Guide to Possibilities_and_Risks_of_Cloud_Computing.html.

Author Profile

Riyaz A Jamadar is working as Assistant Professor, having 15 years of corporate experience in Programming technologies, having passion for Information and Communication Technology. Graduate in Electrical and Electronics Engineering. His areas of Interest: Cloud Computing and its Security, Networking, Programming Paradigms and Java and Android. LMISTE (Life member Indian Society for Technical Education) Member Computer Society of India.

Pritesh A Patil is working as HOD and Assistant Professor, having 11 years of Academic experience fervor towards Database on Cloud and security. Post Graduate in Computer Engineering. His areas of Interest: Database on Cloud and its Security, Network and Cyber Security. LMISTE (Life member Indian Society for Technical Education) Member Computer Society of India.