Cloud Computing: Vulnerabilities, Privacy and Legislation

Amit Kiran*
Priyam Lizmary Cherian**

Abstract

Cloud computing is an indispensable part of the current business and service industries, its usage raising many issues. These issues range from those intrinsic to the nature of cloud itself and those stemming as a result of inability of the legislature to keep up with the dynamic nature of technology. This paper discusses the nature of conflicts and issues that may arise in providing cloud services .Starting with the possibility of security threats to cloud computing, the paper discusses the overlap of cloud services with intellectual property. It further looks at the legal regime for protecting and regulating cloud related activities. The need for standards and best practices is also reviewed. The paper concludes with a call for regulatory reforms both at a national and international level.

Keywords: Cloud Computing, Data Breaches, Green grid

Introduction

In its simplest form, cloud computing maybe said to be the infrastructure provided in the form of computer resources over a network connection, typically the internet, which is determined by the needs of the end user. The National Institute of Standards and Technology define cloud computing as,' a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'[1]. In essence, cloud computing involves self-service, commonly pooled resources, broad network access, elasticity of use and a measured service. Normally, while this service may exist in many forms, it is most commonly used as Software as a Service (SaaS), where programs operating on cloud software are provided to clients, Platform as a Service (PaaS), where the client is allowed to develop software or programs that operate on the cloud services, and Infrastructure as a Service (IaaS), where processing, storage, networks, and other fundamental computing resources are provided for the use of the client. Cloud computing might exist as a private cloud, a public cloud, a hybrid cloud or as a community cloud.

On analysis of cloud computing in its current form, it is clear that many difficulties exist in its regulation, control and classification. For example, servers hosting cloud computing might not operate in the same country as the client themselves, thereby limiting the territorial jurisdiction of the country in regulating and safeguarding such services. Further, while cloud computing is regulated by the standards set by the country hosting such services, offences or breaches of protocol in any other country cannot be contested without a treaty between the countries or a clause in the contract between the parties that specifically deals with the issue of jurisdiction.

Cloud computing is indispensable as most businesses and service providers as well as all online transactions primarily rely on cloud based computing services for any transaction or interface on an as per need basis. In this light, the problem of security in cloud computing is pivotal, as any breach would lead to the loss of crores of rupees (with the value of cloud computing predicted

Amit Kiran*
5th year, B.A. LL.B.
University Law College, Bangalore
2, 5th Cross, P&T Layout, Horamavu, Bangalore

Priyam Lizmary Cherian**
3rd year, LL.B.
Faculty of Law, University of Delhi
1989, Outram Lines, Kingsway Camp, Delhi

to be 5 percent of the total investments in India by 2015[2]), with little or no possible legal recourse.

Security Threats to Cloud Computing

According to the Cloud Security Alliance, the top threats in cloud computing are as follows[3]

- Data Breaches- where sensitive and valuable information is gained by parties who have access to such software.
- Data Loss – of valuable data through malicious processes or physical destruction of such hosting servers.
- Account or Service Traffic Hijacking – through the use of the security clearances or credentials of actual parties to gain unauthorised access to information.
- Insecure interfaces and Application Programming Interfaces – flaws in the basic interface systems would lead to various security issues.
- Denial of Service – by the actions of malicious third parties so as to delay the delivery of any cloud service or increasing the cost of such services.
- Malicious Insiders – where due to improper configuration of cloud services system administrators are allowed unauthorised access to the sensitive data of customers.
- Abuse of Services – by using cloud services, such as computational power, to facilitate hacking of servers or for the distribution of pirated software, etc.
- Insufficient Due Diligence – leading to a lack of internal controls and in the case of breach of contract, ambiguity in its enforcement.
- Shared technology vulnerabilities – with the use of software by customers where any breach in the software could lead to a breach of the entire cloud based system.

Intellectual Property and Cloud Computing

In the process of uploading and storing data on the cloud, there is a possibility of creating new Intellectual Property. For instance, in the service model of PaaS, the consumer may create applications using libraries and tools supported by the provider[4]. In absence of any clause to this effect, it would be difficult to determine who would be the author/owner of the patentable or copyright work that is created on such a platform. A clear claim in the contract(for instance clause 5 of Dropbox business agreementexpressly provides that Dropbox would not have any intellectual property in the consumer data)or assignment of copyright would help in determining the ownership over the/any newly created work.[5]

Primarily, the work that has already been created and thereafter placed on the cloud may indicate clear ownership of the author, i.e. the cloud service user.

While acting as a platform for exchange and storage of huge amounts of data, the cloud service providers are constantly running the risk of storing infringing material. The service providers in such situations are often protected under the safe harbour provisions. In cases where the cloud services provider allows recording and storing of content that may infringe the copyright of a third party, any liability would depend whether the country's statute allows copying for personal use or grants time-shifting exceptions under its copyright laws. (an example is Section 111 of Copyright Act, 1968 of Australia which provides that any recordings made for domestic use and to be viewed or heard at a later time does not infringe the copyright in the work) [6]

An IP owner needs to keep a constant check and be aware of possible loss of confidential data stored on cloud as a result of data mining. Clearly defining and demarcating the confidentiality obligations of the service provider, the customer and other third parties thereby becomes imperative.

Legislation

In India cloud providers can be held liable for any illegal data that they might host, however this is limited to cases where it can be proved that the provider was aware of the 'illegal nature of the data' hosted, and have not taken any steps to limit or remove such data, even when they were made aware of such an infringement. India is currently not a signatory of the Budapest Convention of Cyber Crime[7]; a pivotal international treaty which overruled the principal of

location as a connecting factor from a legal perspective, thereby weakening our position on the matter.

Excluding the provisions of the Indian Contract Act, 1872 the only legislation that governs cloud computing in India is the Information Technology Act, 2000. This Act contains four provisions that specifically deal with breach and misuse of data. Section 43 protects the owner of the computer /computer system/network/ resource from any damage to computers or computer systems with regard to unauthorized copying, extraction, database theft, and digital profiling. In case of cloud services, the owner can be the consumer using the services of the Cloud Service Providers (CSP's). Section 65 protects the cloud service users against the tampering of computer source documents. Such an act is punishable by either or with a combination of a fine up to two lakh rupees and imprisonment up to three years.

Section 66 of the Act deals with computer hacking and protects users from intentional alteration/misuse of data on their computers. The penalty is the same as that for Section 65. Section 72 imposes a fine of one lakh rupees and an imprisonment term of up to two year for any breach of confidentiality or misuse of private data.

These provisions have been widely interpreted by Courts to cover most of the cases involving breach of security or violation of privacy with regard to cloud based computing. However, the absence of specific laws governing cloud computing and the lack of a strong supervisory role of the Telecom Regulatory Authority of India (TRAI), leaves much to be desired. While protection is mentioned in the form of penal liabilities, it is wholly insufficient inasmuch that the economic loss that caused by such infringement is far more severe. In this light, the current legislative regime as it lies is wholly insufficient in dealing with theissues of regulation, protection and supervision of cloud based services and the problems that exist or may arise in its functioning.

Cloud Computing Standards

A plethora of players in the sphere of cloud computing offer varied services. The different terms and standards of these services often pose difficulties to service adopters in migrating to other CSP's , integrating data and applications over CSP's or maintaining effective audit processes across service providers. The lack of a standard in cloud computing not only poses serious questions on interoperability but also creates hurdles at the initial stage of comparing and evaluating the cloud services.

These incompatibilities in transition are broadly categorised as[8] –

1. Technical
2. Business
3. Semantic

Technical: This aspect is related to the reliability and security issues associated with the cloud services. The security related cases in interoperability may include user authentication in cloud, data access authorization policies, and user credential synchronization between enterprises and the cloud. [9]

Business: This may be associated with unavailability/ want of a standard interface that may provide audit or assessment of the environment.

Semantic: It refers to portability and interoperability of CSP's. Interoperability means the ability to communicate with entities to share specific information. Portability on the other hand is the ability to migrate workload and data from one provider to another.

One would assume that transfer and interoperability would be facilitated by setting out one uniform standard. The present scenario suggests otherwise. Instead of collectively creating a single definitive regulation, the top organisations seem to be suggesting their own set of norms.

There are more than 30 standardisation initiatives from around 20 organizations. These initiatives range from The Institute of Electrical and Electronics Engineers Standards Association's P2301[10] and P2302 [11]working groups looking at standardisation in cloud management and interoperability to the National Institute of Standard and Technology's Cloud Computing Standards Roadmap[12]advocating best practices and standards. Other organisations that have proposed best practices for use of cloud computing

include The Green Grid, The Cloud Security Alliance, The Distributed Management Task Force, The European Telecommunications Standards Institute and The Storage Network Industry Association.

In October 2014, International Organization for Standardization(ISO) also released new standards for cloud computing[13]. These set of rules are said to have seven distinct cloud services categories including Network as a Service (NaaS) and Data Storage as a Service (DSaaS) as opposed to the three categories identified by NIST (as discussed above)[14].

These varied and overlapping standards seem to be further delaying creation of a uniform practices.

Conclusions

On analysis of the current legislative regime on cloud computing in India, it is clear that there are lacunae that need to be addressed in order to strengthen the security and regulation of Cloud Services in the interest of protecting sensitive data and the privacy of the users. Such reforms are a double edged sword as they must be strict enough to ensure compliance and liberal enough not to discourage companies from using cloud services.

There must be a greater involvement of the TRAI in line with the National Telecom Policy[15] The TRAI in governing Internet Service Providers (ISP's), can ensure the co-operation of the ISP's in preventing such breaches in privacy, security or violation of any intellectual property rights, a necessary action in the light of voluminous online traffic.

In the absence of clear contractual terms, disputes may arise over accountability of data and its security. Though the Information Technology Act can be of help in cases of any data security breach, ambiguous terms of contract may lead to complex issues when the data is being used by the CSP s for their management and development. Provisions for notification on any breach, and smooth transfer of data on termination of services can also be some aspects that may be considered in the contract of service.

The next big leap in the regime of interoperability of cloud service is definitely the creation of one determinate standard of operation and services. The multiple, overlapping standards proposed are adding to the numerable drafts. The need of the hour is for the stakeholders to come together under one umbrella and adopt one single standard that may be used by the CSP's worldwide. An international treaty setting minimum standards for cloud service could be the way forward for solving the issues surrounding jurisdiction, and interoperability.

The Cloud is increasingly changing the way enterprises are modelling their innovation and development strategies. With its on demand access, elasticity to meet varying demands and its dynamic nature, cloud has redefined the IT and business sectors' operations. The increased subscription to CSP's is a clear indicator of the sailing future of clouds. To avoid any turbulence, the Indian legislature needs to fill the lacunae and make appropriate provisions facilitating trade and transactions over cloud in order to deal with any current or novel issues that are bound to arise.

References

1. PeterMell and Timothy Grace, " The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology", *National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-145*, p.2
2. ShiplaShanbag, "Emerging from the Shadows," *Dataquest,* Vol. XXIX No. 10, May 31, 2011 at 22.
3. "The Notorious Nine: Cloud Computing Threats in 2013", *Cloud Security Alliance,* February 2013, p.6
4. Mell& Timothy, supra note [1] at p. 2
5. Dropbox Business Agreement- https://www.dropbox.com/terms#business_agreement [February 12, 2015]
6. Copyright Act, 1968- http://www.comlaw.gov.au/Details/C2014C00291 [February 12, 2015]
7. GowriMenon, "Regulatory Issues in Cloud Computing: An Indian Perspective",*Journalof Engineering, Computers & Applied Sciences (JEC&AS)*,Volume 2, No.7, July 2013

8. RajinderSandhuand InderverChana, "Cloud Computing Standardisation Initiatives: State of Play", *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.2, No.5, October 2013, pp. 351-362 ISSN: 2089-3337

9. Grace A. Lewis, "The Role of Standards in Cloud Computing Interoperability", Software Engineering Institute, Technical Note CMU/SEI-2012-TN-012, October 2012, Carnegie Mellon University

10. Guide for Cloud Portability and Interoperability Profiles-http://ieee-sa.centraldesktop.com/p2301public/ [February 12, 2015]

11. Standard for Intercloud Interoperability and Federation-http://grouper.ieee.org/groups/2302/ [February 12, 2015]

12. NIST Cloud Computing Standards Roadmap -http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf [February 12, 2015]

13. Standards Catalogue -http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=601355[February 13, 2015]

14. ISO publishes new cloud computing standards and definitions-http://www.cloudcomputing-news.net/news/2014/oct/20/iso-publishes-new-cloud-computing-standards-and-definitions/[February 12, 2015]

15. National Telecom Policy,2012-http://www.trai.gov.in/WriteReadData/userfiles/file/NTP%202012.pdf [31.01.2015]