# Cloud Computing and Privacy Regulations: An Exploratory Study on Issues and Implications

Mr. Atul V Tayade[1], Swapnil A Bobade[2]
[1]Student, College of Engineering and Technology, Akola
[2]Assistent Professor, College of Engineering and Technology, Akola

***Abstract - Cloud computing is a new paradigm in the world of Information Technology Advancement. Considerable amount of cloud computing technology is already being used and developed in various flavors. Cloud Computing affects people, process and technology of the enterprise. In spite of having benefits with Cloud computing paradigm such as efficiency, flexibility, easy set up and overall reduction in IT cost[22],cloud computing paradigm could raise privacy and confidentiality risks. "Not all types of cloud computing raise the same privacy and confidentiality risks. Some believe that much of the computing activity occurring today entirely on computers owned and controlled locally by users will shift to the cloud in the future"[11]. In Cloud computing, users connect to the CLOUD, which appears as a single entity as opposed to the traditional way of connecting to multiple servers located on company premises. Public Private Partnership these days is a usually adopted pattern of governance to meet the diverse needs of their citizens with confidence and providing quality of these services. Cloud Computing Technology can also act as a facilitator between public and private partnership. In such cases there is a possibility that an external party can be involved in providing Cloud Services having partial control over the data storage, processing and transmission of data and privacy regulations become relevant [20]. Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information. A survey by EDUCAUSE involving 372 of its member institutions revealed that a great proportion of the respondents with use cases that involved cloud-based services reported that data privacy risks and data security risks were among their top barriers to overcome [22]. A principal goal of this paper is to identify privacy and confidentiality issue that may be of interest and concern to cloud computing participants and users [11]. Thus this paper explores to elicit possible issues and regulations in the area of privacy that affect the implementation of Cloud Computing Technologies.***

## I. INTRODUCTION

The mission critical and enabling activities can be derived from Michael Porter's value chain concept. Mission critical activities are those that directly produce the output of the organization. Enabling activities are those that directly support the mission [1]. Public Private Partnership (PPP) can be used by the government in order to provide the use of technology to enable such service activities to the public effectively. The purpose of PPP organizations is to communicate, educate, inform, collaborate and manage the public IT management profession [1]. In this kind of scenario, Privacy becomes an important element of discussion because Privacy is considered to be one of the fundamental human rights [6][20]. Privacy is a fundamental human right recognized in the Article12 of the United Nations Declaration of Human Rights (UDHR 1948), Article17 of the International Covenant on Civil and Political Rights(ICCPR 1976) [12]and in many other international and regional treaties. In many of the countries where privacy is not explicitly recognized in the constitution such as the United States, Ireland and India, the courts have found that right in other provisions [6][7]. The most comprehensive translation of these rights into privacy protection legislation is the recent EU legislation on Data Protection(Council Directive 95/46/EC). Indian IT Act and Rules are having many of those provisions present in the IT policy. According to Dr. Gulshan Rai, CERT, India,[14] no country has implemented a true government cloud so far due to complex legal issues. It is because the three aspects such as privacy, security and right to information are like three vertices of a triangle. If someone wants privacy, one should compromise on security and compromise on the right

to information and vice versa. So it is required to strike a balance and for that a lot of maturity and awareness is required [14]. Currently it remains as a challenge to governance. De Boni, Prigmore (2001) [7]argue that the concept of privacy provides a solid basis for the assertion that private in formation is a form of property, a commodity to be bought and sold like any other commodity as an indication of a clear allocation of economic right. Thus the key battle ground lies with the competing aims of individual privacy vs. national interest [7] [8].

Cloud services refer to the provisioning of hardware and software resources across the Internet

[2] [5]. Cloud Service Providers (CSP) typically offer both refined software services, such as databases and raw computer resources such as storage or processing power. Customers often use these services by treating it as pay-per-use (PPU) model thus it can satisfy the argument of De Bony and Prigmore 2001 [7] to achieve privacy as an economic right. Because by using cloud services, companies can chose to, in effect rent computer resources rather than to invest in them outright having such elasticity of computing resources. Examples of such CSPs include Microsoft, Google and Amazon Web Services (AWS), where AWS is claimed currently the largest

## II. CLOUD COMPUTING DEFINED AND OTHER STORMS

NIST Special Publication 800-145 Draft defined 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 [18].

Cloud Computing Models can be categorized as Service Models and Deployment Models. Based on the service functional capabilities Cloud Service Models are classified as Cloud Software-as-a-Service (SaaS), Cloud Platform-as-a-Service and Cloud Infrastructure-as-a- Service (IaaS) [17] [23].

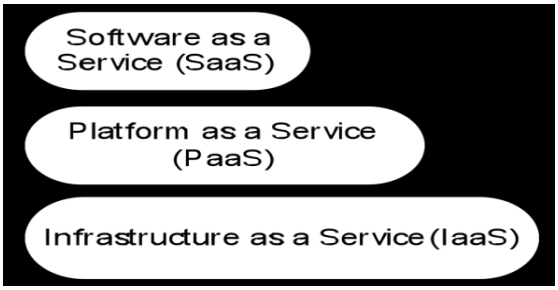


Figure1.The Cloud Service Layers [20]

Based on the service operational capabilities, Cloud Deployment Models are classified [18] as shown in figure [20].

| | Managed by | Owner of infrastructure: | Dedicated hardware |
|---|---|---|---|
| Public | Cloud Service Provider | Cloud Service Provider | No |
| Private, external | Cloud Service Provider | Cloud Service Provider | Yes |
| Private, internal | Internal Organization | Internal Organization | Yes |
| Hybrid | Mixed | Mixed | Depends on contract with the CSP |

Figure2.Cloud Type Classification [18][20]

Some definitions of terms that will help to clarify the discussion made in this paper are given here [11]:

Cloud Computer User: A customer or potential customer of cloud computing service. The user may be an individual, business, government agency or any other entity.

Cloud Service Provider: The organization that offers the cloud computing service. A cloud provider may be an individual, a corporation or other business, a non-profit organization, a government agency or any other entity.

Third Party: A cloud service provider is one type of third party, which maintains information about or on behalf of another entity.

Privacy: It means free from others interference. Privacy control allows the person to maintain varying degree of intimacy. It helps in protecting the love, friendship and trust [9].

To guarantee a satisfactory level of privacy provision, any new technology should take

Nissenbaum three principles into considerations. These principles define the sphere of boundaries for the privacy [9].

They are:

(1) Limiting surveillance of citizens and use of information about them by agents of government

(2) Restricting access to sensitive, personal or private information
(3) Curtailing intrusions into places deemed private or personal.

In 2008, the term cloud computing entered main stream discussion about data protection and privacy. Analysts estimated that during 2009-2014, the global market for cloud computing can grow to $95 billion and that 12% of the worldwide software market will move to the cloud during that period [4]. So in order to realize the cloud potential, the businesses must address the privacy questions raised by this new computing model.

## III. PRIVACY CONCERNS, DATA SECURITY LAWS AND REGULATIONS

The following table summarizes the cloud computing privacy concerns, data security issues, laws, regulations and standards [16]:

| Sl. No. | Cloud Computing Privacy and Data Security Concerns | Description of Issues | Related Laws, Regulations and Standards | Remarks |
|---|---|---|---|---|
| 1. | Compelled Disclosure to the government | Cloud can be subject to different levels of protection than on the information it contain | In USA Electronic Communications Privacy Act (ECPA) Stored Communications Act (SCA) US Patriot Act FTC Fair Information Practice.<br>In UK The Regulation of Investigatory Powers Act [3].<br>In India RTIAct2005 [13]. | In UK, India, Singapore and Malaysia, the national cryptography policies may allow lawful access to plaintext or cryptographic keys/data based on the OECD Guidelines on encryption [3]. India does not have any dedicated Privacy Laws [21]. |
| 2 | Data Security and Disclosure of Breaches | How can customer ensure security compliance when storing information on the cloud?<br>Is there a requirement of giving a notice when cloud security is breached? | Health Insurance Portability and Accountability Act (HIPAA)<br>Health Information Technology for Economic and Clinical health (HITECH) Act Sarbanes Oxley State Laws and Regulations (For Data Breach Notification ) Section 5 of the FTC Act [16] In UK Data Protection Act 1998 The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations2011<br>Directive95/46/EC (Data Protection Directive) [20]<br>In India No Specific laws butITAct2005and 2008 amendments (cyber law) can be helpful. | 2006 (The bill is still pending).<br>In UK Data Protection Act (1998) exists.<br>In India The real problem is that India does not have any dedicated Data Protection Law and Legal Enablement of M- Governance in India [21] |
| 3. | Data Accessibility, Transfer and Retention | Can Companies and consumers have access to data on cloud?<br>Can the data be destructed by cloud owners or should it be returned to customers? | In USA Freedom of Information Act (FOIA) Payment Card Industry Data Security Standard (PCIDSS) FTC Fair Information Practice[15]<br>In UK The Safe Harbor Agreement (for data transfer between Europe and US) [20]<br>No specific laws in India. But the following can be helpful:<br>In India Right To Information Act 2005 [13] | In USA Entities that store consumer information on the cloud face the threat of FTC enforcement if their representations to consumers about where and how information is stored and secured do not Match the actual practices [16]. |
| 4 | Location of Data | The physical location of the server storing the Data may Have legal implications (such as Jurisdiction issues) | In USA NARA regulations (Title36ofthecode of federal regulations)<br>Payment Card Industry Security Standard (PCIDSS), Sarbanes-Oxley Act.<br>FTC Fair Information Practice [15]<br>Butin UK Compliance with EU Data Protection Directive (EC/95/46) (the Directive) is required [20]<br>In India No specific laws in India but IT Act 2008 can be helpful. | In USA It means with cloud computing, are the documents governed by the law of the state in which they ar physically located, by the location of the company possessing them, or by the laws of the state where a person resides?[10]. In UK Depending upon the location of the vendor's servers, traditional approaches such as model contracts or the Safe Harbor program, used to comply with the EU Data Protection Directive (EC/95/46) (the Directive), may not offer a workable solution and, at best, would be cumber some to implement and maintain [4]. |

Apart from the categorized listing cloud computing concerns given above, various other laws and regulations of USA related to: (1) *Compliance* are: the Clinger-Cohen Act of 1996, Office of the Management Budget (OMB) Circular No. A-130, particularly Appendix III, the Privacy Act of 1994, the E-Government Act of 2002 and its accompanying OMB guidance and the Federal Information Security Management Act (FISMA) of 2002(2) *Data Location* are: NARA regulations (Title 36 of the code of federal regulations) (3) *Electronic Discovery:* Freedom of Information Act [15].However incase of USA, NIST guidelines special document no.800-144 provides complete guidelines on Security and privacy in public cloud computing [15]. In case of UK, EU Directive 95/46/EC will help to harmonize the privacy laws that existed in the different member states of the European Union and to provide a basic standard on privacy protection [20]. In case of India, Information Technology Act 2008 (cyber laws included) may provide some help on data security and privacy.

## IV. PRIVACY ISSUES IN THE CONTEXT OF THIRD PARTY STORAGE

Information stored with a third party (including a cloud computing provider) may have fewer or weaker privacy protections than information in the possession of the creator of the information. IT managers are likely to be wary of surrendering control of the resources to outside providers who can change the underlying technology without customers consent. Thus the issues related to performance and latency can be seen as problematic [22]. Government agencies and private litigants may be able to obtain information from a third party more easily than from the creator of the information. The expanded ability of the government and other to obtain information from a third party affects both businesses and individuals. For many users, the loss of notice of a government demand for data is a significant reduction right [11]. In United States of America, the Electronic Communications Privacy Act of 1986 (ECPA) provides some kind of protections against government access to electronic mail and other computer records held by parties (e.g., Internet Service Providers) in an electronic environment. But at the same time, USA Patriot Act, originally enacted in 2001 and amended in 2005 includes provisions allowing the FBI access to any business record by extend the ECPA by compelling the cloud providers to disclosure of records. Similarly Right of Information Law or Freedom of Information Act 2000 kind of law sallow a private litigant or other party might seek records from a cloud provider rather than directly from a user because the cloud provider would not have the same motivation as the user to resist a subpoena or other demand. So Disclosure to third parties by a cloud provider could create problems with other laws, principles and interests.

Similarly the privacy becomes an issue when seeking health information against health related information act, fair credit report act, video piracy protection act, bankruptcy, trade secrets from cloud service providers thus making the effort to maintain secrecy towards debatable.

Web sites keep publishing a long list of publication on their terms and service may be considered as the most important feature of cloud computing for an average user who is not subjected to a legal or professional obligation from a privacy and confidentiality perspective. It is common for a cloud provider to offer its facilities to users without individual contracts and subject to the provider's published terms and service. If these terms of service give the cloud provider rights over a user's information, then a user is likely bound by those terms. This could affect the legality of information sharing by a user. In case of the data stored in multiple locations (in multiple servers) the user might get the reduced risk of legality or increase the risk of failure of protection in terms of not claiming from a specific jurisdiction. If the cloud service provider is an agent of competitor, there is possibility that all the important private information could pass easily to competitor through corrupted prosecutors and intelligence agencies without further notice or process.

## V. COMMON PRINCIPLES IN PRIVACY REGULATIONS

The privacy regulations discussed in this paper have much in common with the notable exception of the USA-Patriot Act or it might have been also included with some other name. But it is important to understand that these principles are recognized worldwide as setting the standards privacy. These principles therefore provide a standard in comparing privacy regulations (see figure 3).

Thus Cloud Service provider (CSP) organizations have a legal obligation to comply with legislation;

these organizations are responsible and accountable for compliance. Organizations can be held liable if a subcontractor breaches compliance with legislation. It is unknown if a CSP is legally considered the same as subcontractor. Currently there is no jurisprudence on this matter. However a CSP can be legally seen as a subcontractor [11]. This implies that organizations should ensure that a CSP is compliant with relevant privacy legislation. Jurisdiction is deemed to impact privacy on Cloud Commuting in other cases.

| | FTC Fair Information Practice Principles | Directive 95/46/EC | The HIPAA | The Gramm-Leach-Bliley Act | The Fair Credit Reporting Act | PCI-DSS |
|---|---|---|---|---|---|---|
| Notice | √ | √ | √ | √ | √ | |
| Choice/Consent | √ | √ | √ | √ | √ | |
| Access | √ | √ | √ | | √ | |
| Integrity | √ | √ | √ | √ | √ | √ |
| Security | √ | √ | √ | √ | | √ |
| Enforcement | √ | √ | √ | √ | √ | √ |

Figure3.Common Principles in Privacy regulations [20]

Horizontal axis: Various Privacy laws and regulations

Vertical axis: Common Principles in the various privacy laws and regulations Check mark: It means the principle is present in the regulation

Thus it can be summarized that various issues in cloud computing includes: Identity management, physical and personnel security, application security, cloud availability and accessibility to customers, privacy and legal issues.

## VI. SOME TECHNICAL ASPECTS OF CLOUD SECURITY ISSUES

There could be a launch of attacks from within the Cloud against external targets such as Cloud-based bot nets or bot clouds. Two bot cloud attacks are Distributed Denial of Service (DDoS) attack and Click Fraud attack. Both of these attacks were constructed and executed in less than one day and for approximately 100 Euros and both were successful in their respective goal. Furthermore, neither attack was detected or shutdown by the Cloud Service Providers. Criminals willing to launch bot net attacks are most likely to commit identity theft. When creating an account for Cloud services, a false name and stolen credit card information is used thus making the cost of the service a non-issue. With a dozen stolen credit cards, a criminal could launch a series of a dozen bot clouds, possibly on different CSPs. When one Cloud is finally detected and shut down, the next is launched and so on, resulting in an ongoing, massive attack. CSPs do not currently have a strong incentive to monitor all customers from the time they start using Cloud Services. Current policy is to wait until victims of attacks contact the responsible CSP at which point actions taken to disable the attack. So it is required that CSPs must implement a comprehensive botcloud detection and removal policy and mechanism otherwise botmaster will continue to move their malicious activities into the Cloud and botclouds will continue to grow. This requires the CSPs to proactively monitor for bot clouds and deploy cloud related extrusion detection systems [5].

## VII. CONCLUSION

Cloud computing has the potential to offer the ability to dynamically reconfigure computing resources as demand for computing resources increases or decreases. A Client Service Provider (CSP) needs to be capable of provisioning this demand. In cases where a CSP fails to provide this demand, the CSP itself may be forced to outsource organizational data to a different CSP, amplifying the location related privacy issues portrayed above. Thus the impact of privacy regulations is most dramatic between external Cloud computing and traditional IT. Thus the concept of Cloud Computing can bring many uncertainties with respect to compliance with privacy regulations. So current privacy regulations are clearly not enough to solve all the privacy issues related to Cloud computing. More matured awareness is required about both the issues and about the existing regulations and seems become a good first step to remedy this. Security could be seen as a major issue in the adaptation of Cloud computing as compared to compliance to privacy regulations [20]. Not many organizations are completely aware of privacy issues in Cloud Computing [19].

## VII. FURTHER RESEARCH

So we believe that research in the fields of privacy legislation and Cloud Computing would benefit substantially if future researcher could have access to more case studies with reference to policies, laws and regulations depicting various scenarios. This could

provide practical examples on how implementation of cloud computing affects the compliance of organizations with privacy regulations.

REFERENCES


[1] American Council of Technology (2011), The Role of Enterprise Architecture in Federal Cloud Computing, Shared Interest Group: Enterprise Architecture, A White Paper, from the collaboration of ACT and IAC, Fairfax, VA, Accessed via WWWandRetrievedon07-02-2012, Available @http://www.actgov. org /knowledgebank/whitepapers/Documents/Shared%20Interest%20Groups/Enterprise%20Architecture%20SIG/Role%20of%20EA%20in%20Federal%20Cloud%20Comp uting%20-%20EA%20SIG-%2001-2011.pdf

[2] Armrest et al. (2011), A view of cloud computing, Communications of the ACM, 53(4), pp.50-58.

[3] Brown, I. and Laurie, B. (2000), Security against compelled disclosure In *Computer Security Applications 16th Annual Conference (ACSAC '00)*. IEEE, New Orleans, LA , USA, Accessed from WWW and Retrieved on 12-03-2012 and Available @ http://www.apache-ssl.org/disclosure.pdf

[4] BrueningandTreacy(2009),PrivacyandSecurity LawReport,TheBureauOfNational Affairs, Inc.,Accessed from WWW and Retrievedon12-032012adAvailable@http://www.hunton.com/files/Publication/6acf0d97-7c21-42d1-ab48-315a04601152/Presentation/PublicationAttachment/37dc2129-4f0c-45a0-8417-651e05dc423f/CloudComputing_Bruening-Treacy.pdf

[5] Clark, K., Warnier, M. and Brazier, F. M. T. (2011), Botclouds: The future of cloud-based Botnets?CloserSciTePress,p.597-603, http:// homepage.tudelft.nl/68x7e/Papers/botclouds.pdf.

[6] Cavoukian, A. (1999), Privacy as a Fundamental Human Right vs Economic Right: An Attempt atConciliation, Informationand Privacy Commissioner, Ontario, Canada Available from <http://www.ipc.on.ca>

[7] De Boni, M., and Prigmore, M. (2001), A Hegelian basis for information privacy as an economic right, Proceedings of the UKAIS conference, Portsmouth.

[8] Edouard, N. & White, W. (eds.) (1999) UK PLC on the World Stage In 2010: Book 1: The Development of The Internet And The Growth Of E-Commerce Research Report, London, Management Consultancies Association.

[9] Esteves, R.M. and Chunming Rong (2010), Social Impact of Privacy in Cloud Computing In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), Nov. 30-Dec. 3 ,2010, pp. 593-596.

[10] Garrie, D., Who has Legal Jurisdiction in the Cloud?, Accessed from WWW and Retrieved on 12-03-2012 and Available @ https://www. gplus.com/legal-issues/insight/who-has-legal-jurisdiction-in-the-cloud-50084

[11] Gellman, R. (2009), Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum, USA.

[12] Global Internet Liberty Campaign, Privacy and Human Rights: An International Survey of Privacy Laws and Practice, Accessed from WWW and Retrieved on 07-02-2012 and Available @ http://gilc.org/privacy /survey /intro. html

[13] GoI, Guide on Right To information Act, 2005, Accessed from WWW and Retrieved on 12-03-2012 and Available @ http://rti.gov.in /RTICorner/Guideonrti.pdf

[14] Gulshan Rai (2012), Technology is changing the Entire Paradigm, Feb 2012, EGov Magazine, Noida, India.

[15] Jansen and Grance (2011), Guidelines on Security and Privacy in Public Cloud Computing, NIST, U. S. Department of Commerce, Special Publication 800-144. Accessed from WWW and Retrievedon13-03-2012andAvailable@http://www.nist.gov/custo mcf/get_pdf.cfm?pub_id=909494

[16] HoganLovells (2010), Cloud Computing: A Primer on Legal Issues, Including Privacy and Data Security Concerns, Retrieved on 12-03-2012 and Available @ http://www. cisco.com/web/about/doing_business/legal/privacy_compliance/docs/CloudPrimer.pdf

[17] Lin, G., D. Fu, J. Zhu and G. Dasmalchi (2009). Cloud Computing: IT as a Service. IT Professional, Vol. 11 No. 2, pp. 10-13.

[18] Mell, P. and Grance, T. (2011) The NIST Denition of Cloud Computing (Draft): Recommendations of the National Institute of Standards and Technology. Special publication 800-145 (draft), Gaithersburg (MD).

[19] Ruiter, J. (2009). The relationship between privacy and Information Security in Cloud Computing Technologies, Master Thesis, Vrije Universiteit Amsterdam

[20] Ruiter, J. and Warnier, M. (2011). Privacy regulations for cloud computing, compliance and implementation in theory and practice. In Gutwirth, S., Poullet, Y., de Hert, P., and Leenes, R., editors, Computers, Privacy and Data Protection: an Element of Choice, chapter 17, pages 293–314. Springer.

[21] Singhand Dalal (2010), In Absence of Dedicated Privacy Law &Data Protection Law -Is India Ready for Cloud Computing? http://www.techno-pulse.com/2010/12/privacy-data-protection-law-india-cloud.html

[22] Sultan, N. (2010), Cloud computing for education: A new dawn? International Journal of Information Management, Volume 30, Issue 2, April 2010, Pages 109–116.

[23] Weinhardt C., A. Anandasivam, B. Blau and J. Stosser (2009), Business Models in the Service World, IT Professional, Vol. 11 No 2, pp. 28-33.