ISSN No. 0976-5697

Volume 4, No. 11, Nov-Dec 2013

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Privacy Issues Regarding Personal Data In Cloud Computing

Anjul K. S. Rai
M. Tech Scholar-IT
NRI Institute of Information Science and Technology
Bhopal, India
anjulrai22@gmail.com

Dr. Samidha D. Sharma
Head of Department-IT
NRI Institute of Information Science and Technology
Bhopal, India
samidhad2000@gmail.com

Abstract: Privacy is a major concern for any organization or person for using the cloud. Managing personal data by others always has been debatable. Organizations are becoming nervous that there data may fall into the wrong hands. Cloud services based systems come together with inherent challenges, and these are difficult as info to privacy in to the cloud network. The flow of the cloud services is increasing the demand for handling sensitive information like personal information, however there are still several sets of circumstances within which the cloud isn't used because of security considerations. Our primary focus in this paper is on the implications of cloud computing and corresponding privacy agreements on personal privacy. There are several legal issues relating to privacy and cloud computing. Cloud services based mostly systems come together with inherent challenges, and these are difficult as info to privacy in to the cloud network.

Keywords: Privacy Preserving issues, Personal Data security, Cloud Computing

I. INTRODUCTION

The National Institute of Standards and Technology[1] defines "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". There are four basic cloud delivery models, as outlined by NIST [2], based on who provides the cloud services. The agencies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services.

a) Private Cloud- The cloud infrastructure has been deployed, and is maintained and operated for a specific organization.

b) Public cloud- Public cloud in which cloud services are available to the public and owned by an organization selling the cloud services, for example, Amazon cloud service.

c) Community cloud- Community cloud in which cloud services are shared by several organizations for supporting a specific community that has shared concerns.

d) Hybrid cloud- Which is a composition of different cloud computing infrastructure (public, private or community).

The working party [3] identifies the concerns as falling into two categories:-

a) Lack of control- Cloud clients does not control of the technical and organisational measures necessary to ensure the availability, portability, isolation, integrity, transparency and confidentiality of data.

b) Lack of information processing- Insufficient data about cloud services process operations poses a risk to controllers also on data subjects because they could not bear in mind of potential threats and risks and therefore cannot take measures they consider acceptable.

This paper focus on the issues of privacy preserving in cloud computing. The specific contractual protections include only authorised personnel to have access to the data. This paper focus is a comparative one from which it explores significant changes in data processing due to the cloud and the resulting tension with contemporary information privacy

II. PRIVACY ISSUES

Certain aspects of information privacy, like the proportionality principle, the aim of information process, and retention periods are, of course, an integral a part of the framework for information privacy. However, within the context of cloud computing they are doing not present any specificity. Area's that are exposed the foremost are the following:

a. Contractual personal data processing,
b. Data security,
c. Transfer of data to third countries.

There are several legal issues relating to privacy and cloud computing, including the uncertain applications of the Health Information Portability and Accessibility Act (HIPAA) [3], the Stored Communications Act [4] and the Fourth Amendment, especially the third-party doctrine of Fourth Amendment jurisprudence [5].

Privacy concerns the expression of or adherence to various legal and non legal norms regarding the right to private life [6]. In the European context this is often understood as compliance with European Data protection regulations. Although it would be highly complex to map cloud issues onto the full panoply of privacy and personal data protection regulatory architectures, the globally accepted privacy principles [6] give a useful frame: transparency, purpose restriction, consent, legitimacy, data subject participation and data security.

A. Issues arising:

Table I shows some issues arising in Cloud. This is populated from the review of the literature made during the course of this study and reflects key concerns noted from the desk research.

If you choose to store your files in the cloud you need to remember that this means they are really just stored on servers controlled by the service provider. Some providers of cloud services may also use the cloud services of another organisation.

Table I. Privacy Issues in Different Area

S. No.	Area	Issues
1	Virtualisation	Segregation of personal data on shared infrastructure
2	Web services	Security and confidentiality
3	Encryption in the cloud context	Security and confidentiality
4	Applicable law (data/service location)	Existence and effectiveness of privacy protection laws/ principles
5	Dispute resolution	Accountability: can disputes in the cloud be resolved?
6	Data protection and privacy	Compliance with privacy principles
7	Electronic communication in the cloud	Safeguarding communications secrecy
8	Validity and consent	Transparency must be ensured. Consent from consumers must be free, specific and informed

III. THE PERSONAL DATA PROTECTION

Alongside the benefit of cloud computing, however, lies a lack of transparency for cloud customers, causing legitimate concerns about how they can comply with the Data Protection.

A. Encrypted Data for Privacy:

According to a article by Aisling Duffy [7], Different types of personal data will require different measures to be put in place to protect it as the level of protection required will depend on the volume and nature of the personal data and the likely damage that would arise in the event of a breach. Carefully select and categorise the type of data being processed, including any metadata that is collected as a result. If the data is sensitive then the cloud customer should require the information to be encrypted. Alternatively, consider removing sensitive personal data (or indeed all personal data if possible) from the data being transferred. If all personal data can be made anonymous or removed prior to transfer into the cloud, that is even better.

B. Redundant Array of Independent Net-storages for Privacy:

According to a recent article by Martin[8], this describes how a redundant Array of Independent Net-storages (RAIN) can be deployed for confidentiality control in Cloud Computing. The RAIN approach splits data into segments and distributes segments between multiple storage providers; by keeping the distribution of segments and the relationships between the distributed segments private, the original data cannot be re-assembled by an observer. As long as each segment is small enough, an individual segment discloses no meaningful information to others, and hence RAIN is able to ensure the confidentiality of data stored in the clouds.

C. Malaysian Personal Data Protection Act:

According to section 43[9] of the Malaysia PDPA 2010, data subject is given the right to prevent processing of personal data for purposes of direct marketing. Cloud computing may breach the right of data subject due to its nature. Personal data stored in cloud computing might be offered to marketers. For instance, many email providers permit secondary advertising employed for e-mail communications. According to recent studies performed by *Pew Internet and* American Life *Project*, the vast majority of cloud computing services users declared serious concern relating to the feasibility of disclosure personal data by cloud computing service provider to others. The statistic reported that 90 % of cloud application users declared they would be very concerned if their personal data is used by the companies for marketing purposes and 68 % stated that they would be very concerned if their personal data such as their photo or other data analyzed and then displayed as an advertisement by the companies.

IV. CONCLUSION

The technology of cloud computing has expose challenge in protective personal information. We tend to conjointly mention some points for shield personal information in cloud computing. However, it's still potential for his or her actions to place their customers in breach of the information Protection Principles. It's so significantly vital once participating a cloud computing provider to require steps to minimize this risk, each in choosing a provider and negotiating a contract.

V. REFERENCES

[1] Peter Mell, Timothy Grance, "The NIST definition of Cloud Computing", National Institute of standards and technology, Special Publication No. 800-145, September 2011.

[2] Mark L. Badger, Timothy Grance and Other, "Cloud Computing Synopsis and Recommendations", National Institute of Standards and Technology, Special Publication No. 800-146, May 2012.

[3] US Government, Public Law 104-191 - Health Insurance Portability and Accountability Act of 1996, August 1996.

[4] US Government, Public Law No. 99-508. Electronic Communications Privacy Act of 1986,

[5] Jay Stanley, "The Crisis in Fourth Amendment Jurisprudence", The American Constitution Society, May 2010.

[6] Neil Robinson, Lorenzo Valeri, Jonathan Cave & Tony Starkey, "The Cloud: Understanding the Security, Privacy and Trust Challenges", RAND Corporation, April 2011.

[7] Aisling Duffy, "Cloud computing: Data protection issues" Shoosmiths LLP 2013, 30 Nov 2012. available at http://www.shoosmiths.co.uk/client-resources/legal-updates/Cloud-computing -Data-protection-issues-4314.aspx.

[8] Martin Gilje Jaatun, Gansen Zhao, Athanasios V Vasilakos, Åsmund Ahlmann Nyre, Stian Alapnes, Yong Tang, "The design of a redundant array of independent net-storages for improved confidentiality in cloud computing", Journal of Cloud Computing, July 2012.

[9] Abdolhamid Rouhani, Nazura Abdul Manap, "The Impact of Cloud Computing on the Protection of Personal Data in Malaysia", IPCSIT vol.45 pp 53-56 August 2012.