Efficient Framework Approach to Extract Privacy Issues in Cloud Computing

Sunny Singh, Nitin Goel
School of Computer Sciences
Chitkara University,
Rajpura, India
Er.singhsunny2207@gmail.com

***Abstract*— To overcome the challenges emerged in adoption of cloud computing technologies, many countries has conceived and designed data privacy and confidentiality protection regulations. The objective of this paper is to identify privacy issues and design a framework pertaining to privacy and confidentiality concerns in adopting cloud computing. It is imperative to note that privacy concern is increasingly important in the online world. The secure processing of personal data in the cloud is a huge challenge now a days. Such a framework and exploration can provide benefits to the all communities linked with cloud computing. It will help in better understanding of the privacy issues associated with cloud and will spark ideas and lead to further research on this subject whom may lead to the development of privacy regulations and/or the improvement of existing Regulations.**

***Index Terms*—CSP, Cloud Computing, Privacy Policy, Principle of Cloud, Public Cloud, Private Cloud**

I. INTRODUCTION

Cloud Computing is comparatively a new model in the IT world. It has-been defined by NIST, as the following: "Cloud computing is a model for enabling 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".
Cloud computing has four deployment models. Those are:
1) Public Cloud: In public cloud infrastructure is made available to general public and is owned and managed by CSP.
2) Private Cloud: In Private cloud, infrastructure is used by a single organization.
3) Community Cloud: In community cloud service the cloud infrastructure is used by several organizations belongs to specific community that has shared concerns.
4) Hybrid Cloud: In Hybrid cloud, cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public).

Cloud computing has essentially five main characteristics shown in the diagram:

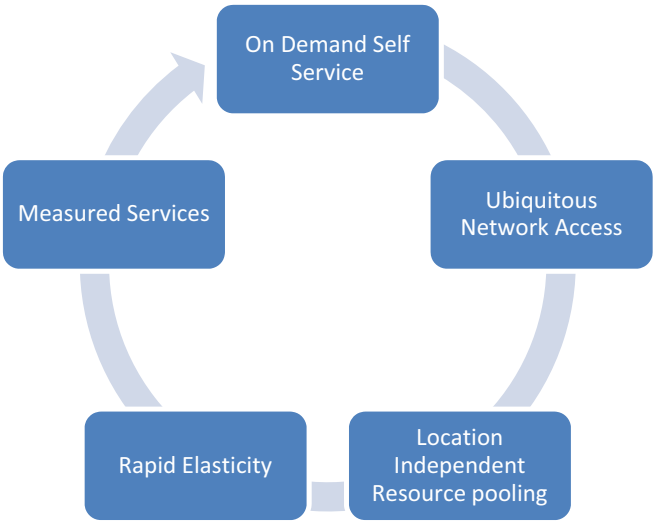

Figure 1: Characteristics of Cloud Computing

Privacy is a key issue in cloud computing. In general, privacy is about the accountability of a cloud provider to customer, as well as the transparency to cloud provider's practice around personal data/information. Cloud computing is a rising technology in the field of Information Technology. Therefore, it is of preeminent importance to deal with issues and challenges of privacy. Offending and violation of privacy not only affects users but also cloud service provider because it maculates their credibility with customers. The concept of privacy varies widely among countries and jurisdictions.

II.METHODOLOGY USED

This main focus of the paper is to find or extract major privacy issues in cloud computing. The process includes:

978-1-4799-1797-6/15 $31.00 © 2015 European Union
DOI 10.1109/CSNT.2015.141

Figure 2: Extracting Privacy Issue in Cloud Computing

III: MAJOR PRIVACY CONCERNS

In the present time the way of managing the data on cloud has been changed. The customers have lost their control over the data and depend on the cloud service provider. This change leads to a number of privacy concerns to be raised. Some of the privacy concerns had been discussed here and these are as follows:

1. Compliance: It indicates the list of applicable laws, regulations, standards and contractual commitments that govern cloud computing data. The privacy laws for different jurisdiction may vary so it is required what is the relevant jurisdiction that governs data in the cloud computing.

2. Access: Access tells about the access rights of the user and the cloud service provider. That is how much access user has on data and the rights of CSP on the data.

3. Storage: Storage is linked to the physical location where the data is stored. Whether the data is stored locally or on foreign land. Whether cloud service provider having sufficient data centers or not. Storing data on the different location may lead to the unauthorized access.

4. Retention: This term is associated with time for which user's data is retained on the cloud. This simply means that for how much time a user can have access to the cloud.

5. Audit and monitoring: It means how customers can monitor their cloud provider and get assurance that privacy requirements are met when their personal data is on the cloud. This is one of the major concern in the cloud computing.

6. Destruction: It is the process of deleting of personal data at the end of the retention period and to ensure that the personal data is destroyed and is not available to another cloud user.

7. Privacy breaches: It means how to know about breach has occurred and ensures that the cloud provider will notify customer when a breach occurs, and who is responsible for managing the process of notifying breaches. Breach simply means violation and infraction of data by the eavesdroppers.

8. Law: As technology is changing day by day the laws should also be updated so that it can provide full fledge security. The cloud provider should establish transparent policies to customer so that customers can easily understand them.

All of the above are major concerns which have to be taken into the consideration for the development of the framework in cloud computing.

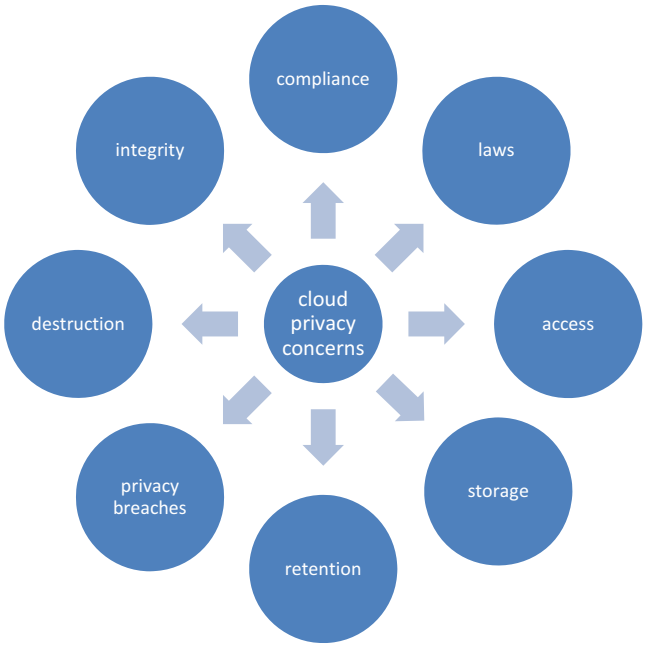

Figure 3: Figure Representing the Cloud Privacy Concerns

II. RELATED WORK

To further find out the privacy issues and concerned privacy principals number of privacy framework which are accepted in various countries of the world has been referred. Those frameworks are:

a) **"U.S-EU Safe Harbor" is** a framework that developed in order to cover up the differences in approach of privacy that is taken by U.S and that has taken by the EU, when data is being transferred from the EU to U.S. "U.S-Swiss Safe Harbor" is a framework to bridge the differences in privacy approaches between the U.S and Switzerland. Many cloud providers comply with this framework, ex: Google, Amazon, HP etc.

b) **"NSTIC2 Fair Information Practice Principles** (FIPPs)": It is a widely accepted framework and is followed by many U.S states , as well as many foreign nations and international Privacy Framework .

c) **"ISO/IEC29100"**- This privacy framework includes International Standard to protecting the personal identifiable information (PII) within information and communication technology (ICT) systems.

VI.THE EXTRACTED PRIVACY PRINCIPLES

By taking the reference from all the above policy frameworks following privacy principles have been extracted.

1. Collection limitation:
It means that the cloud provider should collect the personal data according to the customer's service needs.

2. Consent and Choice:
It means that the cloud provider should get separate consent from a user before collecting the data and before processing that data and customers should have the freedom to withdraw their consent easily and without any harm in terms of efforts and funds.

3. Collection Methods:
It means that the data collection should be lawful and fair.

4. Data Integrity:
It is the duty of cloud provider that data should always be accurate, complete, and current, for all copies.

5. Data minimization:
It means the one should be given access only to the data necessary to do his/her official duties.

6. Use and retention limitation:
It means that the cloud provider should limit the use, retention of personal data to that is necessary to fulfill the specific purposes and data should be completely deleted when retention time is complete.

7. Disclosure and transfer data:
It means that the cloud provider should disclose and transfer personal data to minimum extent possible. And when personal data are transferred internationally the cloud service provider should deal with the necessary processes.

8. Notice and openness:
It means that the cloud provider should be open in terms of its practices and policies regarding to collect, use and processing of personal information; and let it available to the public.

9. Rights and access:
According to this principal CSP should give user the right to access, process and use the data as per need.

10. Security safeguards and encryption:
It means that the cloud provider should be responsible to safeguard personal data with appropriate methods and mechanisms to ensure the integrity, confidentiality and availability of personal data.

11. Accountability and auditing:
It means that the cloud provider should be responsible for its Policies and actions to comply with applicable law, audit and risk assessments for the actual use of personal data with applicable privacy protection requirements.

.12. Compliance:
It means that the cloud provider should indicate all of Applicable laws, regulations and standards that it complies with them.

13. Physical Location:
It means the user should be aware of the actual location of the data and server of CSP. On the basis of above analysis we have found that following are the framework and their respective privacy concerns covered.

Table 1: Table representing the privacy principle

Privacy principles in international framework			
PRIVACY PRINCIPLE	NSTIC FIPPS's	U.S-E.U SAFE HARBOUR	ISO/IEC 29100
COLLECTION LIMITATION	√		√
CONSENT AND CHOICE	√	√	√
COLLECTION METHODS			
DATA INTEGRITY	√	√	√
DATA MINIMIZATION			√
RETENTION AND USE	√	√	√
DISCLOSER AND TRANSFER	√	√	√
NOTICE AND OPENNESS	√	√	√
RIGHT AND ACCESS	√	√	√
SECURITY AND SAFEGUARD	√	√	√
ACCOUNTABILITY AND AUDITING	√	√	√
COMPLIANCE	√	√	√
PHYSICAL LOCATION	√	√	√

The table shown above represents the analysis of different framework studied and relatively covered all the privacy principles.

III. CONCLUSION AND FUTURE WORK

In this paper we have tried to cover up all the related privacy concerns related to the cloud computing and that will help cloud service provider to serve the customers in a better way by covering all of these issues. In future we are considering that we will be able to make new frameworks by combining the perspectives of all the above covered frameworks and will be able to serve as a better cloud service provider. The concept of transparency will be prior for those frameworks which have been made with user's perspective point of view and level of privacy will depends upon the level of transparency.

REFERENCES

[1].J.Ruiter , & M.Warnier (2010). Privacy Regulations for Cloud Computing. *TU Delft*.

[2].M.Zhou, R.Zhang, W.Xie, W.Qian, & A.Zhou (2010, November). Security and privacy in cloud computing: A survey. In *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on* (pp. 105-112). IEEE.

[3].Q.Kuyoro'Shade, I.Frank, & A.Oludele,(2011). Cloud Computing Security Issues and Challenges.

[4].W.A.Jansen, (2011, January). Cloud hooks: Security and privacy issues in cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1-10). IEEE.

[5].M.A. AlSudiari, &T.G.K. Vasista, (2012). Cloud computing and privacy regulations: an exploratory study on issues and implications. *Int J Adv Comput (ACIJ)*, *3*(2), 159-162.

[6].P.You, Y.Peng, W.Liu,& S.Xue, (2012, June). Security issues and solutions in cloud computing. In *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on* (pp. 573-577). IEEE.

[7].H.Tianfield,2012, October). Security issues in cloud computing. In *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on* (pp. 1082-1089). IEEE.

[8]. D.Chen, &H. Zhao,(2012, March). Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 1, pp. 647-651). IEEE.

[9].A. Behl, &K. Behl, (2012, October). An analysis of cloud computing security issues. In *Information and Communication Technologies (WICT), 2012 World Congress on* (pp. 109-114). IEEE.