Volume 4, No. 4, March-April 2013
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Privacy Issues and Measurement in Cloud Computing: A Review

Ishan Rastogi*, Adesh Chandra
Dept. of Cyber Law & Information Security
Indian Institute of Information Technology Allahabad
Allahabad, India
ims2011002@iiita.ac.in*, adesh.004@rediffmail.com

Vivek Kumar Gupta, Dr. Abhishek Vaish
Dept. of Cyber Law & Information Security
Indian Institute of Information Technology Allahabad
Allahabad, India
ims2011003@iiita.ac.in, Abhishek@iiita.ac.in

Abstract: Cloud computing is the future of computing technology, with both the computing power and the data to be processed lying in a distributed environment. However, this nature of cloud computing has raised several concerns related to privacy issues. In this paper we first review various privacy issues related to cloud computing discussing the challenges to privacy in cloud computing, their causes, and effects. Then we review various laws, standards and regulations which are in place to check these issues in different countries and the principles of privacy they adhere to. Finally, we provide a method to calculate the privacy ranking for any cloud provider, aimed at helping a customer to select from different cloud providers.

Keywords: Cloud Computing, Privacy, Privacy Issues, Privacy Impact, Privacy Ranking, Privacy Risk

I. INTRODUCTION

Cloud computing is a new paradigm in the evolution of Information Technology. For some, it is one of the biggest revolutions in the field of information technology to have taken place in recent times, while for others; it is just a step towards the aim of utility computing.

Cloud computing is not itself a new technology but, merely a new way of delivering the computing resources.

The key characteristics of cloud computing are [1]:

a. Multi-tenancy
b. Agility
c. Performance
d. On-demand Self-service
e. Low Cost
f. Device Independence
g. Virtualization
h. Application Programming Interface
i. Reliability
j. Elasticity
k. Location Independence
l. Maintenance
m. Scalability

According to NIST the Cloud computing model can be categorized into three cloud service models, and four cloud deployment models.

Cloud Service Models are:

a. Software-as-a-Service (SaaS): in this delivery model, entire software and its associated data are hosted centrally on the cloud. It is also known as "on-demand software".
b. Platform-as-a-Service (PaaS): in this delivery model, a computing platform and a solution stack is provided as a service. Consumers develop software by using the libraries provided.
c. Infrastructure-as-a-Service (IaaS): in this delivery model, infrastructure in the form of virtual machines is provided as service. The consumers are free to install whatever operating system and applications they may require.

Cloud Deployment Models are [2]:

a. Public Cloud Model,
b. Private Cloud Model,
c. Hybrid Cloud Model,
d. and Community Cloud Model

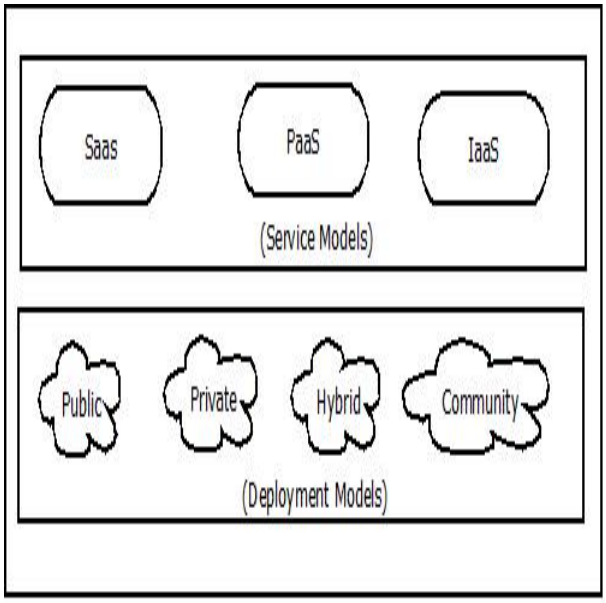

Figure 1: NIST Model of Cloud Computing

However, these features have led to some security risks to cloud computing. The presence of huge computing resources and humongous amount of data has made cloud environment a lucrative target for hacker.

Also, the cloud computing environment has raised various privacy concerns as well because the consumers believe that they have lost control on the data which they have stored in the cloud.

In the following sections we discuss various issues related to privacy in cloud computing, various laws and regulations, do a risk assessment and then provide a model to compute privacy ranking for a cloud .

II. PRIVACY ISSUES IN CLOUD COMPUTING

Privacy could be understood as the right of a person to have his personal data properly secured. Any data that could uniquely identify a person or, which is not supposed to be known to any person other than its owner and/or her immediate family, without her consent is called Private Data.

It is therefore needed to maintain the confidentiality of private data.

However, current cloud services usually cause this data to be exposed, on a machine owned and operated by an organization which is different from the data owner, in unencrypted form. The major privacy issues in cloud computing environment relate to:

a. Trust
b. Uncertainty
c. Compliance

The most common issues related to privacy in cloud computing environment are [3-6]:

A. Lack of User Control:

Complete control of user on the data is not possible in the cloud, since both the visibility and control of a user is reduced as soon as the cloud environment is used. The key aspects here are, that in cloud computing the personal data of a person is present on machines which are not owned or controlled by him/her, and therefore, there is the threat of the data being stolen, misused or even resold without authorization.

It is also not always possible for a cloud service provider to ensure that a person is able to access all of his personal data, what is the current location of the data, and what is currently being done with the data. It is also difficult to control the exposure of the data since many law enforcement agencies monitor the traffic flowing through their countries.

There is also a risk of insecure deletion of data. A cloud service provider may not guarantee complete and safe removal of data on receiving a deletion request.

Provider lock-in is also a concern for any consumer, i.e. it is not easy to change the cloud service provider, as it is extremely difficult to get the data back from the cloud.

It is very difficult to know which privacy breaches have already taken place and which are going to happen because of uncertainties regarding notifications. It is also difficult to identify the person at fault for such breaches.

B. Lack of Training and Expertise:

The deployment and running of cloud services requires high skill jobs, but the unavailability of highly skilled people is a serious issue from the point of view of information security. Employees may also not understand the consequences their decisions could have on privacy. The rise of technology has also worsened the scenario, as more employees are now able to cause such privacy issues which may have far-reaching consequences. Therefore, it is essential to have proper management procedures in place like trainings etc. otherwise there are chances that employees may switch to cloud computing environment without considering the risks and its consequences.

C. Unauthorized Secondary Usage:

The risk of unauthorized use of data either stored or processed in the cloud is always present. The authorized secondary usage of any user's data by the service provider to gain revenue is part of standard business model. However, the data could also be used in a way which is unacceptable to the user. Therefore, it is necessary for the cloud service providers and the customers to enter into a legally binding agreement which explicitly mentions as to how and up to what extent the data of a customer could be used. This will also enhance the trust between the customer and the cloud service provider.

D. Complexity of Regulatory Compliance:

The global and distributed nature of cloud computing environment and the many laws present in different places around the world has made it very complex and difficult to ensure that all the laws and regulations which are applicable in a given case are complied with.

What makes this complex is that in cloud computing environment the same information could be sometimes be in different locations at the same time. It is difficult to even know exactly where the data is or if it is in transit at any given time. Another factor which complicates the compliance issue is the presence of multiple copies of same data in the cloud, and each of these copies may be managed by different entities.

The main properties which make compliance difficult are:

a. Data Proliferation: This is the feature of cloud computing in which, to ensure the availability of some data, the cloud providers replicate that data in multiple locations. This happens in such a way that multiple parties may be involved. It cannot be guaranteed that the data or its copies are not processed or stored in some certain jurisdictions. Deletion of all the copies of data upon receiving such request can also not be guaranteed. Therefore, any cloud computing service which involves both outsourcing and offshoring may raise some very complex and serious issues.
b. Dynamic Provisioning: The problems related to outsourcing which cloud computing environment faces are quite similar to that in traditional outsourcing, but the dynamic nature of cloud computing environment makes many of the existing provisions which address these issues in static environment obsolete. It is not yet clear as to which party will be held responsible for ensuring that proper legal requirements of private data are met, or whether or not appropriate data-handling standards and procedure are followed.

E. Transborder Data Flow:

Privacy laws and data protection regulations restrict the flow of private data outside the national borders, restricting not only the physical transfer of data but also remote access to the data. All countries having national legislations have restricted such transfers.

Personal information however can be transferred between some countries, if either some model contracts have been signed and approved by country regulator, or if the owner of the data has given his free consent. Model contracts are agreements containing data protection commitments, liability requirements of the company and the liability to the concerned individuals.

However model contracts are not very well suited to the cloud computing environment. The main reasons being: the uncertainty in cloud computing environment and the

regulatory complexity, and the factor that this technique is not flexible enough for cloud, as approving model contracts and obtaining regulatory approval may result in long delays.

Trade sanctions and export restrictions may also restrict the transfer of personal data across the national borders.

Therefore, it is very difficult to understand which laws will apply when the routes of information flow are not known.

Even if transit of information is not considered, enforcing transborder data transfer regulations in the cloud computing environment is still very difficult.

F. Litigation:

A government may force a cloud service provider to give them the data stored in the cloud. All they have to do is to show that the requested data is relevant to some case for a subpoena.

To avoid similar situations at the hands of some non-governmental entities, the contract between the cloud service provider and the cloud subscriber should include provisions that decide the response of the cloud service provider upon receiving any such subpoena requests.

G. Legal Uncertainty:

Legal frameworks have played very important role in the protection of the personal and sensitive information of any user. The basic concepts of such legal frameworks are generally technology neutral, and therefore they would still be applicable on cloud computing environment. Still these frameworks need to be updated keeping the current and future technologies in consideration. The dynamic nature of cloud computing environment combined with various trans-border interactions have introduced legal aspects which must be considered carefully while processing the data.

However, there are legal uncertainties regarding the right of privacy in cloud computing environment. Legal frameworks are yet to decide as to whether encrypting the private data may be considered as processing, and how to guarantee that the processed data is private data or not.

All these challenges have not yet been addressed in any legal frameworks and therefore the uncertainties regarding the legal situations still remain.

III. PRIVACY PRINCIPLES, LAWS AND REGULATIONS

In this section, an overview of some of the most important privacy laws which are applicable to cloud computing in the European Union and the United States of America is provided.

A. EU Directive 95/46/EC

It is also called the Data Protection Directive. Its main purpose was to provide a basic standard for the protection of privacy across all the member states of European Union.

This directive deals with personally identifiable information (PII), or personal data. The directive defines that the responsibility for compliance is with the data controller, i.e. with the person who decides how the personal data is processed and stored. The data controller may outsource the processing of the data to a data processor. If the data controller is not in the EU but the data processor is, then it is the responsibility of the data processor to comply with the directive.

The main motive behind this directive was to protect the private information of the residents of EU [7].

B. The Safe Harbor Agreement:

This agreement is only applicable between the EU and the USA. Those organizations in USA that want to do business in EU have to follow this agreement, so that they may adhere to the strict rules in Directive 95/46/EC.

The Safe Harbor Agreement allows those organizations to have business relations with EU, who:

a. Notifies the individuals that their data is collected.
b. Provides the individuals with a choice to opt-out from data collection.
c. Transfers the data only after getting explicit permission of the individual concerned.
d. Maintains security of the data.
e. Maintains the integrity of the data.
f. Provides the individuals with the right to access their data [8].

C. The FTC Fair Information Practice:

It provides with a set of guidelines pertaining to the fair use of personal information of individuals. The FTC Fair Information Practice act contains the following principles:

a. Notice/Awareness
b. Choice/Consent
c. Participation/Access
d. Security/Integrity
e. Enforcement/Redress

These principles, with the exception of Transborder Transfer principle, are same as the principles in the Directive 95/46/EC [9].

D. Other Privacy Regulations:

Few other privacy related regulations in USA are:

a. Health Insurance Portability and Accountability Act
b. The Fair Credit Reporting Act
c. The Gramm-Leach-Bliley Act
d. USA PATRIOT Act
e. Payment Card Industry Data Security Standard

The following is a summary of various privacy laws, standards and regulations which are applicable to the cloud computing environment [10, 11].

E. Compelled Disclosure to the Government:

In USA:

a. Electronic Communications Privacy Act
b. USA Patriot Act
c. Stored Communications Act
d. FTC Fair Information Practice

In UK:

e. The Regulation of Investigatory Powers Act

In India

f. RTI Act 2005

F. Data Security and Disclosure of Breaches:

In USA:

a. Family Educational Rights and Privacy Act
b. Health Insurance Portability and Accountability Act
c. Sarbanes Oxley
d. Gramm-Leach-Bliley Act
e. Section 5 of FTC Act
f. State Laws and Regulations

In UK:
a. Data Protection Act 1998
b. Directive 95/46/EC
c. The Privacy and Electronic Communications Regulations 2011

In India:
a. IT Act 2005 and amendments of 2008 can be helpful

G. Data Accessibility, Data Transfer and Data Retention:

In US:
a. FTC Fair Information Practice
b. Freedom of Information Act
c. Payment Card Industry Data Security Standard

In UK:
a. The Safe Harbor Agreement

In India:
a. RTI Act 2005 can be helpful

H. Location of Data:

In US:
a. FTC Fair Information Practice
b. Sarbanes Oxley
c. Payment Card Industry Data Security Standard

In UK:
a. Directive 95/46/EC

In India:
a. IT Act 2008 can be helpful

IV. RISK ESTIMATION

This section tries to estimate the risk value associated with the privacy issues already discussed in the sections above.

Risk can be calculated by using the formula:

$$Risk = Probability \times Impact \quad (1)$$

Therefore, for calculation of risk it is absolutely critical to estimate the impact which an adverse event may have on any organization and the probability of that event to actually occur.

The impact in itself is dependent on various factors such as: loss of productivity, loss to the assets, loss of reputation, loss of competitive advantage, loss due to fines etc.

Basically the impact which an organization suffers is based on the size and the maturity scale of the organization. The following table provides a basic idea to help in assigning monetary value to a risk [12]. This scale is flexible as different organizations have different tolerance and loss bearing capacity.

Table 1: Risk Categorization

Magnitude	Probable Loss
Severe	>$10,000,000
High	$1,000,000- $9,999,999
Significant	$100,000- $999,999
Medium	$10,000- $99,999
Low	$1,000- $9,999
Very Low	<$1,000

The impact and probability will also be affected by the type of cloud deployment model and the type of cloud service model.

Cloud Service Model:
a. SaaS: Impact = Low
b. PaaS: Impact = Medium
c. IaaS: Impact = High

Cloud Deployment Model
a. Private: Impact = Low
b. Community: Impact = Medium
c. Hybrid: Impact = High
d. Public: Impact = Very High

We now calculate risks for some privacy related issues, and just like the table above, this calculation may vary between organizations [13, 14].

A. Lock-In:
a. Severity: Medium
b. Probability: High
c. Risk: High

B. Loss of Governance:
a. Severity: Very High
b. Probability: Very High
c. Risk: High

C. Challenges of Compliance:
a. Severity: High
b. Probability: Very High
c. Risk: High

D. Dynamic Provisioning:
a. Severity: High
b. Probability: Medium
c. Risk: High

E. Failure of Isolation:
a. Severity: Very High
b. Probability: Medium
c. Risk: High

F. Abuse of High Privilege:
a. Severity: Very High
b. Probability: Medium
c. Risk: High

G. Intercepting Data in Transmission
a. Severity: High
b. Probability: Medium
c. Risk: Medium

H. Data Leakage:
a. Severity: High
b. Probability: Medium
c. Risk: Medium

I. Insecure Deletion of Data:
a. Severity: Very High
b. Probability: Medium
c. Risk: Medium

J. Subpoena and E-discovery:
a. Severity: Medium
b. Probability: High
c. Risk: High

K. Risk from Jurisdictional changes:
a. Severity: High
b. Probability: Very High
c. Risk: High

L. Risks related to Data Protection:

a. Severity: High
b. Probability: High
c. Risk: High

V. PRIVACY RANKING

This section provides a method to calculate the privacy rankings of various cloud providers, so that a customer can select between different cloud service providers present in the market.

The method calculates the Privacy Ranking of a cloud provider based on the privacy risk values (as calculated in Section 4), the compliance status of the cloud service provider for each privacy issues to various laws and regulations and the level of control which is being provided by the cloud service provider to the customer on the data.

$$PR = \sum R_i \times C_i \quad (2)$$

Where, PR is the Privacy Ranking of the cloud service provider; R*i* is the risk associated with individual privacy issues when selecting this cloud service provider; C_i is the completion status of cloud service provider's compliance.

To calculate the privacy ranking for a cloud service provider we first need to rank each individual risk (R_i) on a scale from 1 to 6. The higher the magnitude of risk the higher its rank and the lower its contributing factor towards the privacy ranking estimation.

Table 2: Risk Ranking

Magnitude	Probable Loss
Severe	1
High	2
Significant	3
Medium	4
Low	5
Very Low	6

Completion Status (C_i)

Completion Status can itself be divided into two factors:

a. Compliance Level of Cloud Service Provider (S_i): this factor measures the level of compliance of the cloud service provider for every privacy issue, i.e. the concerning laws, regulations and standards followed by the cloud service provider.

The compliance level of any organization can be estimated by performing a full-scale Privacy Impact Assessment (PIA). In a PIA process, the compliance level of any cloud service provider is estimated on the basis of a set of specifically designed questionnaire [15].

Table 3: Compliance Ranking

Compliance Level	Compliance Ranking
Very Low	1
Low	2
Medium	3
High	4
Very High	5

b. Control Level Offered to the Customer (Ui): this factor measures the level of control which a cloud service provider offers to the customer on the data as per the service level agreement

Table 4: Control Ranking

Control Level	Control Ranking
Very Low	1
Low	2
Medium	3
High	4
Very High	5

The Completion Status (C_i) can now be calculated by using the following table:

Table 5: Completion Level

	VL	L	M	H	VH
VH	M	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	VL	L	L	L
VL	VL	VL	VL	VL	VL

Horizontal Axis: Compliance Level (S_i)
Vertical Axis: Control Level (U_i)

Table 6: Completion Ranking

Completion Level	Completion Ranking
Very Low	1
Low	2
Medium	3
High	4
Very High	5

Now, that the completion status is calculated the privacy ranking can be found out using equation 2.

This privacy ranking can then be used to select from multiple cloud service providers. Now if privacy ranking of cloud service provider A is PRA and the privacy ranking of cloud service provider B is PRB, then if:

a. PRA > PRB : select cloud service provider A
b. PRA < PRB : select cloud service provider B
c. PRA = PRB : then if,
d. $\sum R_i(A) > \sum R_i(B)$: select cloud service provider A
e. $\sum R_i(A) < \sum R_i(B)$: select cloud service provider B

VI. CONCLUSION

In the end it can be concluded that though cloud computing offers various benefits and is surely the way of the future, but still it has some security related issues which are discouraging people from fully utilizing its potential. It is therefore required to have better laws which can tackle the problems such as trans-border flows and better technological solutions which help in anonymizing the private data and protect the privacy of a person.

VII. REFERENCES

[1] Cloud computing - Wikipedia, the free encyclopedia. (n.d.). Wikipedia, the free encyclopedia. Retrieved February 10, 2013, from http://en.wikipedia.org/wiki/Cloud_computing.

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft).NIST special publication, 800, 145.

[3] Pearson, S. (2012). Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing, 3-42.

[4] Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud!: privacy concerns for consumer cloud storage. InProceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM.

[5] ComPUtING, C. (2011). Cloud computing privacy concerns on our doorstep.Communications of the ACM, 54(1).

[6] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. Security & Privacy, IEEE, 8(6), 24-31

[7] Cotino, L. ARTICLE 29 DATA PROTECTION WORKING PARTY.

[8] Industry. (n.d.). Export.gov - Safe Harbor Privacy Principles. Export.gov - Home. Retrieved February 12, 2013, from http://export.gov/safeharbor/eu/eg_main_018475.asp

[9] Reidenberg, J. R. (1994). Setting Standards for Fair Information Practice in the US Private Sector. Iowa L. Rev., 80, 497.

[10] AlSudiari, M. A., & Vasista, T. G. K. Cloud Computing And Privacy Regulations: An Exploratory Study On Issues And Implications. Advanced Computing: an International Journal, 3.

[11] Ruiter, J., & Warnier, M. (2011). Privacy regulations for cloud computing: Compliance and implementation in theory and practice. Computers, Privacy and Data Protection: an Element of Choice, 361-376.

[12]] Jones, J. (2006). An introduction to factor analysis of information risk (fair).Norwich Journal of Information Assurance, 2(1), 67.

[13] Cloud Computing Risk Assessment — ENISA. (n.d.). ENISA. Retrieved February 10, 2013, from http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[14] Saripalli, P., & Walters, B. (2010, July). Quirc: A quantitative impact and risk assessment framework for cloud security. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on (pp. 280-288). IEEE.

[15] Tancock, D., Pearson, S., & Charlesworth, A. (2010, November). A privacy impact assessment tool for cloud computing. In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on (pp. 667-676). IEEE.

[16] Wang, J., Zhao, Y., Jiang, S., & Le, J. (2009, December). Providing privacy preserving in cloud computing. In Test and Measurement, 2009. ICTM'09. International Conference on (Vol. 2, pp. 213-216). IEEE.

