ISSN:0975-9646

A Framework for Enhancing Privacy Provision in Cloud Computing

Fatima N. AL-Aswadi & Omar Batarfi

Faculty of Computing and Information Technology,

King Abdulaziz University, Jeddah, Saudi Arabia

Abstract: Cloud computing is considered a new generation of technology that has offered many benefits such as flexibility, efficiency, reduction in IT cost and so on. However, the dependence on the cloud provider to process and manage the personal data leads to many privacy and confidentiality risks. . In this paper, we propose a framework that aims to evaluate if the cloud provider meets the privacy related issues. Moreover, this proposed framework helps the cloud provider to enhance the privacy provision level to increase the trust of customers on cloud provider services.

Keywords: cloud computing, privacy framework, privacy concerns, personal data.

I. INTRODUCTION:

Cloud Computing is a new model in the IT's world. It has been defined, according to NIST[1], 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."*[1].

Under this definition, the cloud computing model has five essential characteristics that are on-demand self service, ubiquitous network access, location-independent resource pooling, rapid elasticity and measured service [1,2]. And it has three delivery service models they are (1) Software as a Service (SaaS): - it means using provider's applications over a network [2,3]; (2) Platform as a Service (PaaS): - it means deploying customer-created applications to a cloud computing [2]; (3) Infrastructure as a Service (IaaS): - it deals with rent processing, storage, network capacity, and other fundamental computing resources [2,3].

In addition, the cloud computing has four deployment models, they are (1) Public cloud:- the cloud computing infrastructure is made available to the general public or a large industry group [1,2] and it is owned and managed by the cloud provider; (2) Private cloud:- the cloud infrastructure is dedicated to a single organization and it may be managed by the organization or a third party [1,2]; (3) Hybrid cloud:- the cloud computing infrastructure is a composition of two or more cloud computing types [1-3]; (4) Community cloud:- cloud infrastructure is shared by several organizations for specific community [2,3].

[1] National Institute of Standards and Technology- U.S

Privacy is a key issue in cloud computing. Infringing and violation of privacy for customers adversely affect not only customers but also a cloud provider because it weakens their credibility with customers. The concept of privacy varies widely among countries, cultures and jurisdictions [4]. 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 [4].

Many customers of cloud computing have worried about their private or sensitive data from theft, disclosure or from illegal use by cloud providers or others and so on. Furthermore, cloud provider has many available physical locations of data centers throughout the world this lead to a new challenge in maintaining the data protection required by current legislation including restrictions on cross-border data transfer [5].

In this paper we will concentrate on different processes that are used to finally to extract the major principles of privacy in cloud computing. These process including: 1- Defining and studying the privacy concerns in cloud computing; 2- Studying and comparing among widely accepted international privacy frameworks; 3- Extracting the important privacy principles for cloud computing; and 4- Optimizing the privacy principles to find the optimal solution for the problem.

The rest of this paper is organized as follows: Section 2 presents a data life cycle. Section 3 explains the privacy concerns in cloud computing. Section 4 shows the related works. Section 5 defines the privacy principles in cloud computing. Section 6 explains the extracted privacy principles and finally in Section 7 we discuss and conclude our work.

II. DATA LIFE CYCLE:

Protection of personal data should consider the impact of the cloud computing on each of the data life cycle phases [4]. Figure 1 shows the seven phases of data life cycle, according to KPMG (KPMG is a global network of professional firms providing Audit, Tax and Advisory services. They are mostly involved with the management of personal information of the customer [3])

1. **Generation of data phase:**

It means that the cloud provider should know who is the owner of personal data? And how is the ownership maintained?

2. **Use phase:**

Does the personal data used only in cloud provider or it is shared with third parties? Does the use of the data consistent with the purpose that it was collected for?

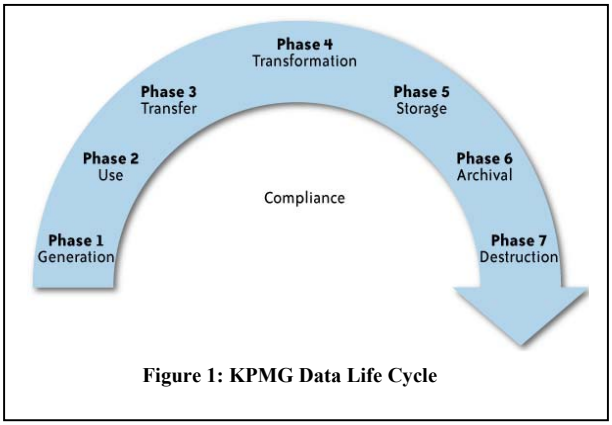

Figure 1: KPMG Data Life Cycle

3. Transfer phase:

When data is transferred to a cloud computing by using public networks, Are there appropriate protection and access controls, and is it encrypted? In other words, is there a chance to intercept data during the transfer? [3].

4. Transformation phase:

During the process of transferring the data, the integrity of data should be ensured for every user (checking if there any intruder during the transfer process)

5. Storage phase:

Restrict the availability of access to data and storage by appropriate access control mechanism, maintain confidentiality of data by use of encryption, and maintain integrity and availability of data.

6. Archival phase:

It determines the period that the cloud provider will retain the data.

7. Destruction phase

The cloud provider destroys personal data that obtained from the customer in a secure manner, and ensure that this destruction is complete and the data can not be recovered.

III. PRIVACY CONCERNS:

In cloud computing, the way to manage the data has been changed. The customers loss of control over their data and dependence on the cloud provider [6]. This changing leads to a number of privacy concerns. Figure 2 shows the key privacy concerns in cloud computing.

1. Compliance:

It indicates to what are the list of applicable laws, regulations, standards and contractual commitments that govern cloud computing data? [3, 4]. Cloud computing is crossing multiple jurisdictions; and the privacy legislation is not even similar in many jurisdictions around the globe [6]. What is the relevant jurisdiction that governs data in the cloud computing and how is it determined? [4].

2. Access:

Cloud provider has the ability to access the customer's data in the cloud [3]. If the customer exercises his right to ask to delete his data, will it be possible to ensure that all of his data have been deleted in the cloud computing? [4].

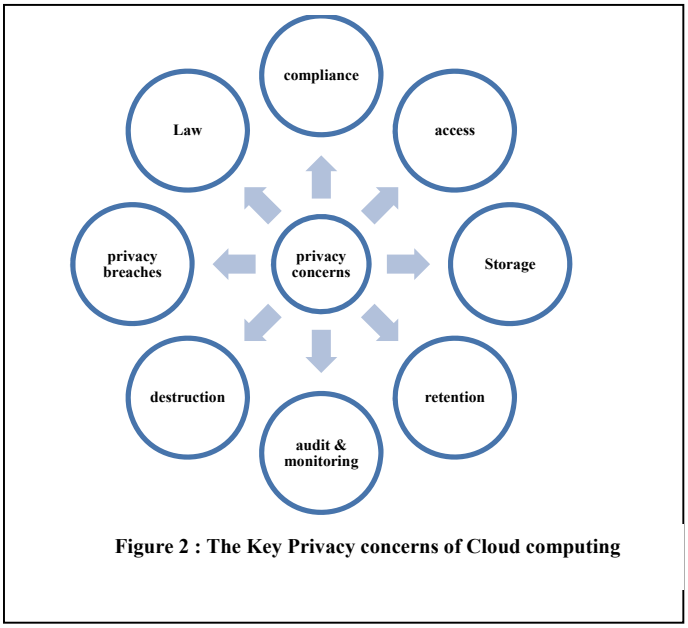

Figure 2 : The Key Privacy concerns of Cloud computing

3. Storage:

It indicates to where is the physical location that the customer's data is stored in the cloud computing. Storing data in different data centers in different locations, may lead to unauthorized access and uses [3]. There is a lack of transparency for customers on their data [6], the cloud providers do not give proper assurance for the transparency of data [3].

4. Retention:

It means how long are personal data retained in cloud computing? Which retention policy governs the data? [4] And who enforces this policy in the cloud computing? The stored data must be deleted automatically after the completion of the specified duration [3].

5. Audit and monitoring:

It means how can customers monitor their cloud provider and get assurance that privacy requirements are met when their personal data is in the cloud computing?

6. Destruction:

It means how does the cloud provider destroy personal data at the end of the retention period? [4] How ensure that the personal data is destroyed and it is not available to another cloud user? How know that the cloud provider did not retain additional copies? Did the cloud provider really destroy the data, or just make it inaccessible? [4]. Increasing the availability is one of the benefits in cloud computing, this benefit turns into a burden when trying destroy all copies of data; it is impossible to guarantee a complete destruction. Therefore, it is difficult to enforce mandatory deletion of data [6].

7. Privacy breaches:

It means how know that a breach has occurred, how ensure that the cloud provider will notify us when a breach occurs, and who is responsible for managing the process of breach notification? [4]. The absence of identifying the breaches will cause a drawback in the business [3].

8. Law:

For every new day, the technology is improving than the previous day and the issues related to the technology change

with this improving. However, the law and regulations that govern these issues is not updated regularly [3]. The current privacy regulations are not enough to solve all the privacy issues related to Cloud computing [7]. The cloud provider should establish transparent policies to customer to can understand them clearly [3].

IV. RELATED WORK:

In [8], the authors designed a mapping framework for providing privacy assurance information to end users and building trust in the privacy practices of businesses and other entities while being practical for deployment in the current infrastructure. This system has been fully implemented as a part of the integrated prototype within PRIME (PRivacy and Identity Management for Europe). It is allowed for the end user to set baseline privacy practices for service providers to adhere to, and providing a means of retrieving information from the service provider in the common language to base their PII (Personal identifying information) release decisions.

In [9], the author assured that the privacy threats vary according to the type of cloud scenario so that the privacy must be taken into account when designing cloud computing services. They suggested key design principles (Notice, openness and transparency; Choice, consent and control; Scope/minimization; Access and accuracy; Security safeguards; compliance; Purpose; Limiting use – disclosure and retention; and Accountability), which must be taken into account when any software engineers are designing cloud computing services. The suggested principles in this study covered most the privacy concerns in cloud computing. However, this study did not cover the law concern, and there are some principles which are related to storage; audit and monitoring concerns that are also not covered such as : proactive measures, physical location, and isolation mechanisms.

In [5], the authors proposed an approach in procedural and technical solutions which are co-designed to demonstrate accountability as a path forward to resolving privacy and security risks within the cloud computing. The accountability refers to the process by which a particular goal – the prevention of disproportionate harm to the subjects of PII – can be obtained via a combination of public law (legislation, regulation), private law (contract), self-regulation and the use of privacy technologies (system architectures, access controls, machine readable policies). Accountability is not a substitute for data protection laws, it is a practical mechanism for helping reduce end user privacy risk and enhance end user control.

In [10], the author proposed a new privacy framework, for B2C (Business-To-Consumer) E-Commerce environment, to make interactive development of an agreement between the web user and the service provider until reaching the privacy terms which are agreed upon. The structure of this framework consists of three actors: web user, service provider, and the author, in this study, proposed a privacy model to establish a new actor called a Third Party Trusted Agency (TTPA). The third party trusted agency is a neutral agency trusted by the end users and the service providers equally. It provides a more trusted environment for the consumer. The author mentioned that the model, which he established or proposed, is just one of many that can be used to implement this privacy framework.

In [7] study, the authors explored the privacy concerns of cloud computing and showed the common principles in several privacy regulations (notice, choice/consent, access, integrity, security and enforcement). This study is an exploratory study on issues and implications of privacy regulations and cloud computing. The authors, in this study, concluded that, the current privacy regulations are clearly not enough to solve all the privacy concerns related to cloud computing. More matured awareness is required about both the concern and about the existing regulations and seems to become a good first step to remedy this.

In [3], the authors presented a survey on different privacy issues involved in the cloud service; they also provided some suggestions to the cloud users to select their suitable cloud services by knowing privacy policies of cloud providers. They indicated six different privacy constraints (Physical Location, Data Recovery, Access Right, Trans-border flow, Audit trails and Laws) that have to be extended to cloud provider's privacy policy (Low Level). However, these constraints have a some lack of detail to can use them to evaluate the cloud provider. Furthermore, this study did not address the way of collecting the customer data or which are the type and amount of data that collected from customers?

V. DEFINING PRIVACY PRINCIPLES IN CLOUD COMPUTING:

To define the main privacy principles for cloud computing, we used two steps, in step 1, we built a manual comparison among six widely accepted international privacy frameworks. While in step 2, we studied the compliance with the extracted privacy principles and if they stratify of the privacy concerns in a cloud computing environment.

Step 1:

We take six widely accepted international privacy frameworks. For instance, "U.S-EU Safe Harbor" is a framework that developed in order to bridge the differences in approach of privacy that is taken by U.S and that has taken by the EU, when transfer personal data from the EU to U.S [11]. "U.S-Swiss Safe Harbor" is a framework to bridge the differences in privacy approaches between the U.S and Switzerland, It has paralleled the "U.S-EU Safe Harbor" [12]. Many cloud providers comply with this framework, ex: Google, Amazon, HP and others.

We also take "NSTIC[2] Fair Information Practice Principles (FIPPs)" to study the privacy principles in U.S. FIPPs is a widely accepted framework that is at the core of the privacy Act of 1974 and is mirrored in the laws of many U.S states [13], as well as many foreign nations and international organizations. In additional, we take "OECD[3] Privacy Principles" [14] to study the privacy principles in the EU. Moreover, we take "APEC[4] Privacy Framework" [15] which is considered as the first

[2] National Strategy for Trusted Identities in Cyberspace, White House-Washington

[3] The Organization for Economic Co-operation and Development- EU

[4] Asia Pacific Economic Cooperation

international framework try to avoid barriers to transfer of data among the Asia Pacific region and their trading partners. It is consistent with the core values of the OECD.

Furthermore, we take "Madrid Resolution on International Privacy Standards" [16]. It is a document that was approved from over 50 countries at the closed meeting of data protection authorities, within the "31st International Conference of Data Protection and Privacy" in Madrid, 2009 [17]; to define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data. Finally, we also take "ISO/IEC 29100- Privacy framework" [18], which includes International Standard to protecting the personal identifiable information (PII) within information and communication technology (ICT) systems.

Figure 3 shows a snapshot of constructed table of manual comparison (we produced 41, A4 pages as a result of filling up the rows of the table with the content of the six international privacy frameworks). Table 1 shows the privacy principles in international privacy frameworks.

Figure 3: snapshot of the first page on the table

As it is observed from table 1, after we finished the comparison, we were concluded 14 privacy principles for cloud computing

Table 1: privacy principles in international privacy frameworks

Principle	NSTIC FIPPs	OECD privacy principles	U.S.-EU Safe Harbor & U.S-Swiss Safe Harbor	APEC privacy framework	Madrid Resolution on International Privacy Standards	ISO/ IEC 29100
Collection limitation	√	√		√		√
Consent and choice	√	√	√	√	√	√
Collection methods		√		√		
Data integrity	√	√	√	√	√	√
Data minimization					√	√
Use and retention limitation	√	√		√		√
Disclosure and transfer data	√		√		√	√
Notice, transparency and openness	√	√	√	√	√	√
Rights and access	√	√	√	√	√	√
Security safeguards and encryption	√	√	√	√	√	√
Sensitive data			√		√	√
Accountability and auditing	√	√	√	√	√	√
Purpose legitimacy and specification	√	√			√	√
Proactive measures				√	√	

Step 2:

By studying the data life cycle and the privacy concerns in a cloud computing environment, we summarize that:

Cloud computing environment has many characteristics and advantages. Shared resources (ex: hardware, database, memory, etc.) and multi-tenancy are most two of characteristics that define it [19]. The probability of isolation failures in Cloud services is considered higher than classic IT [19]. So that separated mechanisms for storage, memory and routing should be strict because any failure in it is leading to serious consequences.

The cloud computing resources are located in different regions of the world; the customers should have a right to know the place where their data is stored. That means the cloud provider should give the exact regional data center of the cloud for the data storage to customers [3]. In addition, the cyber law is not universal [3] and the concept of privacy varies widely among countries, cultures and jurisdictions [4]. For that, the cloud provider should furnish the applicable law when the data are crossing different borders [3].

From all the above, we conclude four additional principles required for privacy in cloud computing, they are: Isolation mechanisms, Compliance, Physical Location, and Trans-border Flow. At the end, we extracted 18 privacy principles for cloud computing that help the customer to evaluate the privacy level of their cloud provider and help cloud provider to enhance its privacy level.

VI. THE EXTRACTED PRIVACY PRINCIPLES:

1. Collection limitation:
It means that the cloud provider should collect the personal data that only needed to provide the specific service.

2. Consent and choice:
It means that the cloud provider should get explicit consent from a customer before collecting the data and before processing it; and should give to customers the freedom to withdraw their consent easily and without cost.

3. Collection methods:
It means that the cloud provider should collect the data from the customer by lawful and fair means

4. Data integrity:
It means that the cloud provider should always ensure that personal data is accurate, complete, and current, for all copies.

5. Data minimization:
It means that strictly minimizes the privilege of processing of personal data and access to it. In other words, 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 after the end of retention period should destroy or anonymize it, in secure and safe manner.

7. Disclosure and transfer data:
It means that the cloud provider should limit the disclosure and transfer of personal data to less extent possible. And when personal data are transferred internationally, the cloud provider should be aware any additional national or local requirements specific to cross-border transfers; before the transfer process.

8. Notice, transparency and openness:
It means that the cloud provider should be transparent and explain (in a clear language) its practices and policies regarding to collect, use and processing of personal data; and let it available to public. Also the cloud provider should notify its customers when any change in its practices or policies is occurring.

9. Rights and access:
It means that the cloud provider should give to customers (in a fast and efficient way without delay or cost) the right to access or correct or delete their personal data, for all copies; and the right to object to processing their personal data.

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

11. Sensitive data:
It means that the cloud provider should apply additional and stricter conditions for processing sensitive personal data.

12. Accountability and auditing:
It means that the cloud provider should be responsible for its practices and policies to comply with applicable law; and audit and risk assessments for the actual use of personal data with applicable privacy protection requirements, to discover the risk and vulnerabilities and then resolve them.

13. Purpose legitimacy and specification:
It means that the cloud provider should ensure that the purpose comply with applicable law and communicate the purpose to the customer before collected the personal data, by using clear language.

14. Proactive measures:
The cloud provider must be proactive, not reactive. That means the cloud provider should implement training program, privacy impact assessment before implementing new technologies of processing personal data or any new methods.

15. Isolation mechanisms:
It means that the cloud provider should have mechanisms of isolation more accurate and strict than existing isolation mechanisms, because the probability of isolation failures in cloud computing is very high and its impact for privacy protection is also very high.

16. Compliance:
It means that the cloud provider should indicate to the list of applicable laws, regulations, and standards that it complies with them; And to one or more supervisory authority (ex: seal programs) that ensure and monitor this compliance.

17. Physical Location:
It means that the cloud provider should show to the customers (without any reservation) the physical location of its data centers.

18. Trans-border Flow:
It means when the cloud provider transfer the personal data between different borders (that have different law and regulations), it should explain these differences to the customers and furnish the law that will use.

VII. DISCUSSION AND CONCLUSION:

In this study, we tried to establish a privacy framework for cloud computing to evaluate if the cloud providers meets the privacy related issues. And to help the cloud providers to increase the customer's trust on them by taking into account these proposed privacy principles when designing cloud services; and by expanding these proposed privacy principles in them policies to be transparent to their customers. The level of privacy depends on the level of transparency.

Table 2 shows the privacy concerns in cloud computing and the proposed privacy principles that solve them (we only write No. of principles).

Table 2: privacy concerns and related privacy principles

Concern	Principles
Compliance	12, 13, 16
Access	3, 9
Storage	4, 7, 10, 11, 12, 15
Retention	1, 2, 6, 9, 11, 17
Audit & monitoring	5, 12, 14
Destruction	1,5, 9, 10, 12, 17
Privacy breaches	8, 12, 15
Law	7, 8, 18

Finally, this study is considered as a step forward to enhance the privacy provision in cloud computing.

REFERENCES:

[1] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", NIST Information Technology Laboratory, 2009

[2] Ronald L. Krutz and Russell Dean Vines, " Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc., Indianapolis, Indiana, 2010, ISBN: 978-0-470-58987-8

[3] Dr. Arockiam L, Parthasarathy G and Monikandan S , "privacy in cloud computing: a survey", SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 321–330, 2012. DOI : 10.5121/csit.2012.2331

[4] Tim Mather; Subra Kumaraswamy and Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media, Inc. 2009, ISBN-13: 978-0-596-80276-9

[5] Siani Pearson and Andrew Charlesworth. 2009. "Accountability as a Way Forward for Privacy Protection in the Cloud". In Proceedings of the 1st International Conference on Cloud computing (CloudCom '09), Martin Gilje Jaatun, Gansen Zhao, and Chunming Rong (Eds.). Springer-Verlag, Berlin, Heidelberg, 131-144, 2009

[6] Marko Hölbl, "Cloud Computing Security and Privacy Issues", CEPIS 2011, LSI SIN (10)02 , Version V17/15.03.2011

[7] Dr. Mohammed A. T. AlSudiari & Dr. TGK Vasista ," cloud computing and privacy regulations: an exploratory study on issues and implications", Advanced Computing: An International Journal (ACIJ), Vol.3, No.2, March 2012

[8] Tariq Ehsan Elahi and Siani Pearson; "Privacy Assurance: Bridging the Gap Between Preference and Practice", Trust, Privacy and Security in Digital Business Lecture Notes in Computer Science, 2007, Volume 4657, 65-74.

[9] Siani Pearson, "Taking account of privacy when designing cloud computing services," icse-cloud, 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009, pp.44-52.

[10] Murthy V. Rallapalli; " A Privacy Agreement Negotiation Model in B2C E-Commerce Transactions"; International Journal of Information Security and Privacy, October-December 2011, volume 5(4), 1-7.

[11] U.S.-Export.gov ,"Safe Harbor Privacy Principles", Available: http://export.gov/safeharbor/eu/eg_main_018475.asp

[12] FTC , "Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks" , Available: http://www.business.ftc.gov/documents/0494-federal-trade-commission-enforcement-us-eu-and-us-swiss-safe-harbor-frameworks

[13] White House- Washington, "National Strategy for Trusted Identities in Cyberspace: enhancing online choice, efficiency, security, and privacy", 2011

[14] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", Available: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[15] APEC, "APEC Privacy Framework", APEC Secretariat, 35 Heng Mui Keng Terrace, Singapore 119616; 2005, ISBN 981-05-4471-5

[16] Madrid , "International Standards on the Protection of Personal Data and Privacy. The Madrid Resolution", International Conference of Data Protection and Privacy Commissioners, 2009

[17] Madrid, "Data protection authorities from over 50 countries approve the 'Madrid Resolution' on international privacy standards", 2009

[18] ISO/IEC 29100, "Information technology — Security techniques — Privacy framework", 2011

[19] Thomas, Haeberlen and Lionel Dupré, "Cloud Computing Benefits, risks and recommendations for information security", ENISA 2012, Rev. B, V no. 2