ISSN:0975-9646

A System for Quantitative Evaluation of the Privacy 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 a new model in the IT's world. The privacy protection is one of the key challenges that the cloud computing faces. The customers, in the cloud computing, depend on the cloud provider to manage their data. In addition, the cloud computing resources are sharing with multi customers and these resources are located in different regions that subject to different jurisdictions. All of these matters lead to many privacy risks. In this paper, we try to develop an initial quantitative evaluating system that aims to help the customers to know what the privacy's weaknesses on the cloud providers by evaluating whether the cloud provider meets the privacy related issues or not.; this will help them to make the decision.

Keywords: cloud computing, quantitative evaluation, privacy, cloud provider.

I. INTRODUCTION:

Cloud computing is the most resonance word in the current age of technology. People usually know cloud computing as applications and services offered over the internet. The United States National Institute of Standards and Technology (NIST) has developed a good working definition, which defines cloud computing with details 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."* (Mell & Grance 2009).

Under this definition, the cloud computing model has five essential characteristics; they are on-demand self service, ubiquitous network access, location-independent resource pooling, rapid elasticity and measured service (International Telecommunication Union [ITU] 2012; Krutz & Vines 2010; Mell & Grance 2009). In addition, it has three delivery service models; they are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (ITU 2012; Krutz & Vines 2010; Mell & Grance 2009). Moreover, the cloud computing has four deployment models; they are public cloud, private cloud, hybrid cloud and community cloud (ITU 2012; Krutz & Vines 2010; Mell & Grance 2009).

Although there are researches that addressed privacy issue on cloud computing, but until now there is not any quantitative evaluation to evaluate the privacy in cloud computing. Evaluation or assessment is a process of gathering data and then analyzing or ordering it (Martinez 2005) to understand the current state of system with the intent of enhancing or improving it (Pressman 2010). It can be used to determine whether the organization is effectively carrying out its practices, and the extent to which it is achieving its stated objectives and anticipated results (Martinez 2005). Both the qualitative factors and quantitative metrics are considered during the evaluation activity (Pressman 2010).

In this paper, we propose creating an initial evaluating system to evaluate the privacy in the cloud provider by using our proposed privacy framework in (AL-Aswadi & Batarfi 2014) which we designed it to help the customer to evaluate the level of privacy in cloud providers and to help the cloud providers to increase the customer's trust on them. This paper considers a supplement to our work that is described in (AL-Aswadi & Batarfi 2014); it shows the way of how to can use this proposed privacy framework to evaluate the privacy of cloud providers.

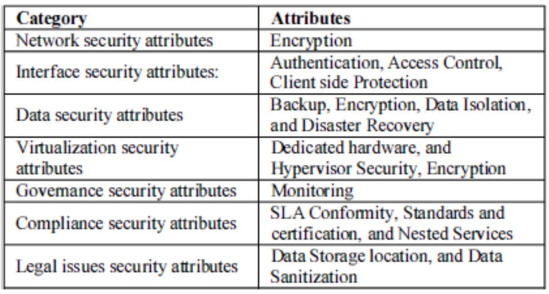
In this paper, we will use the different processes to develop the quantitative evaluating system. First, we will define the key conditions and rules for evaluating. Next, we will develop a scoring system to be used as a quantitative weighting of the principle. Then, we will make an empirical evaluation for some well-known cloud providers, to present how to use this evaluation for assessing and comparing the privacy in potential cloud providers.

This paper consists of seven sections. The rest of this paper is organized as follows: Section 2 shows the related works. Section 3 explains the key conditions and rules for evaluating system. Section 4 presents our proposed scoring system for developing the quantitative evaluation. Section 5 explains the comparison results for three well-known cloud providers. Section 6 discusses the final results and finally in Section 7 we conclude our work.

II. RELATED WORK:

There are few studies about the evaluating the privacy in cloud provider. For example, Abuhussein et al. (2012) tried to identify and categorize the attributes, which highlight the security and privacy provided by cloud computing services. Then they presented how one can use these attributes for assessing and comparing potential cloud computing services from both a provider and a customer standpoint. Table 1 shows their attributes of security and privacy categories. After that, they set a set of important factors for each attribute to assess the security and privacy of cloud computing services. This study may be a one-step of good steps forward to evaluate cloud computing services. However, this study focuses on evaluating the security issue more than the privacy issue. Furthermore, the evaluation in this study was a manual evaluation that did not give numerical values for evaluation to facilitate customers' decision-making.

Table 1: Attributes of Security and Privacy Categories in (Abuhussein et al. 2012)



Category	Attributes
Network security attributes	Encryption
Interface security attributes:	Authentication, Access Control, Client side Protection
Data security attributes	Backup, Encryption, Data Isolation, and Disaster Recovery
Virtualization security attributes	Dedicated hardware, and Hypervisor Security, Encryption
Governance security attributes	Monitoring
Compliance security attributes	SLA Conformity, Standards and certification, and Nested Services
Legal issues security attributes	Data Storage location, and Data Sanitization

The study of Pauley (2010) gave an another example for evaluation cloud provider. In this study the cloud providers transparency was evaluated along four key dimensions—security, privacy, audit-ability, and service levels. Pauley created a scorecard system for evaluating the cloud providers' transparency via the cloud provider's self-service portals and published Web content. This study included a series of questions based on key areas outlined by the CSA, NIST, and the European Network and Information Security Agency (ENISA) as Pauley said. Each question equated to a "0 = no, 1 = yes" value; the overall score based on the total of all scores. Then the domain-based scores were divided by the total possible score to provide a simple percentile equivalent. Also the overall score was divided by the total possible score to derive a percentile equivalent. Then Pauley made an empirical evaluation for six cloud providers (Amazon, Google, Microsoft, IBM, Terremark, and Savvis) to test the scorecard and assess the transparency on them. However, he anonymized the results of the six cloud providers, that he chose them, by referring to them as CP1, CP2..CP6.

III. Conditions and rules:

We extracted 18 privacy principles in our previous work (AL-Aswadi & Batarfi 2014); here we set the key conditions and rules for these privacy principles. Conditions and rules indicate to conditions, status, and explanations that are required to realize the privacy principles. Table 2 shows the key conditions and rules for the privacy principles; it includes the limitation rules of collecting, using, retaining, transferring, accessing and processing the data. In addition, it includes the rights for the customer, the conditions and rules of integrity, isolation and security of data. Note that we only ask about the security (access control) that related to privacy protection not for the security environment in cloud computing. The assessment of the security in the cloud computing is out of this study. Moreover, this table shows the accountability, openness, transparency conditions and rules that ask about the level of transparency of cloud provider and if it commits to all its responsibilities; also ask about the SLAs that the cloud provider guarantees and if the SLAs apply for all services. For example, if cloud provider has SLAs for service A and not has SLAs for service B, then if we combine between service A and B the SLAs will it be equal zero. Furthermore, this table includes the physical location, compliance and rest condition and rules as they are explained in it.

Table 2: The Key Conditions and Rules of the Privacy Principles

Privacy Principle	Conditions and Rules
Collection limitation	1. Is the collection of data limited? 2. Does the cloud provider show what the type of data that are collected?
Consent and choice	1. Does the cloud provider ask consent before collecting any data? 2. Can the customer easily withdraw the consent without cost? 3. Does the cloud provider ask consent before using the data for other purpose?
Collection methods	1. Does the cloud provider explain how the data are collected? 2. Are all collection methods done with the knowledge and consent of the customer before collecting?
Data integrity	1. Can the customer update the data without delay? 2. Does the cloud provider apply the updating process for all copies?
Data minimization	1. Does the cloud provider show who is responsible for processing the data? 2. Does the cloud provider minimize the privilege of process and access to data?
Use and retention limitation	1. Is the using of data limited? 2. Is the retention of data limited? 3. What is the duration of the retention period? 4. Does the cloud provider immediately destroy or anonymize the data after end the retention period?
Disclosure and transfer data	1. Does the cloud provider explain to whom the data is transferred? 2. Is there agreement between them (cloud provider and third party)? 3. Is the disclosure of data limited? 4. Does the cloud provider show which data is disclosed or shared? 5. Does the cloud provider show how the process of transferring data is done? 6. Does the cloud provider explain what the applicable constraints are when the data are processed in the third parties?
Notice, transparency and openness	1. Does the policies, practices and related information are in one place and easy to access? 2. Is there a contact email for queries? 3. Is the privacy policy applied for all services of the cloud provider? 4. What the SLAs does the cloud provider guarantee? 5. Are the SLAs applied for all services of the cloud provider? 6. Does the cloud provider notify the customer when update the policies or practices?

Privacy Principle	Conditions and Rules
Rights and access	1. Can the customer access to the data without delay? 2. Does the customer have the rights to update and delete the data without cost or delay? 3. Can the customer file an objection of how the data processing?
Security safeguards and encryption	1. What are the access controls that are used? 2. What are the encryption methods that are used? 3. What are the validation methods that are used?
Sensitive data	1. What is the sensitive data? 2. What are the additional conditions for processing sensitive data?
Accountability and auditing	1. Does the cloud provider commit to its responsibility for all its practices and policies? 2. Is there a risk assessment for using and processing the data with the applicable privacy protection requirements? 3. Does the cloud provider publish annually privacy breaches?
Purpose legitimacy and specification	1. Is the purpose of collecting the data explained in clear language? 2. Does the cloud provider let the customer set his/her preferences?
Proactive measures	1. Does the cloud provider have training program and/or privacy impact assessment for any new service?
Isolation mechanisms	1. Does the cloud provider have additional isolation mechanisms than that is existing? 2. Does the cloud provider show its isolation mechanisms?
Compliance	1. What is the list of applicable laws? And does it have a certificate? 2. Does the cloud provider have a certificate for its ways of collecting the data? 3. Does the cloud provider have a certificate for all its ways of processing the data?
Physical Location	1. Where are the physical locations of data centers? 2. Can the customer specify the region?
Trans-border Flow	1. What are the law and constraints that will be used when transferring the data between different borders?

IV. Scoring system:

The weighting of every principle is the summation of three sub-weighting fields. The first one is “Obligation”, the weight is assigned to it if the cloud provider clearly obligate the principle. The second one is “Link-ability”, the weight is assigned to it if the information of principle is easy access. The last one is “Conditions and Rules”, it indicates the same conditions and rules that are explained in table 2. The weighting of it is the sum of the weights for all Conditions and Rules of principle.

Figure 1 shows the weighting process for every principle. Ow is the Obligation’s weight, Lw is the Link-ability’s weight, Rw is the weight of Conditions and Rules, n is the number of condition and rules for selected principle, and W is the weight of selected principle which is the sum of the weights for Obligation, Link-ability, Conditions and Rules. Table 3 shows all privacy principles and their weighting and shows the total score of weighting privacy principles.

The final score of privacy level in cloud provider is calculated by the following equations:

$$Pw = \sum_{k=1}^{18} W_k \qquad (1)$$

$$W_k = Ow_k + Lw_k + Rw_k \qquad (2)$$

$$Rw_k = \sum_{i=1}^{n} R_{k_i} \qquad (3)$$

Where Pw represents the final score of privacy, W_k is the sum of the weights for Obligation, Link-ability, and Conditions and Rules for principle number k, Ow_k represents the Obligation’s weight for principle number k, Lw_k represents the Link-ability’s weight for principle number k, Rw_k represents the weight of Conditions and Rules for principle number k, R_{k_i} is the condition or rule number i for principle number k. The value of k represents the numbers of principles while the value of i represents the number of condition or rule of k principle, n represents the total number of conditions and rules for principle number k.

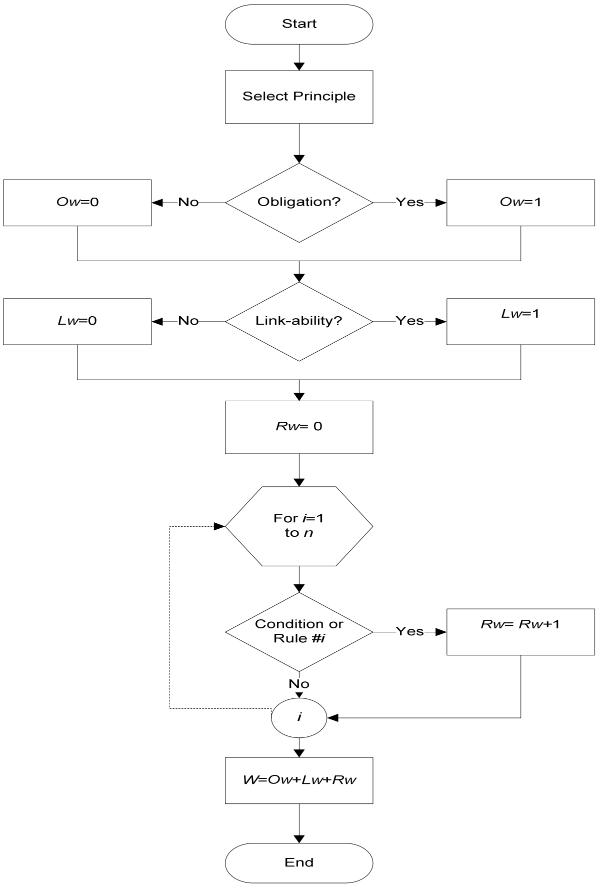


Figure 1: Weighting Process for Selected Principle

Table 3: The Weighting for Privacy Principles

Privacy Principle	Weighting			Total Weight
	Obligation	Link-ability	Conditions and Rules	
Collection limitation	1	1	2	4
Consent and choice	1	1	3	5
Collection methods	1	1	2	4
Data integrity	1	1	2	4
Data minimization	1	1	2	4
Use and retention limitation	1	1	4	6
Disclosure and transfer data	1	1	6	8
Notice, transparency and openness	1	1	6	8
Rights and access	1	1	3	5
Security safeguards and encryption	1	1	3	5
Sensitive data	1	1	2	4
Accountability and auditing	1	1	3	5
Purpose legitimacy and specification	1	1	2	4
Proactive measures	1	1	1	3
Isolation mechanisms	1	1	2	4
Compliance	1	1	3	5
Physical Location	1	1	2	4
Trans-border Flow	1	1	1	3
Total Score				**85**

V. Comparison results:

In this section, we examine the privacy of three well-known cloud providers (Google App Engine, Amazon Web Service (AWS), and Windows Azure). We choose these three cloud providers for two reasons:

1. Their years' length in business is more than 10 years (Pauley 2010).
2. They are the most popular among customers who are interesting in cloud computing (well-known).

We built a manual comparison among the three selected cloud providers to get the comparison results. Table 4 shows the weighting result for Google App Engine provider; table 5 shows the weighting result for AWS provider and table 6 shows the weighting result for Windows Azure provider. This result has been gotten by studying the privacy policies and related links of Google App Engine, AWS and Windows Azure (Amazon 2006, 2011, 2013a-b, 2014a-b, n.d.a-c; Google 2013, 2014a-b, n.d.a-b; Microsoft 2014a-e, n.d.; Palekar 2014; Ross 2011).

Table 4: Weighting Result for Google App Engine Provider

Privacy Principle	Weighting			Total Weight	Explanation
	Obligation	Link-ability	Conditions and Rules		
Collection limitation	1	1	1	3	R_1=0, R_2=1
Consent and choice	1	1	1	3	R_1=0, R_2=0, R_3=1
Collection methods	1	1	1	3	R_1=1, R_2=0
Data integrity	0	1	1	2	R_1=1, R_2=0
Data minimization	0	0	0	0	
Use and retention limitation	1	1	0	2	All Rules=0
Disclosure and transfer data	1	1	3	5	R_1=1, R_2=1, R_3=0, R_4=1, R_5=0, R_6=0
Notice, transparency and openness	1	1	5	7	R_1=1, R_2=1, R_3=1, R_4=1, R_5=0, R_6=1
Rights and access	1	1	3	5	R_1=1, R_2=1, R_3=1,
Security safeguards and encryption	1	1	3	5	R_1=1, R_2=1, R_3=1,
Sensitive data	1	1	1	3	R_1=1, R_2=0
Accountability and auditing	0	1	2	3	R_1=1, R_2=1, R_3=0,
Purpose legitimacy and specification	1	1	1	3	R_1=0, R_2=1
Proactive measures	0	0	0	0	
Isolation mechanisms	1	1	2	4	R_1=1, R_2=1
Compliance	1	1	1	3	R_1=1, R_2=0, R_3=0,
Physical Location	1	1	1	3	R_1=1, R_2=0
Trans-border Flow	0	0	0	0	
Total Score				**54**	

Table 5: Weighting Result for AWS Provider

Privacy Principle	Weighting			Total Weight	Explanation
	Obligation	Linkability	Conditions and Rules		
Collection limitation	1	1	1	3	R_1=0, R_2=1
Consent and choice	0	1	0	1	R_1=0, R_2=0, R_3=0
Collection methods	1	1	1	3	R_1=1, R_2=0
Data integrity	0	1	0	1	R_1=0, R_2=0
Data minimization	0	0	0	0	
Use and retention limitation	1	1	0	2	All Rules=0
Disclosure and transfer data	1	1	3	5	R_1=1, R_2=1, R_3=0, R_4=1, R_5=0, R_6=0
Notice, transparency and openness	1	1	4	6	R_1=0, R_2=1, R_3=1, R_4=1, R_5=0, R_6=1
Rights and access	1	1	1	3	R_1=0, R_2=0, R_3=1,
Security safeguards and encryption	1	0	3	4	R_1=1, R_2=1, R_3=1,
Sensitive data	0	0	0	0	
Accountability and auditing	0	1	2	3	R_1=1, R_2=1, R_3=0,
Purpose legitimacy and specification	1	1	1	3	R_1=0, R_2=1
Proactive measures	0	0	0	0	
Isolation mechanisms	1	1	2	4	R_1=1, R_2=1
Compliance	1	1	1	3	R_1=1, R_2=0, R_3=0,
Physical Location	1	1	2	4	R_1=1, R_2=1
Trans-border Flow	0	1	1	2	R_1=1
Total Score				**45**	

Table 6: Weighting Result for Windows Azure Provider

Privacy Principle	Weighting			Total Weight	Explanation
	Obligation	Link-ability	Conditions and Rules		
Collection limitation	1	1	1	3	R_1=0, R_2=1
Consent and choice	0	1	0	1	R_1=0, R_2=0, R_3=0
Collection methods	1	1	1	3	R_1=1, R_2=0
Data integrity	0	1	0	1	R_1=0, R_2=0
Data minimization	0	1	1	2	R_1=0, R_2=1
Use and retention limitation	1	1	0	2	R_1=0, R_2=0, R_3=0, R_4=0,
Disclosure and transfer data	1	1	4	6	R_1=1, R_2=1, R_3=1, R_4=1, R_5=0, R_6=0
Notice, transparency and openness	1	1	5	7	R_1=1, R_2=1, R_3=1, R_4=1, R_5=1, R_6=0
Rights and access	1	1	1	3	R_1=0, R_2=0, R_3=1,
Security safeguards and encryption	1	1	3	5	R_1=1, R_2=1, R_3=1,
Sensitive data	0	0	0	0	
Accountability and auditing	0	1	1	3	R_1=0, R_2=1, R_3=0,
Purpose legitimacy and specification	1	1	1	3	R_1=0, R_2=1
Proactive measures	0	0	0	0	
Isolation mechanisms	1	1	2	4	R_1=1, R_2=1
Compliance	1	1	0	2	R_1=0, R_2=0, R_3=0,
Physical Location	1	1	2	4	R_1=1, R_2=1
Trans-border Flow	0	0	0	0	
Total Score				**49**	

VI. Final results and discussion:

As it is observed from the comparison results; the Google App Engine provider got the highest score, which is 54, followed by Microsoft Azure provider which got 49 score and then AWS which got 45 score. To calculate the percentage of privacy, we will use the following percentage formula (TutorVista 2014):

$$\text{Percentage} = \frac{\text{Score}}{\text{Total Score}} \times 100 \qquad (4)$$

By using the equation number (4) to calculate the percentage, the Google App Engine got 64% of privacy level, followed by Microsoft Azure which got 58%, and then AWS which got 53%. Figure 2 shows the weight percentage of every privacy principle for Google App Engine, AWS and Windows Azure which are also calculated by using the equation number (4). This figure helps us to know which privacy principles have low score. In other words, where are the weaknesses for protecting the privacy in selected cloud providers?

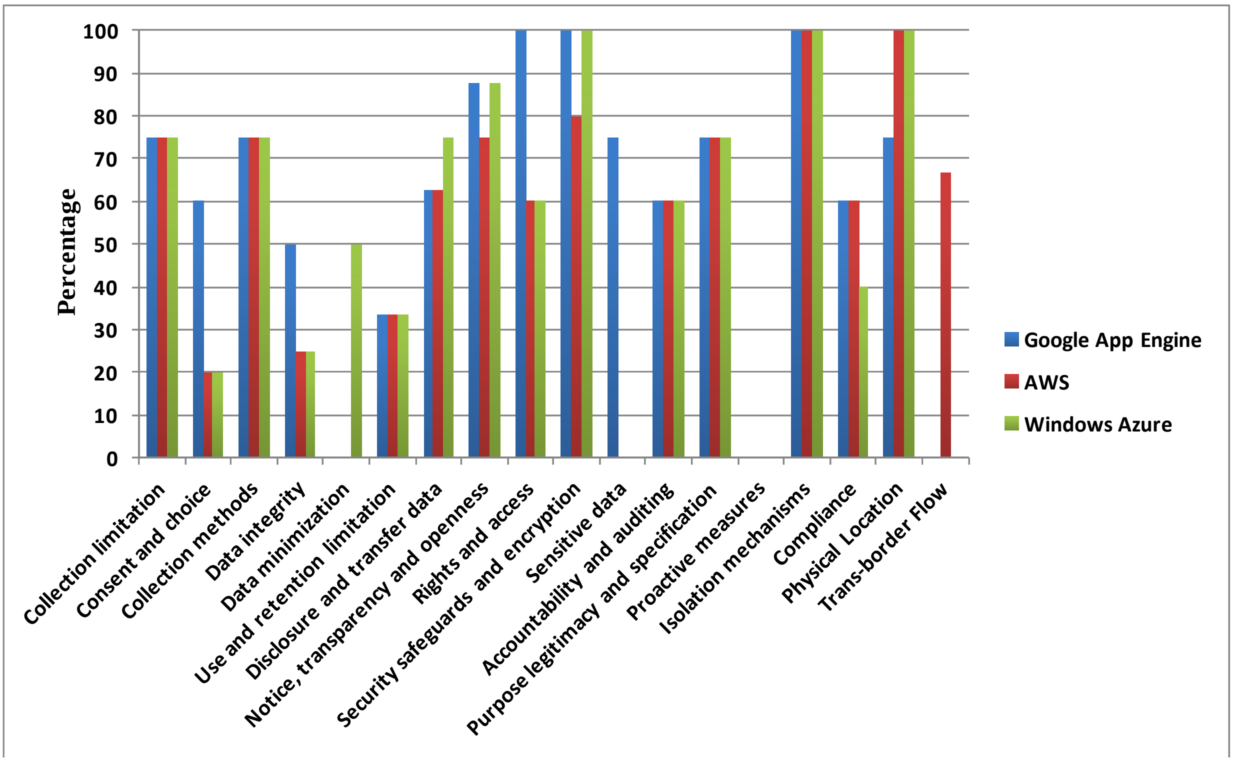


Figure 2: The Weight Percentage of Privacy Principles for Google App Engine, AWS and Windows Azure

In Google App Engine, the data minimization and the trans-border flow principles got 0%; the use and retention limitation principle got less than 50%; while the data integrity principle got 50% and the rest principles got more than 50%. In Windows Azure, the sensitive data and the trans-border flow principles got 0%; the use and retention limitation, the consent and choice, the data integrity and the compliance principles got less than 50%; and the rest principles got more than 50%. In AWS, the data minimization and the sensitive data principles got 0%; the use and retention limitation, the consent and choice and the data integrity principles got less than 50%; while the rest principles got more than 50%.

The satisfactory result depends on the customers' opinions themselves and what their needs are. For example, some of them say it should not be less than 50%, while others may say it should not be less than 70%, etc.

All of these results prove that the cloud providers need to pay more attention and to make more efforts to protect the customers' privacy. In addition, the cloud providers need to be more transparent especially with regards to collect, use, retain, transfer and process the customers' data
.

Note that as we see from these results the isolation mechanisms and security safeguards and encryption may have 100% percentage. This does not mean they are high level, but these are because we do not assess the security in cloud computing, we only ask if there are some mechanisms for access control, encryption and for isolation. This point may be the limitation of this study that we will address it in the future work.

VII. Conclusion:

The privacy protection is one of the most serious challenges that the cloud computing faces. Protecting the privacy in cloud computing is not an easy task especially with the dependence on the cloud provider in the management of customer data, the resources existence in different regions that subject to different jurisdictions and sharing the resources with multi customers of cloud computing.

The responsibility of protecting the privacy in cloud computing falls on the cloud provider and the government; also a part of the responsibility falls on customers themselves through increasing their awareness and experience for evaluating the privacy of the potential cloud providers to choose the suitable one.

In this paper, we try to develop an initial quantitative evaluation system which aims to help the customer to evaluate the privacy in cloud providers for helping them to choose the suitable one of the potential cloud providers. We have done an empirical evaluation for three well-known cloud providers (Google App Engine, AWS, and Microsoft Azure) to apply this evaluating system on them. The results show that the cloud providers need to pay more attention and to make more efforts to protect the customers' privacy.

References:

Abuhussein, A., Bedi, H. & Shiva, S. (2012) "Evaluating Security and Privacy in Cloud Computing Services:A Stakeholder's Perspective", The 7th International Conference for Internet Technology and Secured Transactions (ICITST)

AL-Aswadi, F. & Batarfi, O. (2014) "A Framework for Enhancing Privacy Provision in Cloud Computing", International Journal of Computer Science and Information Technologies (IJCSIT.

Amazon (2006) "Amazon S3 Customer Data Isolation", Access date 11 June 2014, from: http://docs.aws.amazon.com/AmazonS3/latest/dev/DevPayDataIsolation.html

Amazon (2011) "AWS Site Terms", Access date June 3, 2014, from: http://aws.amazon.com/terms/?nc1=f_st

Amazon (2013a) "Amazon EC2 Service Level Agreement", Access date June 5, 2014, from: http://aws.amazon.com/ec2/sla/

Amazon (2013b) "Amazon S3 SLA", Access date June 6, 2014, from: http://aws.amazon.com/s3/sla/

Amazon (2014a) "Amazon.com Privacy Notice", Access date June 1, 2014, from: http://www.amazon.com/gp/help/customer/display.html?nodeId=468496

Amazon (2014b) "What's New from Amazon Web Services", Access date June 11, 2014, from: http://aws.amazon.com/new/?nc1=h_l2_cc

Amazon (n.d.a) "AWS Identity and Access Management (IAM)", Access date June 11, 2014, from: http://aws.amazon.com/iam/?nc1=f_m

Amazon (n.d.b) "AWS Privacy", Access date June 1, 2014, from: http://aws.amazon.com/privacy/

Amazon (n.d.c) "Global Infrastructure", Access date June 3, 2014, from: https://aws.amazon.com/about-aws/globalinfrastructure/?nc1=h_l2_cc

Google (2013) “Self Regulatory Frameworks”, Access date May 11, 2014, from: http://www.google.com/intl/en/policies/privacy/frameworks/

Google (2014a) “App Engine Service Level Agreement”, Access date May 12, 2014, from: https://developers.google.com/appengine/sla

Google (2014b) “Privacy Policy”, Access date May 11, 2014, from: http://www.google.com/intl/en/policies/privacy/

Google (n.d.a) “Data center locations”, Access date May 12, 2014, from: http://www.google.com/about/datacenters/inside/locations/index.html

Google (n.d.b) “Key terms”, Access date May 11, 2014, from: http://www.google.com/intl/en/policies/privacy/key-terms/

International Telecommunication Union (2012) "Privacy in Cloud Computing", ITU-T Technology Watch

Krutz, R. & Vines, R. (2010) "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc., ISBN: 978-0-470-58987-8

Martinez, C. (2005) "The Importance of Evaluation", Access date May 10, 2014, from: http://www.guidestar.org/rxa/news/articles/2005/importance-of-evaluation.aspx

Mell, P. & Grance, T. (2009) "The NIST Definition of Cloud Computing", NIST Information Technology Laboratory.

Microsoft (2014a) "Microsoft Azure Privacy Statement", Access date June 13, 2014, from: http://azure.microsoft.com/en-us/support/legal/privacy-statement/

Microsoft (2014b) "Microsoft Azure Support: Service Level Agreement", Access date June 15, 2014, from: http://azure.microsoft.com/en-us/support/legal/sla/

Microsoft (2014c) "Microsoft Azure Trust Center", Access date June 14, 2014, from: http://azure.microsoft.com/en-us/support/trust-center/

Microsoft (2014d) "Microsoft Azure Trust Center-Privacy", Access date June 12, 2014, from: http://azure.microsoft.com/en-us/support/trust-center/privacy/?rnd=1

Microsoft (2014e) "Privacy & Cookies", Access date June 14, 2014, from: http://www.microsoft.com/privacystatement/en-us/core/default.aspx

Microsoft (n.d.) "Documentation | Azure", Access date June 16, 2014, from: http://azure.microsoft.com/en-us/documentation/

Palekar, A. (2014), "Network Isolation Options for Machines in Windows Azure Virtual Networks", Access date June 17, 2014, from: http://azure.microsoft.com/blog/2014/03/28/network-isolation-options-for-machines-in-windows-azure-virtual-networks/

Pauley, W. (2010) "Cloud Provider Transparency: An Empirical Evaluation", Security & Privacy, IEEE

Pressman, R. (2010) "Software Engineering: A Practitioner's Approach", McGraw-Hill Education, 7th edition, ISBN: 0073375977

Ross, M. (2011) “Transaction Isolation in App Engine”, Access date May 14, 2014, from: https://developers.google.com/appengine/articles/transaction_isolation

TutorVista (2014) "Percentage Formula", Access date June 17, 2014, from: http://formulas.tutorvista.com/math/percentage-formula.html