RESEARCH ARTICLE OPEN ACCESS

Cloud Trust Management Framework Based On Cloud Market spaces

W.P. Eureka Priyadarshani[1], Gihan N. Wikramanayake[2], Andrei Kelarev[3]and E.M. Piyal Ekanayake[4]
[1,4] Wayamba University of Sri Lanka, Sri Lanka
[2]University of Colombo School of Computing, Sri Lanka
[3] Deakin University, Australia

Abstract
Nowadays, applications running in virtual or cloud-based environments are all susceptible to exploitation. However, traditional trust solutions have not been fully optimized for virtualized third party environments. In this situation, the selection of an appropriate cloud service provider is an issue. This paper introduces a completely novel idea on most appropriate cloud service selection through an intermediator. It is based on the new notion of a marketspace. Our paper is devoted to the investigation of a novel architecture suggested for a marketspace. Several theoretical notions related to trust have also been explained extensively in the paper for Cloud service provider selection.
Keywords:*Trust, Cloud Service Provider, Cloud Marketplace, Cloud Marketspace.*

I. Introduction

The selection of the most appropriate and trusted cloud market is a challenge for the user ([1];[2]). The most common type of cloud market, referred to as a cloud marketplace, offers its own services directly to customers. In general, a cloud marketplace consists of a particular Cloud Service Provider (CSP), various types of online services, customers, and, in some situations, third party service providers who try to sell their products through the main CSP.

In a cloud marketplace, a user can select a service or a software application most appropriate to his needs; user requirements can vary with the size of data to be stored, the kind and amount of computation to be performed on data, the level of confidentiality of the data to be maintained and so on. While some users prefer cost effectiveness ([3]; [4]) others are more concerned about data confidentiality [1]. Some cloud marketplaces, for example, spotcloud (SpotCloudTM, http://spotcloud.com/) and CloudCommons (http://www.cloudcommons.com/), even allow users to select a cloud service provider based on cost, quality, location and user ratings.

In relation to assisting a user in the selection of the most appropriate CSP according to user requirements, Pennington states: "Marketing research has provided some empirical evidence of the importance of trust perceptions in market relationships" [5]. The importance of trust and reputation system in selecting a trustworthy service provider in cloud marketplaces is also mentioned by Habib et al. [6] where the authors conclude: "it is extremely difficult for cloud consumers to identify trustworthy (or dependable) cloud providers in these marketplaces". The importance of an independent third party assurance body to accredit the trust of a CSP is explained in [7]. This discussion around trust motivates us to develop a deeper understanding of how cloud markets can be assessed in helping the user to determine the most trustworthy CSP for her needs.

The objectives of this paper are focused on the followings:

- Defining the new concept of a "cloud marketspace".
- Introducing an architecture for a cloud marketspace and its utilization in determining the most trustworthy cloud service provider.

Sections 2 and 3 provide a review of existing organization and architectures which are used to find solutions for trust related issues in cloud service and cloud markets in selecting a CSP.

II. Literature Review

As our thorough search of literature has shown, there is a lack of research on this kind of new marketing strategy, what we call a cloud marketspace. As similar idea has been expressed by Rayport and Sviokla for online markets but not for cloud markets [8]. Their definition can be comprehensively taken to define a bi-directional cloud market as cloud computing is merely an online service. Further, the term marketspace has been used in different subject areas in different ways using its basic structure. For example, Duin has used this for "learning marketspace" to explain a space where learners, employers and learning providers meet together [9]. A comparison between this learning marketspace and our proposed cloud marketspace is explained in section 4.1.

Cloud Security Alliance is the first nonprofit organization formed by professionals of "industry practitioners, corporations, associations and other key stakeholders" [10]. It provides security, trust and assurance within cloud computing.

Considering trust as an important part of cloud marketspaces [6] our research is focused on issues, which the CSA tries to solve, and those which remain unresolved. In this paper, we first focus on aims and methodology of the CSA and associated trust management issues. Thereafter we shall explain how Habib's architecture [6] connects with CSA. These explanations are intended to help the readers to understand all aspects of the new concept "cloud marketspace".

In 2009, a trust management group calling itself the Cloud Security Alliance ([10]; [11])was established. Its mission statement was "To promote the use of best practices for providing security assurance within cloud computing, and educate the use of cloud computing to help secure all other forms of computing". One of the mechanisms introduced by them to determine the industry's perspective on security and trust was a questionnaire (CAIQ) for the users to help them develop a "best practice" model based on these features. The CSA security matters to create trust in customers' opinions in three ways:

a) Creating one standard cloud-specific definition for "secure",
b) Streamlining the process for evaluating providers, and
c) Overcoming security fears to cloud adoption.

All these issues are addressed in their "cloud security certification" [12].

Further, the CSA provides great support to the International Standardization Council (ISC) in all standards-related activities. At the end of 2011, CSA launched the STAR which stands for Security, Trust & Assurance Registry. This registry improves transparency and assurance in the cloud and is accessible to the general public, thereby helping users assess the security of cloud providers. In March of 2014, a new version of Cloud Control Matrix (CCM v3) was introduced to the cloud market and from March 2015 onwards, all customers will be audited against this Matrix.

The Open Certification Framework Working Group of CSA STAR has defined a multilayered structure (Figure 1) to encourage providers to make security capabilities according to the customer's level of trust, security and assurance requirements. The multilayers [10] defined by CSA STAR can be easily activated in our proposed cloud marketspace as each layer of their structure demands the level of trust.

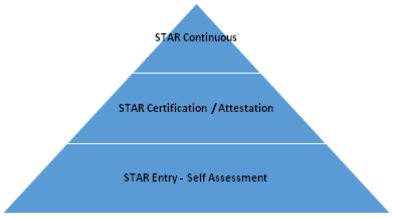

Fig 1: Multi-Layered Structure as Defined by CSA STAR

- STAR Entry - Self Assessment: The bottom level represents non-critical application users in the cloud and they might be satisfied with the results of a provider self-assessment. Publication of the results of a due diligence self-assessment based on CSA Consensus Assessment Initiative (CAI)Questionnaire and/or Cloud Control Matrix (CCM).
- STAR Certification / Attestation: The middle level represents a complex cloud environment and the assessment is executed by a qualified and independent third party. Publication of available results of a third party assessment based on CCM and ISO27001 or AICPA SOC2.
- STAR Continuous: At the top level more advanced assessment based on a continuous verification of some key parameters and SLAs are taken into account. Publication of results of security properties monitoring, based on Cloud Trust Protocol (CTP) CSA STAR is capable of assuring trust in three layers.

Our proposed cloud marketspace (Section 4) operates on this multi-layered structure according to the user's desired levels of trust. Meanwhile, in the next section, a detailed review on Habib et al. [6] trust management architecture is presented to identify the trust issues which remain to be solved.

Habib and his research group highlight the need to establish trust for selecting trustworthy service providers in cloud environments in most of their publications from 2010. In 2010 [13] they extensively explained trust and reputation-based approaches for supporting customers to select service providers in the cloud market. They explored a number of parameters such as "(i) Service Level Agreement (SLA), (ii) Compliance or accreditation or certification, (iii) Portability feature, (iv) Interoperability feature, (v) Geographical location of the data center (cloud), (vi) Customer support facilities, (vii) Performance test, (viii) Deployment models (e.g., private, public, and hybrid clouds) (ix) Federated identity management solution, (x) Security measures, and (xi) User recommendation, feedback and publicly available reviews". They focus on trust establishment from the user's perspective and define two ways to establish trust: one by hosting trust models in a centralized storage, in which case, a trusted third party is required and the other by using a decentralized trust model which has the drawback of not preserving privacy.

Similarly, in 2012 they introduced some Quality of Service (QoS) parameters to be considered in measuaring trust. Some of them are: "SLAs, Portability, Interoperability and Geographical Location, Performance, Security, User feedback, Customer Support, Service Deployment and DeliveryModels" [4]. In 2013 a multi-faceted Trust Management system [6] was introduced by them to support the customers in identifying trustworthy cloud providers and it was heavily based on the CSA trust architecture, basing trust assessments on user ratings, provider statements, measurements and property certificates. In the following paragraph a detailed description of that model is given.

In the paper [6] we could identify wherein the trust has been considered as an important factor in the cloud markets. Most of the user issues identified by Habib et al. in [6] are resolved in their recent paper [14] which assumes the availability of a suitable trustworthy cloud service provider.

Their trust assessment is based on the following four features:

- User Ratings
- Provider Statements
- Measurements
- Property Certificates

The choice of the abovefeatures was based on the results of the CSA questionnaire mentioned above. The questions focused on the following factors:

- Compliance
- Data Governance
- Facility Security
- Human Resources Security
- Information Security
- Legal
- Operations Management
- Risk management
- Release Management
- Resiliency
- Security Architecture

However, we argue that attaching a higher weightage on user ratings destroys the real trust of a service provider, but makes them more popular in the cloud markets.

III. Dealing with Trust

Although extensive research has been carried out on cloud marketplaces, no single study exists which adequately covers all user requirements for DBaaS, SaaS, PaaS separately based on trust. Comparing the highly valued features with their rankings in existing cloud markets ([15]; [16]) we conclude that disproportionate weighting is allocated to trust in most CSPs. In fact, we have identified the following two specific problems, namely lack of service level trust and trust saturation and aging in existing cloud markets.

3.1. Lack of Service Level Trust

Most trust measurement models for cloud services are based on general cloud trust and not categorised based on the specific services they provide [6]. For instance, a particular DBaaS may be competent in storage service but not in other services such as computation and data management; such a DBaaS should have separated different rankings for these services. As an example, in the month of January 2014, justhost.com was in the 3rd place of database ranking list [15] but in the 1st place in storage ranking list [16].

3.2. Trust Saturation and Aging

In some cases high popularity of cloud services may be a function of their long period of service (age) in the cloud market. In this case, user ratings tend to maintain higher service provider rankings, adversely affecting the opportunity for new services in the marketplace to gain an edge. This phenomenon is known as *trust saturation* and it can be explained by the example of user ratings in the Habib trust model [6]. Thus, a long history of positive user ratings can contribute to a high level of trust.

A way to overcome this problem was proposed by Varadharajan in 2009 with the introduction of two types of trust measures referred to as "Soft Trust" and "Hard Trust". Soft Trust is derived from social control mechanisms and intangible information such as reputation, experiences and cooperation while Hard Trust is derived from concrete security mechanisms and information such as certificates, credential tokens and their verifications. Finally, the

overall trust is measured as a combination of these two [17].

A similar approach is adopted by Garg et al. [18] where two types of parameters, called quantitative and qualitative, are defined for ranking cloud service providers.

In Section 3, we propose our own structure of cloud marketspace with a focus on providing trust as a feature for users. Three types of trust measures, "Direct Trust" and "Relative Trust " as proposed in [19] and a high level trust called Transparent Trust, have been considered in the cloud marketspace Structure. We shall discuss how the trust can be generated precisely in our proposed architecture.

IV. Cloud Marketspace

Cloud marketspace is different in operation from the marketplace (virtual marketplace [20], cloud computing marketplace [2]) as follows:

Role is different - Cloud marketspace is an online space where cloud customers and cloud service providers meet and establish a relationship. But marketplace sells goods and services directly to the customer when the payment process is within the marketplace.

Transaction is different- Cloud marketspace matches sellers and buyers so that a successful match will culminate in a transaction. It is not necessary for the transaction to materialize through the cloud marketspace but it builds the relationship.

Customer's loyalty is different -Cloud marketspace helps customers to select the most appropriate cloud service provider according to their requirements. In other words, it helps the customer to scale the trust of different CSPs who engage in particular user expected service. The Figure 2 outlines the basic idea of a cloud marketspace.

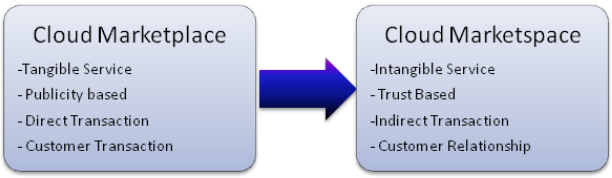

Fig2: Difference between Cloud Marketplace and Cloud Marketspace

Therefore, we define the concept of cloud marketspace as follows:

A cloud marketspace is an online space that facilitates bi-directional business. The Cloud Service Providers (CSP) list their capabilities with evidences so that cloud customers can match their needs with CSP's capabilities. The role of the cloud marketspace is to match cloud customers' requirements and CSP's capabilities and to produce a list of best matches. Then a successful match can pave the way for a transaction.

This type of cloud marketspace consists of various cloud service providers, customers, authenticated past cloud users or expertise. In short, the operation of a cloud marketspace can be defined as an online auction which helps to select cloud service providers according to user requirements. In other words, a cloud marketspace can be considered as a combination of various cloud marketplaces [21] and CSPs. It is managed by authorized cloud users with experience and also provides a platform for the user to get an idea about the standards followed by cloud service providers.

4.1 Comparison between Proposed Cloud Marketspace and Other Marketspace Architectures.

It is hard to understand the operation of the marketspace without having a "radical shift in thinking from markets defined by physical place to ones defined by information space" [8]. According tothefirst basic idea on "marketspace" by Rayport and Sviokla [8], marketspace transaction is very different from marketplace transaction. In short, a direct transaction is maintained within the marketplace. However only a relationship is developedwithin the marketspace and the transaction process is not expected within the marketspace architecture. A practical usage of this kind of architecture called "learning marketspace"wasexplained by Duin [9] in 2001.It facilitatescollaboration between leaning providers, learners and the organizations. In other words it provides a consistent interface to a knowledge domain. Learners can do the subject selection, course selection, university selection, discussion with experts etc. through this learning marketspace.

Whencompared to learning marketspace, our proposed cloud marketspace architecture ensuresnot only a collaboration between cloud customers, cloud service providers and knowledge of experts but also a trusted environment for CSP selection.

V. Our Proposed Cloud Marketspace Structure

Our proposed marketspace maintains data on various cloud service providers. Cloud service providers who wish to sell their services through the internet can join the cloud marketspace by disclosing and entering their features to the storage of CSP's capabilities. The cloud marketspace is synthesising the features of the CSPs and offering these on an interface with the prospective user.

This cloud marketspace structure explains the CSP selection in general. It maintains a database of

evidence of trust in each and every cloud service provider it lists. The cloud marketspace is linked with databases having answers to questions related (see Figure 3) to customer requests. For the accuracy of answers provided by CSPs, the cloud marketspace compares the authenticated past cloud user experiences with the evidences provided by CSPs. Futher it is validated by an independent group of experts as shown in Figure 3.

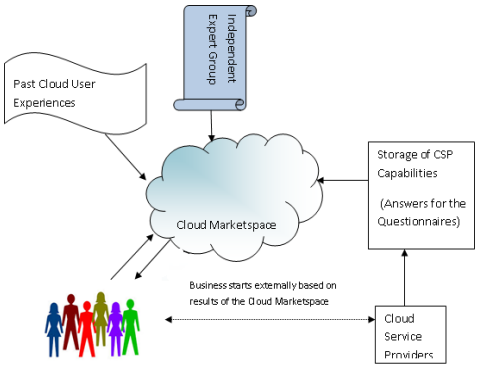

Fig 3: Structure of the Cloud Marketspace

For instance, if a user is concerned about trust only, then it considers only the trust related answers provided by the CSPs. According to the level of trust (Low, medium and High) requested by the user, the number of answers considered by the cloud marketspace can vary. The cloud marketspace has the ability to analyse the levels of trust separately.
Therefore, as the customers of this cloud marketspace, users have the opportunity to select the required level of trust and level of cost for each and every service.
Past cloud user experiences based on the history (failures, certainty, losses etc.) and the independent group of experts jointhe cloud marketspace, control and validate the results.
Finally, the cloud marketspace reveals the most suitable CSP according to the user requested factors after having a detailed analysis on existing CSPs. Based on this feedback, the user is able to decide on which cloud service provider to be chosen. The cloud marketspace is not involved with any kind of transaction. This ensures that the cloud marketspace is consistent with controling trust saturation. The customer has to establish the relationship externally with the selected CSP.
Figure 4 explains how a perticular customer can trace the best choice from the cloud marketspace.

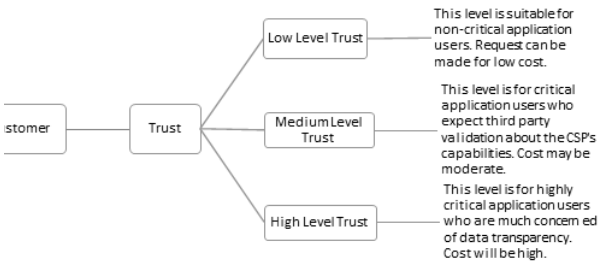

Fig4: Levels of Customer Requirenments on Trust

According to Figure 4, the customer has three basic types of choices according to their necessities and their awareness of cloud computing. These types of trust levels ensure the elimination of selections associated with a cloud service provider simply based on their long period of service in the cloud market.The low level of trust is measured with Direct Trust [19] and medium trust is measured with both Relative Trust and Direct Trust. Transparent Trust will be a novel trust level still under consideration by CSA STAR.
Thus the cloud marketspace can be generalized in selecting the most appropriate CSP from other aspects such as quality of service, cost etc. other than the trust.

VI. Case Study on Transparent Trust Calculation

The Direct and Relative trustcalculation methods can be found in a number of publications ([17], [19]). According to the latest released by the Cloud Security Alliance (CSA) [10], thetypes of questions considered under trasparency as a service have been used in the transparent trust calculation in this architecture. Table 01shows how those questions can be converted intofactors that can be measured by assigning values.

Table 01: Transforming Questions into Factors

No	User Raises Questions	Supportive Factors t_x	Factor ID $t_{x.y}$
1	What does my cloud computing configuration look like right now?	On premises	$t_{1.1}$
		Off premises	$t_{1.2}$
		On and off premises	$t_{1.3}$
2	Who has access to my data now?	Only me	$t_{2.1}$
		CSP or Broker	$t_{2.2}$
		Unknown Third party	$t_{2.3}$
3	Where are my data and processing	On Premises	$t_{3.1}$
		Off premises in an authenticated CSP	$t_{3.2}$

	being performed?	server.	
		Off premises in an unidentified server.	$t_{3.3}$
4	Who has had access to my data?	Only me	$t_{4.1}$
		Known third party-Authenticated CSP or broker	$t_{4.2}$
		Unknown thirdparty	$t_{4.3}$
5	What audit events have occurred in my cloud configuration?	User management	$t_{5.1}$
		Group management	$t_{5.2}$
		Project changes	$t_{5.3}$
		Permission changes	$t_{5.4}$
		Workflow changes	$t_{5.5}$
		Notification changes	$t_{5.6}$
		Custom field changes	$t_{5.7}$
		Component changes	$t_{5.8}$
		Version changes	$t_{5.9}$
6	What vulnerabilities exist in my cloud configuration?	Continuous scaning to provide visibility into both server and client-side vulnerabilities	$t_{6.1}$
		Vulnarability assessment	$t_{6.2}$
		Network security monitoring	$t_{6.3}$
		Full asset discovery	$t_{6.4}$
		Mobile risk identification	$t_{6.5}$

If a particular customer C is interested in transparent trust measures from selected factors of the CSPs who are registered in the cloud marketspace, then the final transparent trust values of each and every CSP is given by a function $TT\ (x_c\ )$.

According to Table 01,if the customer C selected factors from the question categories t_1, t_4 and $t_5$and they were evaluated by expert groups in the marketspace then the final transparent trust (TT) is a function of $t_1, t_4 and\ t_5$ .As the customer C is not concern of t_2, t_3, t_6 factors for his required transparent trust it is not included in the TT (x_c). Hence x_c is the function value specific to customer C.

$TT\ (x_c\ ) = f(t_1, t_4, t_5)$, where

$t_1, t_4, t_5 < 1\ and\ may\ be\ negetive\ \ values.$

$$t_1 = f_1(t_{1.1}, t_{1.2}, t_{1.3}, \alpha) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

$$t_4 = f_4(t_{4.1}, t_{4.2}, t_{4.3}, \beta) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2)$$

$$t_5 = f_5(t_{5.1}, t_{5.2}, t_{5.3}, t_{5.4}, t_{5.5}, t_{5.6}, t_{5.7}, t_{5.8}, t_{5.9}, \gamma) \dots (3)$$

The functions $f_1, f_4\ and\ f_5$ have the parameters α, $\beta\ and\ \gamma$ respectively andthose parameters determine the final decision of the expert groups associated with the marketspace to the functions. The parameter $t_{x.y}$may assume both positive and negetive values. If a factor gives positive values to the function itimplies that the particular CSP is optimisticon the associated factors. However if it gives negative values thenit indicates thatthe particular CSP is destructive on the associated factors. Finally the total transparent trustTT(x_c) is based on thefactors $t_1, t_4\ and\ t_5$selected by customer C .

VII. Conclusion

The cloud marketspace has been introduced to act as an intermediator for the selection of cloud service providers. The terminology is introduced as a foundation to build standards for cloud resources trading which establishes relationships through a trustworthy intermediator.

Furthermore, the paper presented a one-stop cloud market solution that enables the simulation of different business cases to market their service offerings. The proposed solution introduces advanced aggregated price models and integrates a new resolution approach that helps customers to search and select cloud service providers. The theoretical implication of the proposed approach is a taxi fleet management application and a trusted application for CSP selection.

References

[1] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing", *InTrust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference*, pp. 933-939.

[2] H. Li, and J. J. Jeng, "CCMarketplace: a marketplace model for a hybrid cloud", *In Proceedings of the 2010 Conference of the Center for Advanced Studies on Collaborative Research*, 2010, pp. 174-183.

[3] M. Creeger, "CTO roundtable: cloud computing", Commun. ACM, 52.8, 2009,pp. 50-56.

[4] S.M. Habib, S. Hauke, S. Ries, and M. Mühlhäuser, "Trust as a facilitator in cloud computing: a survey". Journal of Cloud Computing, 1(1), 2012, pp.1-18.

[5] R. Pennington, H.D. Wilcox, and V. Grover, "The role of system trust in business-to-consumer transactions", *Journal of Management Information Systems*, Vol *20*, No 3, 2003, pp. 197-226.

[6] S.M. Habib, S. Ries, M. Mühlhäuser, and P. Varikkattu, "Towards a trust management system for cloud computing marketplaces: using CAIQas a trust information source", *Security and Communication Networks*, Vol. *7, No* 11,2013, pp. 2185-2200.

[7] C. Everett, "Cloud computing – A question of trust. Computer Fraud & Security", 2009, http://dx.doi.org/10.1016/S1361-3723(09)70071-5

[8] J.F. Rayport, and J.J. Sviokla"Managing in the Marketspace",*Harvard Business Review*, 1994, 72(6), pp. 141-150.

[9] A.H. Duin, L.L. Baer, and D. Starke-Meyerring, "Educause Leadership Strategies", volume 4: Partnership in the Learning Marketspace, San Francisco, CA, USA: Jossey-Bass, 2001.

[10] Cloud Security Alliance (CSA), "CSA Security, Trust and Assurance Registry (STAR) Overview", available at https://cloudsecurityalliance.org/star/, 2015.

[11] S. Waddington, J. Zhang, G. Knight, J. Jensen, R. Downing, and C. Ketley, "Cloud repositories for research data--addressing the needs of researchers",*Journal of Cloud Computing: Advances, Systems and Applications*, Vol 2, No 1,2013, pp.1-27.

[12] M. Anita,"ThreeProblemsCloudSecurityCertificatinCanSolve", https://blog.cloudsecurityalliance.org/2010/05/17/3-problems-cloud-security-certification-can-solve/, 2010.

[13] S.M. Habib, S. Ries, and M. Muhlhauser, "Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation", *In the Seventh International Conference on Ubiquitous Intelligence & Computing and Autonomic & Trusted Computing*, 2010, pp. 410-415.

[14] S.M. Habib, V. Varadharajan, and M. Mühlhäuser, "A framework for evaluating trust of service providers in cloud marketplaces",*In the Proceedings of the 28th Annual ACM Symposium on Applied Computing*, 2013, pp. 1963-1965.

[15] Hosting-Review,"Top 10 Database Hosting Review", Retrieved 24.01.2014, 2014, from http://www.hosting-review.com/hosting-directory/top-10-lists/Top-10-Database-Hosting-Companies.shtml

[16] Top10CloudStorage, "Comparison Table for Cloud Storage", available at http://www.top10cloudstorage.com/compare-specs/.

[17] V. Varadharajan,"A note on trust-enhanced security", Security & Privacy, IEEE, Vol 7, No 3, 2009, pp. 57-59.

[18] S.K. Garg, S. Versteeg, and R. Buyya, "SMICloud: A framework for comparing and ranking cloud services", In *Fourth IEEE International Conference on Utility and Cloud Computing (UCC)*, 2011, pp. 210-218.

[19] W.P.E. Priyadarshani, G.N. Wikramanayake, and E.M.P. Ekanayake, "Measuring Trust and Selecting Cloud Database Services", *Advances in Computer Science: an International Journal*, Vol. 2, 2013, pp. 114-120.

[20] M. Tsvetovatyy, M. Gini, B. Mobasher, Z.W. Ski and W. Ski, "MAGMA: an Agent-Based Virtual Market for Electronic Commerce", *Applied Artificial Intelligence*, Vol. 11, 1997, pp. 501-523.

[21] J.M. Ferris, and D.P. Huff,"Systems and methods for multiple cloud marketplace aggregation", Google Patents", 27.05.2010, available at http://www.google.com.jm/patents/US20100131624.