J. Appl. Environ. Biol. Sci., 5(9)76-83, 2015
© 2015, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Case Study: Cloud Computing Consumer Protocol in Australia

Kalum Udagepola[1,5], Li Xiang[2], Naveed Afzal[3], Mahboob Ali[4], Mike Robinson[1]

[1]Department of Information and Computing Sciences, Scientific Research Development Institute of Technology Australia (SRDITA) Brisbane, Australia
[2]College of Computer and Science Technology, Harbin Engineering University, Harbin, PR China
[3]Department of Biomedical Informatics, Mayo Clinic Rochester, MN, USA, 55901
[4]Faculty of Computing and Information Technology, University of Jeddah, Jeddah, Saudi Arabia
[5]School of Information Technology Communications, American University of Nigeria, Adamawa State, Nigeria

Received: May 3, 2015
Accepted: June 26, 2015

ABSTRACT

Cloud computing can be separated into three major categories, namely private clouds, public clouds and hybrid clouds. These categories are facing a gauntlet of challenges, including data privacy and data security between cloud service providers and their consumers. In order to address these challenges and elicit suggestions and useful information from vendors and consumers, the Australian Computer Society (ACS) circulated a discussion paper in July 2013. The ACS received a number of submissions from various prestigious and globally prominent organizations. The objectives of this case study are to analyze and explore the emerging threats and challenges in the public cloud environment. In this paper we have collected procedures and recommendations on how Australian organizations might deal with the relative opportunities, risks and challenges associated with this topic. Efforts to produce a protocol that includes ways to address lack of confidence and strengthen consumers' trust are ongoing with cloud computing.
KEYWORDS— cloud computing; data integrity; consumer protocol; privacy policy

I. INTRODUCTION

The work at hand presents a discussion on cloud computing protocols as a means to resolve Cloud Computing (CC) issues - mostly for the consumer (security, reliability, privacy) and the provider (business case) - based on questions and answers of a discussion paper prepared by the Australian Computer Society.

This paper analyses potential threats and challenges of consumer cloud computing in a public cloud environment, and suggests some strategies and recommendations that service provider organizations may need to consider in order to improve the quality of their service and build up consumer trust.

CC has attracted a lot of interest in the recent past. Many organizations have attempted to explain CC in simple and general ways. However, CC has a complex architecture that extends over arrange of underlying technologies, configuration possibilities, and service and deployment models. After paying a sum of money as an access rent, consumers can make use of fully featured CC applications, including their environment and computing infrastructure resources, such as network-accessible data storage and processing [1].

CC provides services to businesses and/or consumers via a cost-effective, scalable, flexible, and proven delivery platform. Regardless of how attractive public cloud services are, they pose significant security risks to applications and data beyond what is expected using traditional on-premises architecture. Evidently, public CC services always involve a high risk-level because essential services are often outsourced to third-party service providers. The resulting process makes it complicated and cumbersome to maintain data security, privacy and support, while demonstrating compliance and service availability. Software-as-a-Service (SaaS) can cut the overall cost of hardware and software development, maintenance, and operations. Platform-as-a-Service (PaaS) can lessen the cost and complexity of buying, housing, and handling the hardware and software components of the platform. Infrastructure-as-a-Service (IaaS) can be deployed to avoid buying, housing, and supervising the elementary hardware and software infrastructure components [2]. CC comes in different forms and public offerings (IaaS, SaaS, PaaS); it also inherits its own security issues. Furthermore, there is no globally accepted industry standard/protocol to endorse or validate the security compliance or maturity level of CC environments. Such international standards and frameworks are still in the process of development (e.g., ISO, cloud security alliance).

Corresponding Author: Kalum Udagepola, Department of Information and Computing Sciences, Scientific Research Development Institute of Technology Australia (SRDITA), Brisbane, Australia.& School of Information Technology Communications, American University of Nigeria, Adamawa State, Nigeria. Email: kalumu@srdita.com.au

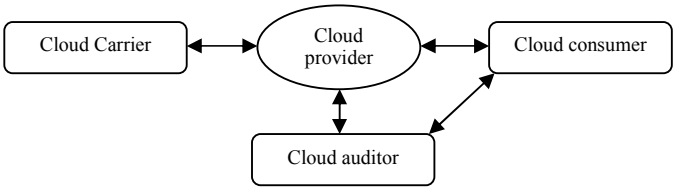

Fig. 1. United States Department of Commerce's National Institute of Standards and Technology defined cloud [3].

Fig. 1 demonstrates interactions between the major components of the National Institute of Standard Technology (NIST) framework for providing cloud services. The cloud carrier interacts mainly with the cloud service provider, while the other associations could be categorized as one-to-many relationships.

Despite perceived threats, vulnerabilities and risks in cloud environments, the global trend of adopting CC increases rapidly. There is a growing need to address the prevailing concerns and upcoming trends in information security and data privacy in public cloud environments. Other areas of concern are: new attacks as they surface; the need for common frameworks and compliance standards; and possible solutions to these problem areas [4].

CC is facing many challenges. The challenges are largely focused around scalability, huge collections of data due to the internet revolution, a large increase in the number of people who make use of these services, the amount and speed of data transfer, and the increasing variety of unusual circumstances applicable to CC.

The popularity and emergence of CC have transformed the way individual consumers and small businesses store and use data. However, CC also involves many risks for consumers, risks which must be carefully managed. According to a cloud survey report in 2013[5], 65% of organizations list security as one of their top concerns in implementing CC, 73% cite reliability as the most important factor in selecting a cloud partner, and 70% are in the process of implementing cloud or already have applications in the cloud.

II. CLOUD COMPUTING IN AUSTRALIA

A considerable market exists for CC services in Australia. A majority of Australians use CC services as consumers of webmail and social networks. Significant numbers of Australians regularly use Facebook and YouTube, both of which are CC applications although many people would not recognize or consider them as 'cloud' [6]. The rapid rise of CC services has also provided a huge opportunity to small businesses to find new customers, and for suppliers to conduct their business in a more efficient and effective way[7]. In April 2013 Deloitte conducted a survey [8] to study the impact of the web on 500 Australian small businesses. The survey showed business uptake as follows: high digital engagement (16%), medium (25%), low and very light (24%), and not using the Web at all to reach customers (35%). Moreover, the survey revealed that small businesses which use the web and its services grow two times faster than those that do not.

ACS is trying to understand CC consumers' needs and promote good industry practices for CC in Australia. In order to attain this goal, in July 2013 the ACS published a discussion paper to stimulate recommendations and guidelines both from vendors and consumers of CC services regarding data protection, data privacy, and the use of such services with confidence and a high level of trust. In the discussion paper the ACS raised seven main questions and asked for feedback from leading CC service providers and consumers. We will discuss these questions and their respective feedbacks one by one in the following sections.

III. A VOLUNTARY PROTOCOL

The discussion was open to vendors and consumers of CC services to canvass their ideas about a voluntary protocol in which cloud suppliers disclosed undertakings and information about their services that would result in increased market assurance and enhanced adoption and take-up of CC services.

In response to this question, many cloud service providers (such as Google and Microsoft) argued that there is no need for a voluntary protocol as there are already many existing CC industry codes, and enforcing a new protocol would create more confusion among consumers and service providers. Google, one of the leading cloud service providers, claimed the proposed protocol would have a negative impact on the fast-growing Australian cloud service industry, and as a result their reputation would suffer globally. Microsoft responded that the protocol needs to be clear about its objective and purpose. Moreover, they believed the protocol should not become a mandatory requirement for

procurement. In their view, many legislative protections already exist, such as Competition and Consumer laws and the Privacy Acts, which offer acceptable security for cloud consumers [9, 10].

In response to this question, many cloud consumers supported the idea of having such a protocol, as it would make the whole process more transparent and understandable from a consumer's perspective. Moreover, the protocol would provide a simple way for consumers to validate and evaluate their cloud service providers according to their needs and requirements.

IV. KNOWLEDGE ABOUT CLOUD COMPUTING AND ITS BENEFITS TO BUSINESS

Many cloud service providers agree that they strongly support transparency and privacy relating to consumers' data. They argued that instead of introducing new rules and regulations, which would have a negative impact on the growing industry, it would be better to create more awareness among consumers by educating them about issues relating to consumer requirements. Meanwhile many consumers reported that there is a strong need for more clarity from service providers, and providers need to take a more balanced approach when stating CC benefits. They should also disclose the total costs and other impacts of externally hosted arrangements such as data protection, data backup and service reliability. In this way, consumers would be in a better position to evaluate the advantages and disadvantages of CC services offered by providers.

V. OTHER CONCERNS ABOUT CLOUD COMPUTING FROM CONSUMERS' PROSPECTIVES

Potential or present users of cloud services should have a much better overview of CC than is presently the case, and the numerous practical experiences of users could be very useful in formulating a protocol.

In response to this question many consumers reported the following major concerns: being unaware of hidden terms and conditions; portability constraints; and offshore hosting. They stressed the need for service models that are more transparent and more easily understood by consumers.

Service providers need to give more information to consumers in regards to on-shore/off-shore storage, relevant jurisdiction, privacy regulations, data ownership, and data security. Moreover, cloud service providers should disclose complete details regarding physical and online access control to prevent unauthorized access to consumer data.

VI. OTHER DISCLOSURES FROM CLOUD VENDORS

Cloud vendors possess much more information than ACS obtained via these research questions. Pioneer Australian Telecommunication Company gave numerous unexpected responses in this regard, responses that were industry-oriented, practical, and very valuable.

The major telecommunication supplier in Australia is Telstra. In their response Telstra said a protocol might be useful in promoting disclosure within the different categories of information mentioned in section IX of this paper. Telstra recommended that customers should seek detailed information from service providers, but unless there is evidence of market failure it would be counterproductive to propose a regulatory scheme that dictates disclosure of very specific information.

Telstra also recommended that, given the wide range of cloud services as well as the size and scope of providers, information provided to CC customers regarding CC products should be precise, comprehensive, honest and relevant to consumer concerns and needs.

Given the concerns articulated in the most-recent MYOB (commercial accountancy software) survey that Australian business operators basically do not have time to understand cloud services because of other demanding priorities, it would be counterproductive to over-burden customers with compulsory disclosure information that may not be important.

Furthermore, Telstra recommended that, rather than forming a new regulatory scheme, the protocol should be articulated in a way that would allow providers to achieve better compliance using current consumer protection and privacy legislation. This would strengthen the role of existing Australian legislation in this area, and give agencies implementing the legislation a single and predictable set of regulatory requirements appropriate to CC providers.

Major impacts of regulatory duplication would include: additional regulative difficulty, an upsurge in the price of cloud products, possible smothering of innovation or discouragement of entry by new suppliers, questions about which regulator has authority (and a possible result in forum shopping) without offering the regulatory certainty that is required.

Duplication of regulations also raises questions about any additional remedy consumers and small businesses would achieve from a mandatory protocol. It is unclear what practical penalty a vague disclosure document would attract under the protocol, or how suppliers could be forced to alter disclosure documents. As mentioned in the ACS discussion

paper, protections exist under Australian consumer law (ACL) against false and deceptive claims made in disclosure documents.

A protocol that enforces strict disclosure requirements is only as good as the information it discloses. The danger of an excessively autocratic disclosure regime is that cloud providers will reveal only what is required by the protocol and nothing more. Strict disclosure requirements will not be adequate to respond to market failures, evolving technology, or new concerns that may arise; as opposed to existing regulations that address unfair terms, privacy and deceptive behaviour.

An additional concern with compulsory disclosure of specific categories of information is that disclosure, in some instances, might be used to deceive customers. For example, disclosure of data location might be used to suggest that the pertinent type of data is subject to a compulsory on-shoring obligation. Under Australian law, customers have a choice on data location and may be able to obtain cost and other benefits through using an offshore provider. This is a classic example of the risk created when very granular disclosure is mandated, rather than relying on the integrity of information provided to the customer.

Regardless of best efforts, no list of mandatory disclosure topics will ever be complete because technology and service development change rapidly. The risk of using a specific list of mandatory disclosures is that consumers will derive a false sense of security that all necessary concerns have been addressed. The managers of a self-regulatory scheme have to ensure that a diverse range of individual consumer requirements are catered for, so that consumers can have confidence that their needs are as safe as they would be under a compulsory disclosure scheme.

In the case of offshore providers of CC services into the Australian market, the prospect of those providers signing up to a compulsory disclosure protocol is very low. National providers need to be able to operate on a level playing field in terms of compliance costs, and that level playing field is already provided under ACL. Offshore providers already supply services to Australian consumers. In any event, ACL has extra-territorial application that extends to conduct engaged in outside of Australia by Australian corporations, and by foreign corporations conducting business in Australia.

Access controls prevent unauthorized access to cloud data, and the process by which this is achieved should be clearly describe to consumers by cloud service providers. They must show that their services have adequate access controls. Cloud providers must ensure they have internal auditing systems even though clients' data resides in a public cloud environment. Consumers must know the exact location of data centers. This information should be adequate to select a hosting provider with certainty and security. Hosting providers should give data segregation guarantees because most public clouds are in a shared environment. A disaster management plan would improve consumer confidence, assuring customers that their data is safe and could be recovered in the event of any catastrophe. Consumers will be attracted to service providers who implement suitable disaster detection and recovery procedures. Consumers constantly pursue business development. Service providers who guarantee a portable data solution without lock-in will attract consumers looking for business security and continuity [11].

VII. CLOUD COMPUTING ISSUES

In Australian, the majority of telecommunications is controlled by Telstra, which has highlighted numerous problems in the sector regarding privacy, data location and data security.

The telecom giant is responsible for data security and compliance with applicable privacy laws. It would be helpful if the ACS explicitly invited consumers and businesses to outline their experiences with these particular issues, and advise whether they are aware of the applicable Australian legislation and the regulatory agencies with which they can raise their concerns, and whether the available remedies assisted them.

In terms of corporate identity and data location disclosure, the Australian Privacy Principles scheduled to begin in March 2014 would require Australian providers of cloud services to inform their customers if they are planning to send personal data overseas, and if so to where that confidential data would be sent [12].

There is a need for a regulation that deals with data breaches, but it is appropriate for this to be done under existing privacy laws. In this way, it has more general application rather than addressing it separately in a prescriptive protocol that has more limited application. The ACS discussion paper acknowledges that draft legislation has been proposed and been passed by the House of Representatives.

For some consumers data location may be highly significant, but Telstra cautions against placing excessive emphasis on the issue of data location. For example, a provider might host data offshore but offer superior security for that data compared to a provider who is onshore.

Telstra acknowledged that vendor lock-in is an issue that can arise due to disparity in negotiating power between the cloud provider and the consumer. However, here again ACL offers satisfactory protection against unfair terms and conditions. Unfair contract terms under ACL apply to services that are purchased by individuals for personal, domestic

or household use or consumption. Accordingly, cloud services purchased by consumers for individual use would be covered by [13] and Australian Consumer Law, s23 (3).

In respect of concerns associated with the quality of CC services offered to consumers and small businesses, ACL already provides satisfactory protection through a legislative guarantee. The legislative guarantee applies to services costing less than $40,000 (consumer and business) and to services that are normally acquired for personal domestic or household use. For instance, under ACL there is a guarantee that services will be rendered with due care and skill. There is a guarantee that services and the products of those services are reasonably fit for any purposes that the consumer made known to the supplier (expressly or by implication, Australian Consumer Law, Part 3-2). ACL also provides consumers with real remedies if a cloud service fails to comply with a statutory guarantee (Australian Consumer Law, Part 5-4). The execution of the guarantees is a statutory responsibility of the Australian Competition and Consumer Commission [14].

VIII. PRESENT STATE OF MARKET CONFIDENCE IN CLOUD COMPUTING

Cloud service providers provided feedback regarding current market confidence in CC, which highlighted several major issues regarding consumers.

According to Telstra's experience, as customers develop greater understanding of the benefits of cloud and test the services more frequently, their usage levels rise significantly. An initial investment in education and awareness about the benefits of cloud services seems to provide an increasing return over time as consumers develop understanding and trust. Consumers also have a wide range of approaches: some start more cautiously with trial services whereas others launch straight into production systems. It would be valuable to understand why consumers' approaches differ in this way. Furthermore, Telstra says it is important to recognize that consumers use a variety of cloud services, from premium services to virtual private cloud (VPC), as well as 'commodity' cloud services. Consumer experiences and their confidence levels in these differing service 'flavors' may be divergent given their different characteristics and applications.

Telstra believes that the current state of CC market confidence is relatively high, but there is room for further improvement through education and demonstration of the benefits of CC, particularly to consumers, small and medium sized enterprises, along with not-for-profit organizations.

According to Google, there are numerous reasons why consumers and small businesses are failing to adopt cloud services to their full potential. The main questions they highlighted in this regard are: lack of understanding regarding the role of technology; what to do with existing technology; and time and cost. A large number of small businesses are already use CC facilities, but lack of education keeps them from achieving its full usage potential.

Current consumer and privacy laws provide a robust regulatory protection framework between consumer and provider, but a new self-regulatory regime may negatively influence the market. According to Google's research CC is not the problem from the consumer viewpoint: the main issue is what kind of benefits consumers can get from using CC services, which leads back to the issue of awareness and education.

There are huge potential benefits in the uptake of CC technology for small business. Presently, 95% of small businesses are using emails, primarily webmail, which is actually Internet/Web computing. Google says the acceleration of CC in the market is growing at a rapid pace. The CC market is already exhibiting many characteristics of developing markets, and CC providers are continuously guarding their reputation by delivering superior product quality.

According to IDC research data, public cloud spending could reach $98 billion in the next two years, which demonstrates a growing confidence level among CC consumers. Microsoft believes any potential concerns can be overcome by promoting CC information and education. However, the final analysis belongs to consumers; CC providers must ensure the availability of analytical, educational and comparison tools.

Introduction of a self-regulatory protocol might make things worse than they are currently. Introduction and implementation of additional protocols might result in confusion and panic, not only from the vendors' point of view as prices might have to increase to encompass new protocols, but eventually it might affect the entire CC market. Small business and individuals might avoid the CC market because of price unattractiveness.

The Australian Privacy Foundation in their response highlighted the following key concerns from consumers' perspectives: service providers must accept privacy impact assessments; service providers must provide detailed security information and avoid privacy risks to consumers using CC products; and service providers must give users full access control to their products [15].

IX. A VOLUNTARY PROTOCOL COMPLEXITY WITH PRESENT GLOBAL CLOUD STANDARDS

A voluntary protocol has jurisdictional complexities, along with potential compliance costs and the interaction problem between current global protocols and other cloud standards.

Telstra's view is that there is no need for such a protocol as no case has been made for the introduction of a detailed and prescriptive compulsory disclosure scheme that would overlap existing consumer protection and privacy law, and involve significant costs for all participants.

Conversely, if a protocol was established in the form of educational guidelines and key questions that customers should ask from the service providers, then it could summarize or link to the existing resources and information available. The CC synopsis and recommendations published by NIST are a well-known example [16]. There is no lack of good information, but the information is mostly presented at a level of detail that can be overwhelming; making it consumer-friendly and easily accessible requires hard work. Generating regulatory schemes may create the illusion of action but does not replace the necessity for providing effective communication. Compliance costs may be difficult to determine. However, a community-informed "cookbook" of best practices would be a cost-effective first step. Reliance on community input may need due diligence to certify that feedback is not tainted by bias. Enterprises or regulators may want to consider automating the remote monitoring of cloud services for real-time and historical trend analysis of cloud service performance. It should be a regulator or an independent organization that chooses to offer this monitoring service. It may be possible to cover costs by offering a snapshot overview to the public, followed by a more detailed paid report for interested enterprises [17].

X. DISCUSSION

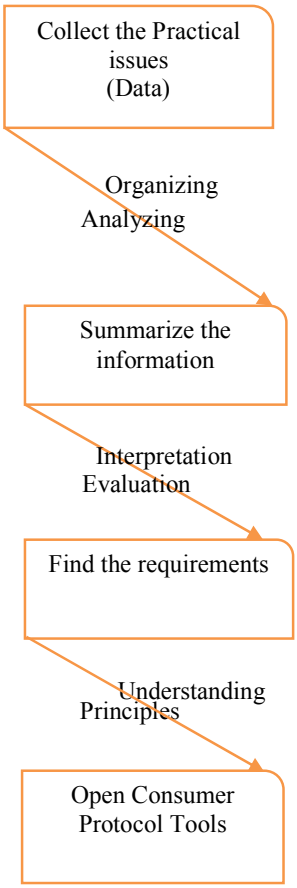

Fig. 2. Block diagram of the case study

Fig. 2 illustrates a summary of our case study. We believe that, in this modern era of technology where the world is becoming a small global village, there is a growing need for an international CC standard/protocol rather than having various regional standards/protocols that will have a detrimental impact on the growing CC industry in Australia. Moreover, introduction of unnecessary self-regulation will impede growth and development in this sector. A global standard/protocol should encourage and promote good industry practice for a safe, secure and trusted CC industry globally.

We completely agree that consumers have genuine concerns regarding issues such as transparency, quality of services, data security, offshore data hosting and data privacy. In our opinion these concerns can be dealt with by educating consumers regarding the CC industry so that they will be able to do their own due-diligence in order to find services that are suitable for their specific needs. Moreover, cloud service providers need to take initiatives that improve the trust of consumers in their services. Security is a crucial and critical factor to the success of a cloud service provider. Many cloud service providers are investing large sums of money in making their services secure. For example, Google, one of the leading cloud service providers, is currently investing billions of dollars in data security by hiring expert security professionals and streamlining the overall process of their services.

XI. CONCLUSION

The Australian Computer Society collaborated with the National Standing Committee on Cloud Computing, the Australian Information Industry Association and other government and industry stakeholders to develop a voluntary CC protocol to encourage information disclosure by cloud providers, and support consumers of cloud services in being well-informed.

Overall, the CC industry has to implement strong measures regarding data security and data privacy; it has to explain these measures to its consumers in a more concise and user-friendly manner; it must assure consumers that their data is in safe hands; and it must be seen to be following best industry practices.

Acknowledgments

The work is fully supported by Scientific Research Development Institute of Technology Australia (SRDITA). The authors would like to thank the ACS for playing a major role in assembling the industry's views. This case study used many details provided in the responses provided by 500 Australian companies. The authors sincerely thank Logan City Council, QSR International, OzHub, Telstra Corporation Limited, Mr. Holly Raiche, Mr. Philip C. Roberts, Microsoft, Google, the Australian Information Industry Association, Coca Cola Amatil CIO, the Australian Communications Consumer Action Network, Australia's Academic and Research, Brereton Consulting, Xamax Consultancy Pty Ltd, the Australian Privacy Foundation, NAB Technology, Information Integrity Solutions Pty Ltd and Communications Alliance.

REFERENCES

1. Julisch K. and Hall M. (2010), Security and Control in the Cloud, Information Security Journal: A Global Perspective, vol. 19:2099-309.
2. Jansen W. (2011), Cloud Hooks: Security and Privacy Issues in Cloud Computing, Proceedings of the 44th Hawaii International Conference on System Sciences(HICSS-44). Kauai, HI, USA 4-7 January. University of Hawai'i at Manoa, HI, USA.
3. Samba A.(2012), Logical Data Models for Cloud Computing Architectures, IT Pro January/February 2012, IEEE Computer Society, pp. 19-26.
4. Svantesson D. and Clarke R. (2010), Privacy and Consumer Risks in Cloud Computing, Computer Law and Security Review, vol. 26: 391-397
5. Symantec (2012), http://www.findwhitepapers.com/force-download.php?id=29085, Accessed 04 May 2015
6. http://www.socialbakers.com/facebook-statistics/australia, Accessed 04 January 2015.
7. Deloitte Access Economics, "Connected Continent," 2013, http://goo.gl/lQJTto, Accessed 04 December 2014.
8. Deloitte Access Economics, "Connected Small Businesses," 2013, http://goo.gl/p3V4kK, Accessed 04 January 2015.
9. Ziyuan W.(2011), Security and Privacy Issues within the Cloud Computing, The 2011 International Conference on Computational and Information Sciences (ICCIS). Chengdu, Sichuan, China, 21 – 23 October, Southwest Petroleum University, Sichuan, China, pp. 175-177.
10. Ullah K and Khan M. N. A. (2014), Security and Privacy Issues in Cloud Computing Environment A Survey Paper, International Journal of Grid and Distributed Computing 7(2): 89-98.
11. Almulla S. A. and Yeun C. Y.(2010), Cloud Computing Security Management, Second International Conference on Engineering Systems Management and Its Applications (ICESMA), 2010.
12. http://oaic.gov.au/images/documents/migrated/2010-11-25052337/privacy-and-the-cloud.pdf, Accessed 04 January 2015.

13. Hamlen K., Kantarcioglu M., Khan L., and Thuraisingham B. (2010), Security Issues for Cloud Computing. International Journal of Information Security and Privacy, vol 4(2): 39-51.

14. http://www.accc.gov.au/publications/compliance-and-enforcement-policy, Accessed 04 January 2015.

15.Zia A., Khan A. and Naeem M. (2012), Identifying Key Challenges in Performance Issues in Cloud Computing, International Journal of Modern Education & Computer Science, vol. 4(10): 59-68.

16. Badger L., Grance T., Patt-Corner R. & Voas J. (2012), Cloud Computing Synopsis and Recommendations. Available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075, Accessed 04 December 2014.

17. https://www.acs.org.au/__data/assets/.../ACS-Cloud-Discussion-Paper.doc, , Accessed 09 June 2015.