User Concerns on Cloud Security – A UAE Perspective

Maurice Danaher
Associate Professor, College of Technological Innovation
Zayed University
Abu Dhabi, United Arab Emirates
Email: Maurice.Danaher {at} zu.ac.ae

Choo Je Chong
Adjunct Professor, College of Business
Zayed University
Abu Dhabi, United Arab Emirates

Abstract— **Cloud computing is a technology that offers many benefits to users including access from anywhere and paying only for resources that are consumed. However there are many risks associated with cloud usage and a major area of concern for many users is the risk of privacy breaches. Studies in various countries have reported security and privacy concerns as the most significant barriers to cloud adoption. In the research described here a survey was conducted of 225 tertiary educated Internet users in the United Arab Emirates. The purpose of the survey was to explore user perceptions of privacy in cloud computing and also to explore their awareness of the privacy risks. The users were unrelated individuals working in a variety of occupations in different locations in the country. Our results show that users consider cloud services to be intrinsically insecure and do not trust service providers to keep their data private. In this paper we discuss the issue of privacy and the legal status of privacy protection in the UAE. We present the results of our study and discuss the findings. We make recommendations for possible measures that could be taken in the UAE to allay the concerns of potential users and facilitate greater uptake of cloud services.**

Keywords – cloud adoption, barriers, privacy, confidentiality, trust

I. INTRODUCTION

Cloud computing is a technology approach that can benefit almost every organization or user that consumes IT services. The cloud is a virtualization of resources such as servers and other computers, networks, applications, data storage and services to which the end user has on-demand access. The systems are configured in such a way that they can be shared by many organizations or individuals. Cloud services are provided to the user without the need for the user to have any knowledge of the underlying systems.

A major difference between the cloud and traditional approaches is its scalable and elastic nature. Cloud computing provides the flexibility of quickly scaling up or down thus adjusting to demand. Other benefits of cloud computing include: access to a huge range of applications; access from anywhere in the world; avoiding expenditure on hardware and software and maintaining systems; paying only for resources that are consumed.

The primary models of cloud computing service are Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service. These cloud services may be offered in a public, private or hybrid network. Software-as-a-Service is a software delivery model in which software and associated data are centrally hosted on the cloud e.g. GoogleDocs and Salesforce.com. Platform-as-a-Service is a category of cloud computing services that provides a computing platform and a solution stack as a service e.g. Google App Engine and Microsoft Azure. In Infrastructure-as-a-Service providers offer processing (virtual machines), storage, networks and other resources e.g. IBM SmartCloud.

There are many benefits to be derived from cloud computing, however there are also many risks associated with it [1,2]. These include: user's data is residing on a machine owned and controlled by someone else; responsibility for the security of the data lies in the hands of the service provider; users could become dependent on service provider; problems could arise when changing service providers or if the service provider shut down; service problems from the provider could have a serious negative impact on the user's business.

While there are numerous risks to users of cloud computing the focus of this work is on the risk to the privacy and confidentiality of information. The users of cloud computing depend upon service providers to safeguard their private information and critical data and applications. Any violation of the privacy of the users' information could, as well as cause them a major problem, expose them to serious problems if they have clients or customers.

Many organizations around the world are stepping into this new mode of computing. In the UAE more users are adopting the technology [3] so it is becoming increasingly important for users and businesses alike to better understand the issues associated with cloud computing. Of particular importance is the question of how we can take advantage of benefits of the various types of cloud services while still preserving privacy and confidentially of information.

The purpose of the study described in this paper was to explore user perceptions of privacy in cloud computing and also to explore their awareness of the privacy risks. By better understanding user's beliefs, awareness and knowledge steps

can be considered on how to best address the issues here in the UAE.

II. Privacy Issues of Cloud Computing

In the past few years various researchers have published reports describing privacy and confidentially issues and challenges in cloud computing, e.g. [1, 2, 4, 5, 6, 7, 8]. A summary of the most significant issues described in these reports is presented here. A fundamental point is that when an entity discloses or stores information with an outside party such as a cloud service provider, the information may have fewer or weaker privacy controls than when the information remains only in the possession of the entity. The terms of service and privacy policies may not provide adequate protection to users and indeed many users may not fully understand the terms of service. Providers may even reserve the right to change their terms and policies at will. The secondary use of user's information by the service provider may breach laws under which the information was originally collected. Service providers acquire transactional data on the user that may have commercial value, or that could be used for any purpose that the provider chooses. It may be easier for private litigants or government agencies to obtain information from a third party than from the original owner. A cloud provider might even be compelled to search through a user's data for information that may be of interest to private litigants or government agencies. Information stored on the cloud may be subject to the laws of other countries. The country where the physical machine is located may very well be different from the country of residence of the user. Further, the cloud provider may move the user's data to machines in other countries of business of the provider thus involving different jurisdictions with differing legal consequences. Additionally, there is a possibility of more jurisdictions due to locations of communications equipment, or locations where the user may communicate with the provider. Some jurisdictions may require that service providers report to the police any material that they find on their systems that is illegal. It may be that governments could require service providers to monitor their systems for illegal activity such as copyright violation, or for criminal or offensive behavior. A user could possibly be prosecuted for having illegal copies of video, music or software. A service provider could possibly be required to monitor the activities of particular types of users such as a suspected sex offender.

A big issue in all of this is the lack of any clear understanding of the legal position. Laws lag some considerable period of time – years – behind technology. Current laws related to IT and data protection may or may not be applicable to cloud technology. Further, the result of the application of old laws to new technology issues can be unpredictable.

III. Legal Status in UAE

Privacy and confidentiality are constitutional rights in the UAE and granted as follows in the constitution: "Freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law" [9]. Privacy and confidentiality is also addressed in other laws. The Penal Code of the UAE [10] provides protection by prohibiting interception of data and prohibiting any disclosure of private and confidential information. Severe penalties are in place for violations of the law. The Electronic Commerce and Transactions Law [11] is a law specifically aimed at privacy and confidentiality of electronic data and provides for significant penalties for breaches of the law.

A review by the author of existing legislation in the UAE revealed that there are no laws, regulations and/or official standards specifically in relation to cloud computing services. This is corroborated by Cruz [12] in an article discussing legal risks associated with cloud computing in the UAE .All laws that refer to privacy and confidentiality would apply to cloud services. In the absence of a legislative framework users enter into a contract with the service provider in a relationship of trust

Typically the cloud services are offered to the user "as is", without the cloud provider accepting any risk. It would be difficult in the event of a security breach for a user to successfully make a claim against a cloud provider outside the scope of contractual rights. A user would need to prove breaches of law on the part of the provider.

IV. Results of Survey in UAE

A study was conducted in the United Arab Emirates in order to explore awareness among IT users of privacy issues associated with cloud computing. We wished to learn about what privacy concerns they may have, their awareness of privacy risks, their awareness of legalities and their awareness of the privacy protection provisions in contract terms and conditions.

A survey consisting of multiple choice questions with provision for comments was developed and presented to participants using SurveyMonkey. 225 regular Internet users in the UAE were surveyed. The respondents were unrelated individuals working in a variety of occupations and living in different parts of the country. All were tertiary educated and 95% of them were using the Internet for more than 5 years. The respondents were using the Internet daily and the average usage was about 5 hours per day. They used a variety of services including social networking, email, office suites, platform services, and media storage. The main results are summarized below. The percentages have been rounded to the nearest 5%, a level of accuracy appropriate for this discussion.

- 30% stated that they did not understand the meaning of the term Cloud Computing. However, after an explanation of what it encompassed all agreed that they either were using it or aware of it.
- 80% do not trust cloud service providers to maintain the privacy of the information that they disclose to them or store on their systems.
- 75% believe that service providers have access to all information that they may store on the cloud

- 85% do not want to disclose personal information to service providers
- 85% believe that data placed on the cloud cannot be kept secure
- 85% believe that private information should not be stored on the cloud
- 85% do not believe that all their data would be permanently deleted after they deregistered from a service
- 80% do not know where (i.e. geographical location) the data is stored on the services that they are using
- 50% of respondents do not know if the UAE has any laws in relation to privacy or security of data placed on the cloud or disclosed to service providers.
- 30% of the users read the privacy notices
- 70% felt that privacy notices were too difficult to understand

V. Discussion of Results

30% stated that they did not understand the meaning of the term Cloud Computing. However, after an explanation of what it encompassed all agreed that they either were using it or aware of it.

In our survey of relatively well-educated users it was found that nearly one third did not understand the meaning of the term but after an explanation they realized that they were using it in some form or at least they were aware of it. While cloud computing is very much at the forefront of discussion topics among the IT community in recent times, the fact that some users do not understand the term suggests a possible lack of awareness of cloud related security and privacy issues.

80% do not trust service providers to maintain the privacy of the information that they disclose to them or store on their systems.

It is very evident from this result that the question of trust is a big issue. Users do not have complete trust in the service provider to maintain the privacy of information that they place on the service provider's system or that is given to or otherwise obtained by the service provider. This lack of trust is in line with findings by researchers in other parts of the world e.g. [1, 13]. Typically users feel that when their information is on the system of some outside party they cannot trust the party to keep it as secure as if it was on their own system.

75% believe that service providers have access to all information that they would store on the cloud.

Since users are placing their information on systems in the cloud provider's datacenter rather than on their own computers the majority believe that the service provider has access to their information. A minority believe that the service providers have restrictions on access to their information. Some commented that if they use encryption the provider can't access their data; while others commented that the provider would have to ask them for permission. If the majority feel that the cloud providers can access their information then that would deter them from storing private information. The suggestion by some that encryption would prevent unauthorized access to their data is in line with that of researchers e.g. [14].

85% of users do not want to disclose personal information to service providers

Most users probably do not want to disclose personal information because they sense that it may not be kept completely private. Some commented that they only disclose personal information if necessary, such as when opening an account. Others said that providers sometimes ask for information that is not necessary and they do not want to give the information. Others said that they prefer to remain anonymous, if possible, when using a cloud service. Some commented that their personal information may be used for other reasons such as given to organizations who will send them advertising material. According to Culnan & Armstrong [15] collection of information and subsequent usage should follow certain principles of fair use. It may be that some providers in the UAE are requesting more personal information than is necessary and that is a cause for concern.

85% believe that data placed on the cloud cannot be kept secure and that private information should not be stored on the cloud

Most of the respondents believe that it is not possible to keep data completely secure on the cloud. Many comments were along the line that when information is placed on a system that you do not personally control you cannot be completely certain of the security immaterial of assurances and guarantees you may receive. Comments by some were that data stored on cloud could possibly be viewed by other parties, such as the cloud storage providers, hackers, or law enforcement agencies. However, a small minority believe that data can be kept secure and a few respondents mentioned that if they use encryption no one could ever access their data. The opinion of the majority of users on this point is in line with that of many researchers i.e. that privacy cannot be guaranteed and that information may possibly be accessed, for example, by law enforcement agents [7].

85% do not believe that all their data would be permanently deleted after they deregistered from a service

Most of the users believe that their data could be retrieved later by the service provider even though it was deleted after deregistering from a service. Some commented that the providers maintain archives and others said that electronic

records can be retrieved in many cases even though they had been deleted.

80% do not know where (i.e. geographical location) the data is stored on the services that they are using

Users generally had no idea of where their data was stored. Some commented that they believe they should be told. Others said they thought it made no difference where the information was stored. We can deduce from this that most users do not consider it important to know where their data is stored. This further tells us that users have not considered the possible legal implications of their data being stored in a jurisdiction outside the UAE. The location of the cloud provider's systems poses a risk and possible negative impact on a user.

50% of respondents do not know if the UAE has any laws in relation to privacy or security of data placed on the cloud or disclosed to service providers.

The purpose of the question was to see if users had considered legal aspects of privacy before using cloud services. From the response it can be seen that half of the respondents had not previously considered it. Some commented that they assume that normal privacy laws would also be applicable to the cloud. The fact that half of the respondents do not even think about legal aspects of privacy indicates that there is a lack of understanding of the importance of legal protection and requirements.

30% of the users read the privacy notices

Only a minority of respondents read the privacy notices. Users commented that they take too long to read and are probably all the same. They also commented that if they want to use a particular service they have no choice but to accept the policy. This result indicates that the majority of users are not aware of the terms and conditions and do not know what rights or protection they have. A study by Ion et al [16] found that users believe they have more rights and protection than the cloud provider actually grants them.

70% felt that privacy notices were too difficult to understand

The majority of respondents felt that the privacy notices were too difficult to read. Comments were made that the notices should be short and simple to read. Some commented that the notices were too complex and too long and a few commented that they may have been purposely written in such a way so as to discourage people from reading them. According to McDonald et al [17] privacy notices are far too difficult to read and they maintain that policies need to be understandable by all users of online services.

VI. CONCLUSIONS AND RECOMMENDATIONS

In this study we explored users' perceptions of privacy in cloud computing and also their awareness of privacy risks. Our results show that users have a strong belief that cloud computing is intrinsically insecure. The vast majority of users believe that they could not trust cloud providers to keep their data secure.

If cloud computing is to have greater uptake in the UAE then both Government and service providers should take steps to address privacy concerns. A number of possible measures are briefly outlined here. These measures should be further studied.

1. Cloud service providers should write their privacy policies and terms of service in a manner that is easy to read and easy to understand.

2. The Government should run awareness campaigns about privacy and expectations of privacy in the cloud.

3. Users should be encouraged (as part of 2 above) to seek advice and education on privacy issues in the cloud.

4. The Government should look at improving its legislation on privacy in the UAE to encompass cloud computing.

5. Cloud computing providers should have better and clearer policies and practices, so that users could better understand the privacy risks they face. Users then, for example, may select cloud services for some categories of data and avoid it for others.

6. The Government should establish clear exclusive ownership rights over data. This includes personal data, usage data and other data collected by the service provider.

7. At an international level countries should harmonise their laws so as to reduce inconsistencies in relation to privacy. As the cloud does not have borders, security would be considerably enhanced and simplified if countries adopted similar policies and legislation.Selection (Heading 4): Highlight all author and affiliation lines.

Finally, in order to build user confidence in cloud computing there is a need for more research and development on privacy protection frameworks.

REFERENCES

[1] S. Pearson, Privacy, security and trust in cloud computing. 2013. DOI: 10.1007/978-1-4471-4189-1_1

[2] C. Rong, S.T. Nguyen, M.G. Jaatun, Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering Volume 39(1) pp 47–54, 2013. http://dx.doi.org/10.1016/j.compeleceng.2012.04.015

[3] State of cloud computing in the UAE. Frost & Sullivan, 2013. Retrieved from http://www.reportlinker.com/p01628615/State-of-Cloud-Computing-Security-in-the-UAE.html

[4] R. Gellman, Risks to privacy and confidentiality from cloud computing. World Privacy Forum. 2009. Retrieved from http://www.worldprivacyforum.org/2009/02/report-privacy-in-the-clouds

[5] K. Hashizume, D.G. Rosado, E. Fernández-Medina, E.B. Fernandez, An analysis of security issues for cloud computing. Journal of Internet Services and Applications February, 4:5 2013. DOI: 10.1186/1869-0238-4-5

[6] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, A survey on security issues and solutions at different layers of cloud computing. The Journal of Supercomputing Volume 63(2) pp. 561-592 2013. DOI: 10.1007/s11227-012-0831-5

[7] I. Walden, Accessing data in the cloud: The long arm of the law enforcement agent. ResearchGate 2013. DOI: 10.1007/978-1-4471-4189-1_2

[8] Z. Xiao, Y. Xiao, Security and privacy in cloud computing, . Communications Surveys & Tutorials, IEEE 15(2) pp. 843-859, 2013. DOI: 10.1109/SURV.2012.060912.00182

[9] United Arab Emirates Constitution 2011 Retrieved from file:///C:/Documents%20and%20Settings/user/My%20Documents/Downloads/UAE%20Constitution.pdf

[10] Penal Code UAE 1987 Retrieved from http://www.icrc.org/ihl-nat/6fa4d35e5e3025394125673e00508143/e656047207c93f99c12576b2003ab8c1/$FILE/Penal%20Code.pdf

[11] Electronic Commerce and Transactions Law 2006 Retrieved from file:///C:/Documents%20and%20Settings/user/My%20Documents/Downloads/legal_references-Electronic%20Transactions%20%20Commerce%20Law_Final%20for%20May%203%202007.pdf

[12] X. Cruz, The state of cloud computing around the world: United Arab Emirates, Cloud Times. 2013. Retrieved from http://cloudtimes.org/2013/04/01/the-state-of-cloud-computing-around-the-world-united-arab-emirates/

[13] Overcoming the apprehension of cloud computing: Results from the 2012 cloud computing security survey. Information Security Media Group. 2012 Retrieved from https://assets1.csc.com/cloud/downloads/Cloud_Survey_Report_2012_1.pdf

[14] R. Arora, A. Parashar, Secure user data in cloud computing using encryption. International Journal of Engineering Research and Applications (IJERA) Vol. 3(4) pp. 1922-1926. 2013. Retrieved from http://www.ijera.com

[15] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science Volume 10 (1), pp. 104-115, 1999.

[16] I. Ion, N. Sachdeva, P. Kumaraguru, S. Čapkun, Home is safer than the cloud!: privacy concerns for consumer cloud storage. Proceedings of the Seventh Symposium on Usable Privacy and Security Article No.13 2011. DOI:10.1145/2078827.2078845

[17] A.M. McDonald, R.W., Reeder, P.G. Kelley, L.F. Cranor, A comparative study of online privacy policies and formats. Computer Science Volume 5672, pp. 37-55, 2009. DOI: 10.1007/978-3-642-03168-7_3