

Factors Influencing Information Privacy Concern in Cloud Computing Environment

Ahmad Mohammad Zaher Asadullah
Information System Department,
International Islamic University Malaysia
Kuala Lumpur, Malaysia

Ishaq Oyebisi Oyefolahan
Information System Department,
International Islamic University Malaysia
Kuala Lumpur, Malaysia

Abstract— Cloud computing technology is one of the newest technologies widely used by consumers globally due to its advantages. One of the common advantages is that users can get access to applications and their own files and data on demand. However, there are privacy concerns and issues which discourage users from being active in cloud computing. This paper attempts to investigate the factors that influence information privacy concern in cloud computing environment by using a quantitative research approach. A total of 340 cases were gathered from a sampled population of students. Based on SPSS analysis, the study found that perceived privacy risk is influencing information privacy concern in cloud computing environment. Meanwhile, perceived privacy control and perceived effectiveness of privacy policy have no significant impact on information privacy concern in cloud computing environment.

Keywords—privacy concern, cloud computing, perceived effectiveness of privacy policy, privacy control, cloud, privacy risk in cloud.

I. INTRODUCTION

Cloud computing technology is a recent trend in the field of information and communication technology. It is defined by the US National Institute of Standards and Technology (NIST) as “a model for enabling ubiquitous, 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”. This definition seems to be the most accepted and satisfied definition of cloud computing as the Federal Bureau of Investigation (FBI) and Criminal Justice Information Services department (CJIS) has agreed and acknowledged this definition as shown in their 2012 CJIS Cloud Computing Report [1]. It can be said that cloud computing technology is a kind of storing and accessing of applications and computer data often through a Web browser rather than running installed software on personal computer or office server [2].

II. BACKGROUND OF STUDY

Cloud computing technology offers various types of services and applications for the public and organizations. One of the most commonly used cloud computing services is social networking websites such as Facebook, LinkedIn, Twitter, Instagram and many others, although these were not initially considered cloud computing services. Another example of

cloud computing services is E-mail services. Other major example of cloud computing services is Google Drive. All of Google's services could be considered as cloud computing such as Gmail, Google Calendar, Google Reader, Google Voice, Google glass and so on. In addition, Apple's cloud service is primarily used for online storage and synchronization of user mail, contacts, calendar, and more. All the data you need is available to you on your iOS, Mac OS, or Windows device. Prior studies found that information privacy concerns is an essential factors that discourage and influence users from transiting through online channel [3]. On the other hand, many issues have been raised in cloud computing environment, from the consumer's perspective. According to D. Chen & Zhao (2012) argued that information privacy and security concern in cloud computing are the main inhibitor for adopting and using cloud computing services [4]. Also, S, Daniel, & Vasanthi (2013) claimed that privacy concern is the major barriers in the growth and adoption of Cloud Computing by the IT industry and public consumers due to absence of any reliable and efficient privacy evaluation mechanism [5].

Therefore, it is required to conduct an empirical investigation upon the factors that influence users' information privacy concern in cloud computing environment. As a result, it would give a clear view to cloud computing service providers regarding the gap that they have in their cloud services, which should be assessed and overcome.

III. RESEARCH MODEL AND HYPOTHESES

Fig. 1 shows research model and hypotheses. It has been developed based on Communication Privacy Management theory (CPM). CPM theory established by Sandra Petronio who is communication professor at Indiana University, it provides researchers a comprehensive view on the processes of exchanging individuals' private information [6]. According to Hammonds (2009) Communication privacy management theory illustrates a very clear and inclusive guideline while examining how people measure and manage their private information.

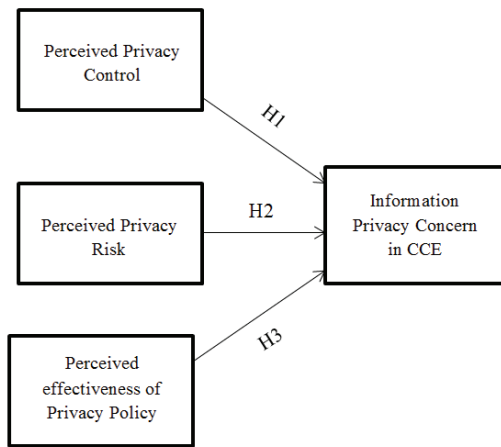


Fig. 1. Research Model

A. Information Privacy Concern in Cloud Computing Environment (CCE)

In this study information privacy concern is a dependent variable which has been addressed by allocating four variables. Hence, in this study it is assumed that these variables are influencing information privacy concern in cloud computing environment. However, according to Oxford Dictionaries privacy means “The state or condition of being free from being observed or disturbed by other people”. While, Mishra, Ranjita; Dash, Sanjit K (2011) indicated that privacy is the protection of transmitted data from passive attacks [7]. Another popular definition provided by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard is “*The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information*”. In other words, it is the matter which is related to the data collection, use, disclosure, storage, and destruction of personal data or personally identifiable information [4]. In addition, as cloud computing system usually offers services (e.g. DaaS, SaaS, IPaaS, PaaS, and so on) on the other hand of the Internet in terms of its users, the secret information of individual users’ and business’ are stored and managed by the service providers in cloud, and consequently results in privacy concerns. In fact, privacy issues exist since a long time in the computing literature [4]. Nevertheless, most of the information system literatures researchers have addressed and approach the concept of information privacy concern as general concern which reflect users’ natural worries and concerns upon the possibility of information privacy loss [8][9]; whereas, in this study the researcher is attempting to investigate and find out the factors that influences users’ information privacy concern in cloud computing environment.

B. Perceived Privacy Control

Cloud computing technology involves distributed computation on multiple large-scale data sets across a large

number of computer nodes. Every Internet user is able to share his or her personal data to the Cloud Computer systems which are located on the other side of the Internet. For instance, a user’s click stream across a set of webs (e.g., Amazon book store, Google search web pages, etc.) can be used to provide targeted advertising [10]. However, few studies tried to clarify the nature of control in the privacy context. For instance, in privacy literature, control has been utilized to refer to several objectives such as social power and procedural fairness of an organization’s privacy [8]. Studies have specified perceived privacy control based on three dimensions: 1) knowledge: users should be aware of a service provider’s information practices. It is assumed that without this knowledge, a consumer is unable to make a decision as to either disclose personal information or not. 2) Choice/access: users should be provided with choices as to how their personal information is utilized beyond the use for which the information was provided. 3) Use of privacy tools: when privacy tools like protocol for privacy preferences (P3P) or privacy seals are used by some service providers then the user begins to believe that his control over his personal information is growing [11] [12].

Therefore, hypotheses1: Perceived privacy control will negatively influence consumers’ information privacy concern in cloud computing environment [8].

C. Perceived Privacy Risk

Overall, risk has been defined as the uncertainty resulting from the potential for a negative outcome [13] and the possibility of another party’s opportunistic behaviour that can result in losses for oneself [14]. Therefore, usually negative perceptions are related to risk and it may influence an individual emotionally, materially, and physically [15]. Previous studies agreed that since online service providers requesting users’ personal information as a part of online transactions, the users express their concern about such information being misused, sold, disclosed, or exchanged with other parties without authorization from the owners [16]. It has been proved that such risk perceptions of online users constitute an obstacle to the widespread acceptance of online transactions mainly when sensitive information is required [17] [18]. There is thus a consensus among researchers that risk is vital factors in making any kind of online decisions [19]. According to S. Chen & Li (2010) unlike consumers in the physical market, consumers may be dealing with remote vendors that they have never met and products that cannot be touched and felt. Hence, consumers tend to be reluctant to conduct businesses based only on the information provided by e-commerce vendors because such information may not be reliable [20].

Therefore, this study is trying to measure users’ privacy risk and its impact on users’ information privacy concern. Thus, hypotheses2: Perceived Privacy Risk will positively influence consumers’ information privacy concern in cloud computing environment [8] [21] [11].

D. Perceived Effectiveness of Privacy Policy

Privacy policies are notices that are displayed on an online service provider, accessible to the public, and describe an organization's information practices. In fact, privacy policy not always true in practice. Privacy policies are made to reflect a service provider's actual privacy practices and serve as a contract between the service provider and the users. The privacy policies and strategies that online service providers adopt, implement and communicate to users can have an impact on users' information privacy concern [22] [23].

Prior studies found that perceived effectiveness of privacy policy is influencing users' information privacy concern. According to Milne and Culnan (2002) reported that privacy policy notices are an important means for reducing users' privacy concerns by providing users with information about the service providers' information practices [24]. Also, Shepard (2004) illustrated that roughly 60% of a sample of online service users said they decided not to use a website or not to purchase something from a web site because they were not sure about the collection and use of their personal information [25].

Therefore, hypotheses3: Perceived effectiveness of privacy policy will negatively influence consumers' information privacy concern in cloud computing environment [26].

IV. METHODOLOGY

A quantitative survey method has been adopted to collect data from targeted respondents. For that, we conducted a self-administered and online questionnaire to be answered by Undergraduate and Postgraduate students from the International Islamic University Malaysia. A total of 340 cases were usable. The survey items were adopted from prior studies where a five point-Likert scale was applied for each item.

V. DATA ANALYSIS AND RESULT

A. Reliability Test

Cronbach's alpha test was used to measure the reliability of the items. Overall, the result of the reliability test was successful; it was agreed upon the lower limit which is 0.7 across all constructs. Table I illustrates that.

TABLE I. RELIABILITY RESULT

Construct	Number of Items	Reliability value
Privacy concern	4	.841
Perceived Privacy Control	4	.845
Perceived Effectiveness of Privacy Policy	3	.842
Perceived Privacy Risk	4	.854

B. Demographic Information of respondents

The demographic profile of the respondents is shown in Table II. The largest number of cases was from female students (51.2.1%) and 35.6% of the total respondents were

aged in the group of below 20. Moreover, the majority of the respondents were undergraduate students (70.9%).

TABLE II. DEMOGRAPHIC INFORMATION

Characteristics	Item	Frequency	Percent
Gender	Male	166	48.8
	Female	174	51.2
	Total	340	100.0
Age	Below 20	121	35.6
	22 to 25	142	41.1
	26 to 30	44	12.9
	30 and above	33	9.7
	Total	340	100.0
Educational Level	Undergraduate	241	70.9
	Postgraduate	99	29.1
	Total	340	100.0

C. Measuring users' information privacy concern in cloud computing environment

The dependent variable in this study is information privacy concern in cloud computing environment. The researcher tried to measure users' information privacy concern, throughout the instrument for measuring information privacy concern the result of individual items are depicted, the first item which states that '*I am concerned that the data I submit to the cloud could be misused*' indicates that 32.4% of the respondents are agree with the statement, while 4.7% of the respondents are strongly disagree. Moreover, 10.9% of the respondents are disagreeing, 21.5% are strongly agreed and 30.9% remained neutral. The second statement says that '*I am concern about submitting my data in the cloud because of what others might do with it*' the result shows that 39.4% of the respondents agree while 3.8% strongly disagree. Disagree has 7.1% of the respondents, 24.7% neutral, 25% strongly agree. The third statement '*I am concerned that others can find data about me in the cloud computing services*' resulted that 37.6% of the respondents agree whereas 3.2% strongly did not agree with statement. While 31.5% of the respondents strongly agree, 19.7% remain neutral, 7.9% did not agree with the statement. The last statement says that '*I am concerned about providing my data to the cloud services, because it could be used in a way I did not foresee*' the result shows that 34.7% of the respondents agree whereas 2.9% strongly disagree. Meanwhile, 27.6% of the respondents strongly agree, 27.1% neutral, 7.6% did not agree.

Therefore, users' are concerned about the privacy of their information in CCE.

D. Cloud computing services usage rate

Based on the previous studies cloud computing services categorized into five categories: Social Networking (e.g., Facebook, Twitter and others), Email Services (e.g., Hotmail, Gmail, Yahoo and others), Google Services (e.g., Google Drive, Google Apps and others), Apple Services (e.g., iCloud, iTunes and others) and Data Storage Services (e.g., Box, Dropbox and others). However, it can be seen that Social Networking services has the highest percentage of respondents with 29.93%, whereas apple services has the lowest

percentage of respondents with 7%. Between the highest and the lowest percentage of respondents there are other categories Email services 26.70%, Google services 21.64% and Data storage services 14.73% respectively. Fig. 2 explains that.

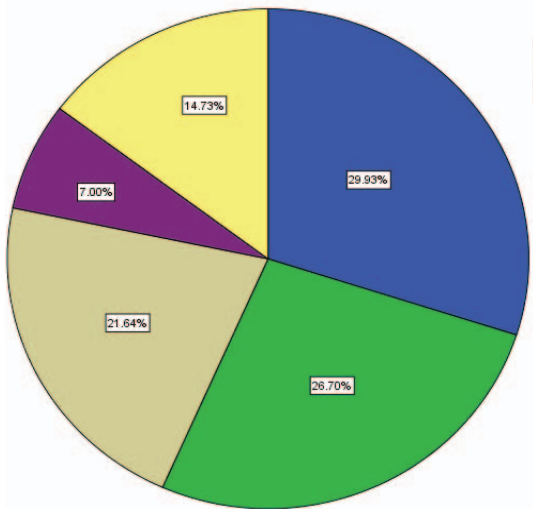


Fig. 2. Cloud computing services usage rate

E. Testing research hypotheses

Multiple linear regression technique was used to test research hypotheses. Information privacy concern was enrolled as a dependent variable. While perceived privacy risk, perceived privacy control and perceived effectiveness of privacy policy were entered as independent variable. The result of multiple regression provides two tables. The first table entitled ANOVA which illustrates the goodness of fit of the model, while the second table entitled Coefficients shows the significance of the independent variables (perceived privacy risk, perceived privacy control and perceived effectiveness of privacy policy) drivable to the dependent variable (Information Privacy concern). The result of ANOVA demonstrates that the model is significant at 99% because P value is less than 0.05, this result strongly validate and show the goodness of fit of the model. According to Gupta (1999) if Significance value is < .01, then the model is significant at 99%.

However, the Coefficients table provides information about the effect of independents factors on the dependent variable and the confidence with which we can support the estimate for each such estimate. Moreover, it can be seen that there is a significant relation between perceived privacy risk and information privacy concern ($p = .000, < 0.05$), which means that P value is true at 95% level of confidence. In another word, the result shows that consumers with high degree of privacy risk in Cloud Computing Environment (CCE) have high degree of information privacy concern in CCE as well.

Therefore, H2: “Perceived Privacy Risk will positively affect consumers’ information privacy concern in CCE” is supported. While, perceived privacy control and perceived effectiveness of privacy policy have no significant relation

with information privacy concern in CCE (perceived privacy control $P = .210$, perceived effectiveness privacy policy $P = .396, > 0.05$). This result indicates that perceived privacy control and perceived effectiveness of privacy policy does not influence individuals’ information privacy concern in CCE. In another word, perceived privacy control and perceived effectiveness of privacy policy have no significant relation with information privacy concern.

Therefore, H1: “Perceived privacy control will negatively affect consumers’ information privacy concern in CCE” is not supported.

Also, H3: “Perceived effectiveness of privacy policy will negatively affect consumers’ information privacy concern in CCE” is not supported.

To conclude, perceived privacy risk is influencing information privacy concern positively in CCE. Whereas, perceived privacy control and perceived effectiveness of privacy policy have no significant relationship with information privacy concern in CCE. Table III illustrates that.

TABLE III. RESULT OF MULTIPLE REGRESSION ANALYSIS

ANOVAa						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	108.876	3	36.292	84.431	.000b
	Residual	144.427	336	.430		
	Total	253.303	339			

a. Dependent Variable: Privacy Concern
b. Predictors: (Constant), Privacy_Control, Priavcy_Risk, Privacy_Policy

Coefficientsa						
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.457	.255		5.703	.000
	Priavcy_Risk	.648	.043	.652	15.206	.000
	Privacy_Policy	.039	.046	.039	.850	.396
	Privacy_Control	-.057	.046	-.057	-1.255	.210

a. Dependent Variable: Privacy Concern

VI. DISCUSSION

This study revealed that, Social Networking (e.g., Facebook, LinkedIn, MySpace, Twitter, Instagram, WhatsApp others) services has the highest percentage of usage rate among the participants. The outcome proves the prior studies [27] [25] where their investigations found that more than 98.6% of the consumers engaged and using social networking websites such as Facebook, Friendster, MySpace and Twitter.

On the other hand, this study found that perceived privacy risk is influencing information privacy concern in cloud computing environment statistically and significantly. Yet, In the same time the finding of Odeyinde (2013), Yuan, Shu, Yifeng, Tong, & Wei (2009) and Smith (2009) have found that there is positive relationship between privacy risk and privacy concern. In other words, when users have the feeling of privacy risk the concern of information privacy would be high [11][21][29]. Whereas, this study found that perceived privacy control has significant impact on information privacy concern

in CCE, but Xu et al. (2011) study showed that there is statistically and significantly negative relation between perceived privacy control and privacy concern [8]. The difference in the result might be because of the difference in the targeted population whereby this study has been conducted on the population of International Islamic University, while, Xu et al.'s (2011) study has been conducted on three large universities in the southeastern and northeastern of United States of America. Moreover, the previous reason goes to the result of hypotheses three where perceived effectiveness of privacy policy has no significant relationship with information privacy concern, while Wu et al.'s (2012) study showed that privacy policy has negative influence on privacy concern and it was partially supported [26].

VII. CONCLUSION AND RECOMMENDATION

In this study, the primary objective was to find out the factors that influence information privacy concern in cloud computing environment. Prior studies focused on the factors that influence privacy concern in e-commerce and online banking environment and so on, whereas, this study investigates it in cloud computing environment. Our findings proved that perceived privacy risk has statistically significant on information privacy concern in CCE. Meanwhile, perceived privacy control and perceived effectiveness of privacy policy has no significant on information privacy concern. Therefore, the researcher believes that the main objective of this study is accomplished and this finding is really vital to understand users' information privacy concern in CCE. Also, this study recommends that the quality of cloud service should be improved to overcome privacy's gap. Moreover, cloud service providers should have a clear privacy risk management plan, so that users' information privacy concern would be reduced.

REFERENCES

- [1] T. Report, "Recommendations for Implementation of Cloud Computing Solutions," 2012.
- [2] W. T. Lai, H. Trancong, and S. Goh, "A Fresh Graduate's Guide to Software Development Tools and Technologies: Cloud Computing," pp. 1–27, 2013.
- [3] A. Morton, "Measuring Inherent Privacy Concern and Desire for Privacy - A Pilot Survey Study of an Instrument to Measure Dispositional Privacy Concern," 2013 Int. Conf. Soc. Comput., pp. 468–477, Sep. 2013.
- [4] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 Int. Conf. Comput. Sci. Electron. Eng., no. 973, pp. 647–651, Mar. 2012.
- [5] M. S. E. Daniel, and N. Vasanthi, "Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions," pp. 1076–1081, 2013.
- [6] S. Petronio, "Communication Privacy Management Theory," 2002, pp. 168–180.
- [7] R. Mishra, D. P. Mishra, A. Tripathy, and S. K. Dash, "A privacy preserving repository for securing data across the cloud," 2011 3rd Int. Conf. Electron. Comput. Technol., pp. 6–10, Apr. 2011.
- [8] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," vol. 12, no. 12, pp. 798–824, 2011.
- [9] O. Nov and S. Wattal, "Social Computing Privacy Concerns: Antecedents & Effects," pp. 333–336, 2009.
- [10] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," 2010 Sixth Int. Conf. Semant. Knowl. Grids, pp. 105–112, Nov. 2010.
- [11] O. Odeyinde, "Information Privacy Concerns of Undergraduate Students in a Nigerian University and their Willingness to Provide Personal Information to Transact on the Internet by Olufemi Babajide Odeyinde A dissertation submitted to the faculty of Wilmington University," no. November, 2013.
- [12] A. Zorotheos and E. Kafeza, "Users' perceptions on privacy and their intention to transact online: a study on Greek internet users," Direct Mark. An Int. J., vol. 3, no. 2, pp. 139–153, Jun. 2009.
- [13] W. J. Havlena and W. S. DeSarbo, "On the Measurement of Perceived Consumer Risk," Decis. Sci., vol. 22, pp. 927–939, 1991.
- [14] S. Ganesan, "Determinants of long-term orientation in buyer-seller relationships," J. Mark., vol. 58, p. 1, 1994.
- [15] Y. Moon, "Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers," Journal of Consumer Research, vol. 26, pp. 323–339, 2000.
- [16] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," Inf. Syst. Res., vol. 17, pp. 61–80, 2006.
- [17] M. A. Eastlick, S. L. Lotz, and P. Warrington, "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment," J. Bus. Res., vol. 59, pp. 877–886, 2006.
- [18] C. Van Slyke, J. T. Shim, R. Johnson, and J. Jiang, "Concern for Information Privacy and Online Consumer Purchasing," J. Assoc. Inf. Syst., vol. 7, pp. 415–444, 2006.
- [19] C. Liao, C.-C. Liu, and K. Chen, "Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model," Electronic Commerce Research and Applications, vol. 10, pp. 702–715, 2011.
- [20] S. Chen and J. Li, "Examining Consumers' Willingness to Buy in Chinese Online Market," J. Comput., vol. 5, no. 5, pp. 815–824, May 2010.
- [21] W. Yuan, Y. Shu, X. Yi-feng, Z. Tong, and G. Wei, "The Impact of Perceived Emergency and Essentiality on Perceived Privacy Risk, Privacy Concern and Intention to Use in Mobile LBS Environment: An Example of China Mobile and Unicom," 2009 Eighth Int. Conf. Mob. Bus., pp. 267–272, 2009.
- [22] J. S. Mollick, "Privacy Policies, Fairness, Trustworthiness And Willingness To Transact With Firms Online," 2005.
- [23] K. L. Hui, H. H. Teo, and S. Y. T. Lee, "The value of privacy assurance: An exploratory field experiment," MIS Q. Manag. Inf. Syst., vol. 31, no. 1, pp. 19–33, 2007.
- [24] G. R. Milne and M. J. Culnan, "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys," Information Society, USA, 2002.
- [25] D. Shepard, "The practitioner's bottom line," J. Interact. Mark., vol. 18, pp. 3–5, 2004.
- [26] K.-W. Wu, S. Y. Huang, D. C. Yen, and I. Popova, "The effect of online privacy policy on consumer privacy concern and trust," Comput. Human Behav., vol. 28, no. 3, pp. 889–897, May 2012.
- [27] M. Alhamed, K. Amiri, M. Omari, and W. Le, "Comparing privacy control methods for smartphone platforms," 2013 1st Int. Work. Eng. Mobile-Enabled Syst., pp. 36–41, May 2013.
- [28] A. Dharmi, N. Agarwal, T. K. Chakraborty, B. P. Singh, and J. Minj, "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook," pp. 465–469, 2012.
- [29] H. Xu, T. Dinev, H. J. Smith, and P. Hart, "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," in International Conference on Information Systems (ICIS) ICIS 2008 Proceedings, 2008.