Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings

Proceedings

Better Safe than Sorry: A Conceptual Framework for the Use of the Cloud

Olajumoke Azogu
University of North Texas, Denton, TX, United States., Olajumoke.Azogu@unt.edu

Sherry Ryan
ITDS, University of North Texas, Denton, TX, United States., sherry.ryan@unt.edu

Better Safe than Sorry: A Conceptual Framework for the Use of the Cloud

Olajumoke Azogu
College of Information
University of North Texas
Olajumoke.Azogu@unt.edu

Sherry Ryan
College of Business
University of North Texas
Sherry.Ryan@unt.edu

Abstract

Cloud computing has come to stay and is expanding rapidly. The mode of deployment of services has implications for users who store data in the cloud and risk exposure to potentially severeconsequences. The safe use of cloud computing services is therefore necessitated. Drawing on the principle of self-preservation and the theory of protection motivation, this paper develops a conceptual framework for the safe use of cloud computing services by individuals.

KEYWORDS

Cloud computing, protection motivation theory, self-preservation

INTRODUCTION

Cloud computing (CC) is being hailed as the next big thing and receiving a great deal of interest in the information technology (IT) industry (Khajeh-Hosseini, Sommerville, and Sriram, 2010), infiltrating every corner of the Internet even though users may remain unaware of the utilization of services it offers (Jaeger, Lin, Grimes, and Simmons, 2009). Being touted as the fifth utility, after Water, Gas, Electricity and Telephony, it is steadily moving away from product offerings to services with emphasis on ubiquity rather than physical hardware (Buyya, Yeo, Venugopal, Broberg, and Brandic, 2009).

The National Institute of Standards and Technology (NIST) defines CC as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources….that can be rapidly provisioned and released with minimal effort or service-provider interaction" (Mell and Grance, 2011, p.2). Jaeger et al. (2009) see it as infrastructure, components and applications that provide varied computing power for the complex – scientific research, to the simple – email, to individuals, businesses and governments, with minimal burden to the user, and without the conventional need to buy, configure and maintain own computing infrastructure: in a manner, the centralization of information and computing resources.

CC services are typically deployed as; Software as a Service (SaaS): clients use provider applications running on provider infrastructure, Platform as a Service (PaaS): clients deploy and manage their own application on provider infrastructure (hardware and software), and Infrastructure as a Service (IaaS): clients use provider hardware infrastructure for their computing needs but maintains control over all software, storage and networks (Katzan, 2010a).

Miller (2009) finds that this has implications on how information is stored and applications run, with all (data and applications) being hosted in the cloud. The advantages of CC are numerous and have been touted by several (e.g. Jaeger et al., 2009; Buyya et al., 2009) to include the elimination of the need to deploy resource intensive IT infrastructure, the ability to pay for computing needs as required, and cost benefits from economies of scale (Armbrust et al., 2010) and the provision of superior processing power for very complex scientific problems and increased collaborations between major research institutions (Jaeger, Lin and Grimes, 2008). However, there is danger in using the cloud because there is a possibility of stored data not being secure (Miller, 2009).

Khajeh-Hosseini et al. (2010) find that beyond the advantages of the cloud lies potential insecurity of data, legal and privacy issues that bedevil cloud computing. Osterhaus (2010) posits that because users have no idea about how their data is stored, issues of trust, privacy, rights and confidentiality come to the forefront. This is especially true for users of SaaS who have absolutely no control over their use of CC services, and yet store their data in the cloud owned by another, in a place where they have no clue (Jaeger et al., 2009). Horrigan (2008) found individual users' concerns over their stored data to include misuse of information, persistent information they would have otherwise wanted deleted, and unapproved transmittal of their information to security agents, yet 69% of online users in the US have used cloud services in one way or another.Individuals have taken up CC because they find it easy and convenient, irrespective of provider truthfulness or potentially questionable practices (Horrigan, 2008). Nevertheless, the disadvantages of cloud computing will not go away. It therefore calls to reason that strategies for the safe use cloud services are needed. Jaeger et al. (2009) believes that the education of the general population of Internet users is important, and cloud service providers would do well to educate in clear terms, issues pertaining to, but not limited to client rights and provider responsibility.

This study therefore hopes to provide a conceptual framework for the individual user's safe use of CC services. There is a limited amount of literature in the field and yet, there is agrowing interest and utilization of CC services in practice. The aim is therefore to provide a conceptual framework to contribute to knowledge and provide a basis for expanded knowledge and practice. It might be pertinent to note here that the focus of this effort is not on intention to use CC services, but rather on the safe use under the assumption that the individual has gone beyond intention, and has already made the decision to use CC services.The proposed framework uses the principle of self-preservation and the theory of protection motivation.

Williams and Kim's (1975) work on the development of theorydefines theory as a conceptual framework of inter-related concepts. Consistent with their work, this paper develops a conceptual framework in a deductive systematized manner by producing predictions and logical deductions from extant literature in the applicable domain. This effort stops short of carrying out an empirical validation of the proposed framework – hoping that this framework will stimulate future research.

The rest of the paper is organized thus; starting with a discussion on the theoretical foundation of the study, the methodology used to identify framework development articles follows, after which the framework is presented. In conclusion, implications for knowledge and practice are discussed.

THEORETICAL FOUNDATION

The principle of self preservation posits that the need for survival drives individual decision making, and this need singularly determines how their collection of strategies is ranked (Karni and Schmeidler, 1986). Therefore, when confronted with a set of decisions to be taken in the face of a perceived threat, an individual will consider as most crucial the one option that is believed to be the optimal decision to protect self and ensure continued survival. Beaudry and Pinsonneault (2005) believe that when IT users perceive a threat they have limited control over, the decision strategy will focus on adapting to survive, maintain emotional stability and reduce tension by changing their perception of the occurrence. However, the question might be asked: what happens when there is the possibility of some measure of control over the perceived threat? It falls to reason that they might just be motivated enough to take action?

Maddux and Rogers' Protection Motivation Theory (PMT) (1983) in Norman, Boer and Seydel (2005) proposes the potentials of persuasive behavioral change communication whereby an individual's cognitive processes can be trained to perceive threats and recognize available preventive options and his/her own ability to take action to save his/herself. Originating from Rogers' original theory (1975) which focused on the appeal of fear, the revised theory by Maddux and Rogers focused on coping with health threats. PMT hypothesizes that self protection depends on two categories of four factors (Maddux and Rogers, 1983). The first category of threat appraisal which includes: Severity: perceived seriousness or gravity of threat; and Vulnerability: perceived likelihood of threat occurring. And a second category of coping appraisal: Response Efficacy: perceived effectiveness of recommended preventive action(s); and Self-efficacy: perceived confidence in self to perform recommended preventive action(s). These, resulted in motivation to protect self and subsequently protection behavior. Rogers (1983) in Boer and Seydel (1996) modified the theory to include advantages of risky behavior as a factor of threat appraisal, and the cost of protective behavior, as a factor of coping appraisal.

The theory has since been used in a variety of fields including online ITsystems researchto study online safety behaviors (LaRose, Rifon and Enbody, 2008; Youn, 2009). Herath and Rao (2009) adapted the theory to develop a framework for security policy compliance in organizations. Chenoweth, Minch and Gattiker (2009) used PMT to shift focus away from technologies, and to user behavior in the adoption of protective technologies to avoid harm from the use of IT. Our study takes the PMT and adopts it to model desirable behavior for the individual user's safe use of CC services.

METHODOLOGY

This study set out to develop a conceptual framework based on existing literature. To initiate the literature search process, a preliminary search for CC-related concepts was carried out by searching for the phrase cloud computing on the web using Google. The decision to do this was based on original perceptions of CC from professional literature (www.itwhitepapers.com; www.zdnet.com). Browsing through search results, a determination of key phrases: security, risk, privacy and security, regarding individual use of the cloud was made. Subsequently, selecting databases relating to IT: ABI Inform, ACM Digital Library, Business Source complete, IEEE Xplore and ISI Web of Knowledge, a search was carried out using the following keywords; cloud computing, cloud computing security, cloud computing trust, cloud computing privacy and cloud computing risk. The unit of analysis being the individual; articles found were filtered based on this criteria. Because of the small number of relevant articles obtained, the search was expanded to include the terms online computing, online security, online trust, online privacy and online risk with articles found also filtered out for relevance to CC and the unit of analysis. The exercise produced 22 articles that were subsequently reviewed and used in the development of the conceptual framework.

Table 1 shows a summary of concepts used in previous research, which made up part of the knowledge base of this effort as it relates to CC and online safety, and contributed to the development of the proposed framework.

Author(s)	Safety Construct
Ambrose and Chiravuri, 2010	Privacy
Durkee, 2010	Cost
Featherman et al., 2010	Risk, Security
Information Management Journal, 2011	Security
Ion et al., 2011	Cost
Jaeger et al., 2008	Privacy, Security
Jones and Leonard, 2008	Trust
Katzan, 2010b	Privacy, Security, Trust
Khajeh-Hosseini et al., 2010	Privacy, Security
Korzaan et al., 2009	Privacy, Risk, Trust, Self-efficacy
LaRose et al., 2008	Self-efficacy
Liu et al., 2004	Privacy, Trust
Mell & Grance, 2011	Cost
Miller et al., 2010	Trust
Morrow, 2011	Privacy, Risk, Security, Trust
Onwubiko, 2010	Privacy, Risk, Security, Trust
Pennanen et al., 2006	Privacy, Risk, Security, Trust
Roberts and Al-Hamdani, 2011	Security
Sangmi et al., 2009	Privacy
Tian et al., 2010	Trust
West, 2008	Risk, Security
Yao et al., 2007	Privacy, Risk, Trust, Self-efficacy

Table1. Selected Cloud Computing and Online Safety Research Papers

SAFE USE OF THE CLOUD CONCEPTUAL FRAMEWORK

We define safe conduct in CC as premeditated and precautionary actions taken by the user based on the awareness of probable threats that exist as a result of the use of cloud services. The user is defined as an individual who uses SaaS CC; using software and storing information in the cloud (Ambrose and Chiravuri, 2010).The awareness of threat is based on the user's appraisal of his/her use situation, while premeditated precautionary action is an outcome of the awareness of threat coupled with an awareness of functional capacities.

Adapting the principle of self-preservation (Karni and Schmeidler, 1986) and PMT (Maddux and Rogers, 1983, Rogers, 1983) to promoting behaviors that encourage the safe use of the cloud, we deduce that, the need to protect one's self, is primarily driven by the awareness of threat. In addition, an individual will respond to this need by developing protection strategies influenced by the awareness of the availability and accessibility of retinue of weapons – functional awareness. Rogers' PMT include construct for maladaptive behaviors; traits that inhibit from response to situations, thus putting the user at risk. We remove this construct from our framework and replace it with an adaptive behavior (need for privacy) which in contrast to maladaptive behaviors would drive a need to protect self, and along with other constructs drive a protection strategy for self-preservation.

The conceptual framework presented in Figure 1 is proposed.

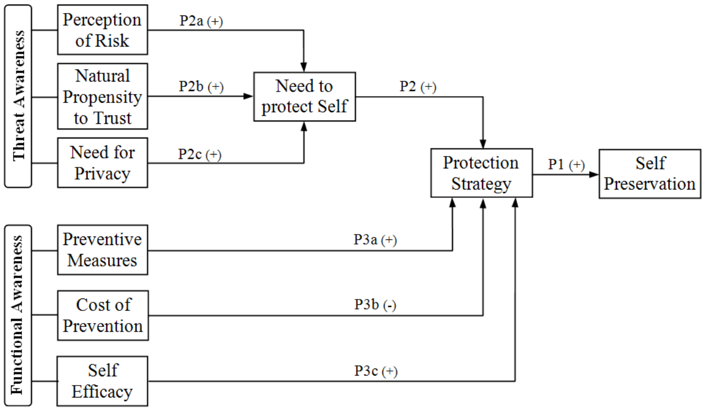

Figure1. The Safe Use of the Cloud Conceptual Framework

Protection Strategy

As evidenced in the dearth of extensive literature, CC safety behavior is a relatively uncharted area. Nevertheless, a synthesis of the selected literature reveals concepts consistent with Internet safety. However, this is not to say that the issues involved are one and the same with other online interactions such as e-commerce. Onwubiko (2010) believes that CC introduces a whole new set of challenges, while Jaeger et al. (2009) sees significant implications for individual users (and corporate institutions as well) in the rapid spread of services while still in relative infancy raising fundamental concerns about issues involving the centralization of resources, loss of control over personal data and a fundamental question on ownership of data. Khajeh-Hosseini et al. (2010) agrees with these opinions, adding that though many of the safety issues are not specific to CC, they are made even more significant because of the heavy reliance of CC services on web-based technologies – a significant source of vulnerability. Roberts and Al-Hamdani (2011) though deem the responsibility of securing the cloud to be that of the provider, they propose responsibilities for the cloud user.It therefore follows that the uptake of CC services should be well thought out, with a strategy for safe and beneficial use, given its enormous potentials and accompanying benefits. We therefore propose that;

Proposition1 (P1): *The development of a protection strategy is positively associated with self preservationin the CC environ.*

Need to Self Protect

The principle of self preservation reasons that an individual would instinctively want to protect self when threatened, and would therefore develop strategies to do so (Karni and Schmeidler, 1986). Alicke and Sedikides (2009) see self protection as ‘a form damage control” and can “be evoked by a failure of interests to advance sufficiently” (p.14). Therefore, if the cloud user perceives threats it falls to reason that to protect self, strategies would be required. Onwubiko (2010) perceives such threats and calls for new types of essential protection strategies. This is especially true for the cloud user in view of the Ponemon Institute study that revealed that CC providers are not overly concerned with the security of users' data, and consider it part of the user's responsibility (Information Management Journal, 2011). Considering that CC involves allowing third party control over personal information which has inherent security issues (Morrow, 2011), we propose that;

Proposition2 (P2): *The need to protect self positively influencesthe development of a protection strategy in the CC environ.*

Threat Awareness

Perception of Risk

The cloud user's perception of risk determines the severity attached to probability of a threat. Onwubiko (2010) believes that the abuse, misuse and exposure to theft of the user's data are real and present risks in CC. Khajeh-Hosseini et al. (2010) add that the lack of control over the computing infrastructure is a major source of the risk. However, the issue is not the existence of the threat, but the user's awareness of it. West (2008) supposes this is because of the difficulty in an individual's ability to evaluate risk and uncertainty, adding that a person's behavior is primarily motivated by his risk belief. He therefore proposes the need to increase an awareness of risk; noting that users are not necessarily stupid but rather unmotivated by a lack of apprehension, and thus do not appreciate the need for implementing security measures. From the ongoing, we propose that;

Proposition2a (P2a): *Anindividual's perception of risk generates awareness of probable threats and positively influences the need to protect self.*

Natural Propensity to Trust

Onwubiko (2010) thinks that trust while using CC must be earned; requesting users to be diligent in their dealings with service providers irrespective of service agreements. Miller et al. (2010) agree, adding that trust should not be consider a fixed binary entity, but rather shifts in a continuum, and therefore must be constantly verified. However, others (Liu et al., 2004; Pennanen et al., 2006; Jones and Leonard, 2008) see trust as personality trait and conditioned by life experiences and as such not so easy to control. Pennanen et al. (2006) do however concede that this natural propensity to trust (Jones and Leonard, 2008) is important when consumers find themselves in new circumstances. Given that blind trust could put users at risk (Onwubiko, 2010), it would be beneficial for CC users to tamper down their innate trust that sees the good in all. But first, it must be recognized for what it is. So, we propose that;

Proposition2b (P2b): *Perception of an individual's natural propensity to trust generates awareness of vulnerability to probable threats and positively influences the need to protect self.*

Need for Privacy

The need for privacy is also implicated in the perception of the severity of threat. A person who has nothing to lose is by no means under threat. However, the CC user who invariably stores data in the cloud has concerns about his privacy (Jaeger et al., 2008; Khajeh-Hosseini et al., 2010). Ambrose and Chiravuri (2010) consider that there is a possibility of privacy violation because of the location of client data. Featherman et al. (2010) note the risk of loss of privacy as an assessment of potential losses includes an assessment of the possibility of identity theft. Katzan (2010b) sees this as the crux of the debate on privacy. Because individuals need to be able to determine to whom, what, when and how personal information is communicated to others (p. 220), the cloud user, who may have a lower level of privacy assurance than a desktop user (Jaeger et al., 2008), would be concerned about personal sensitive information. Having made the decision to use CC services, the individual with a need for privacy would expectedly move to protect it. Therefore we propose that;

Proposition2c (P2c): *An individual's need for privacy generates awareness of probable threats and positively influences the need to protect self.*

Functional Awareness

Preventive Measures

Though each category of online safety concerns issue spawns significant challenges in itself, Pennanen et al. (2006) believe they are interconnected and should be handled in a similar manner. In agreement, LaRose et al. (2008) finds that the same online safety behavior such as the removal of spyware and cookies, can span multiple online safety concerns. They therefore propose the framing of online safety issues in terms relevant to the user, which for instance stress the multiple positive results of safe online behavior and of personal benefit to the user. They believe in the efficacy of user responsibility noting that if threat information is accompanied by personalized intervention strategies to deal with it, improved safety practices are more likely to happen trusting that "the average user can be induced to take a more active role in online safety" (p.76). Onwubiko (2010) requests that users should be made aware of the provider's guidelines and practices also believing in the efficacy of providing the user with needed information.Consequently we propose that;

Proposition3a (P3a): *The perceived availability and value of preventive measures positively influences the development of a protection strategy.*

Cost of Prevention

One of the key selling points of cloud computing is reduced cost as a result of economies of scale, and the advantage to individuals and small businesses that no longer have to devote scarce resources to setting up IT infrastructure (Buyya et. al, 2009). However, as Durkee (2010) points out, while initial cost might seem low, hidden cost will most likely crop up and may continue to rise. This agrees with (Mell and Grance, 2011) who find that addressing issues such as security after implementation is much more expensive. And while (Ion, Sachdeva, Kumaraguru and Capkun, 2011) found that about 79% of respondents were prepared to pay a token amount for CC services to ensure that their data was not sold to others, there is no proof that if price goes higher they will still pay. Even more uncertain was their finding that only about 50% were interested in buying insurance to protect against data loss. We therefore propose that;

Proposition3b (P3b): *The cost of preventive measuresnegatively influences the development of a protection strategy.*

Self Efficacy

LaRose et al. (2008) deem self-efficacy to be affected by availability of necessary information on online safety. They find that self-efficacy increased with increased involvement in online safety tasks. Self-efficacy concerns the user's awareness of his/her ability to carry out online safety measures. Yao et al. (2007) argue that frequent computer users have higher computer efficacy. It can therefore be conjectured that a CC user has a high level of Computer and Internet use efficacy based on his/her use of cloud services, and in agreement with LaRose et al. (2008), would continue to increase with greater involvement with and use of the services. It can therefore be assumed that online safety self-efficacy is a given for the cloud user and only needs to be encouraged. Therefore, we propose that;

Proposition3c (P3c): *The perception of an individual's self efficacy positively influences the development of a protection strategy.*

DISCUSSION AND CONCLUSION

The conceptual framework that we developed is believed to have implications for knowledge and practice. First, by modeling the framework, a comprehensible, logical analysis of cloud computing safety has been created. Because this effort stopped short at validating the framework, it is hoped that future research ideas would be inspired: both to validate the framework and to expand it to better represent the individual use of cloud services. No cognizancewas given to differences in individuals that have probable mediating effects on CC safety. Effects such as age or sex, have been found in some previous studies (e.g. Ambrose and Chiravuri, 2010) to mediate online safety. This is seen as a future area of interest.

The safe use of CC services cannot be disregarded. Though Jaeger et al. (2009) and Horrigan (2008) find significant security and privacy concerns for the single user of CC, the number of single users of CC services continues to grow. Service providers therefore should not ignore this class of users or their concerns and have a duty to protect them (Onwubiko, 2010). Providers also have to protect themselves, and should understand that unprotected users could turn out to be the weakest link that threatens their own systems (Dlodlo, 2011). The propositions in our framework contribute to the literature by helping us better understand the protection issues related to the CC user.

REFERENCES

1. Alicke, M. D. and Sedikides, C. (2009) Self-enhancement and self-protection: What they are and what they do. *European Review of Social Psychology*, 201 – 48. doi:10.1080/10463280802613866
2. Ambrose, P. and Chiravuri, A. (2010) An empirical investigation of Cloud Computing for personal use. In *Proceedings of the Fifth Midwest Association for Information Systems Conference, MWAIS 2010.* Paper 24. Retrieved from http://aisel.aisnet.org/mwais2010/24
3. Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010) A view of cloud computing. *Communications of the ACM, 53* (4), 50–58. doi:10.1145/1721654.1721672
4. Boer, H. and Seydel, E. R. (1996) Protection motivation theory. In*Connor M, Norman P, editors. Predicting health behavior*. Buckingham (UK): Open University Press. Retrieved from http://doc.utwente.nl/34896/1/K465____.PDF
5. Buyya, R., Yeo, C., Venugopal, S., Broberg, J. and Brandic, I. (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems, 25* (6), 599-616. doi:10.1016/j.future.2008.12.001.
6. Chenoweth, T., Minch, R. and Gattiker, T. (2009) Application of protection motivation theory to adoption of protective technologies. In *Proceedings of 42ndHawaii International Conference on System Sciences. HICSS '09*, 1–10. doi:10.1109/HICSS.2009.74
7. Cloud Providers Aren't Much Concerned with Security. (July/August, 2011) *Information Management Journal, 45*(4), 7. Retrieved from http://content.arma.org/IMM/Libraries/July-Aug_PDFs/IMM_0711_up_front.sflb.ashx
8. Durkee, D. (2010) Why Cloud Computing will never be free. *Queue,* 8(4), 20-29. doi:10.1145/1755884.1772130
9. Dlodlo, N. (2011). Legal, privacy, security, access and regulatory issues in cloud computing. In *Proceedings of the 2nd International Conference on Information Management and Evaluation*, 161-168. Retrieved from http://hdl.handle.net/10204/5011
10. Featherman, M.S., Miyazaki, A.D. and Sprott, D.E. (2010) Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. *Journal of Services Marketing,24*(3), 219 – 229. doi:10.1108/08876041011040622
11. Herath, T. and Rao, H. R. (2009) Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*, 106-125. doi:10.1057/ejis.2009.6

12. Horrigan, J.B. (2008) Use of cloud computing applications and services. *Pew Internet and American Life Project*. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf
13. Ion, I., Sachdeva, N., Kumaraguru, P. and Čapkun. S. (2011) Home is safer than the cloud!: Privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (SOUPS '11), Article 13, 1 – 20. doi:10.1145/2078827.2078845
14. Jaeger, P. T., Lin, J. and Grimes, J. M. (2008) Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology & Politics*, *5*(3), 269-283. doi:10.1080/19331680802425479
15. Jaeger, P., Lin, J., Grimes, J., and Simmons, S. (2009) Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. *First Monday, 14*(5). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171
16. Jones, K. and Leonard, L. N. K. (2008) Trust in consumer-to-consumer electronic commerce. *Information & Management, 45* (2), 88-95. doi:10.1016/j.im.2007.12.002
17. Katzan, H. (2010a) On an ontological view of cloud computing. *Journal of Service Science*, *3*, 1 - 6. Retrieved from http://journals.cluteonline.com/index.php/JSS/article/view/795/779
18. Katzan, H. (2010b) On the privacy of cloud computing. *International Journal of Management &Information Systems,14* (2), 1-12. Retrieved from http://journals.cluteonline.com/index.php/IJMIS/article/view/824
19. Khajeh-Hosseini, A., Sommerville, I. and Sriram, I. (2010) Research challenges for enterprise cloud computing. Retrieved from http://arxiv.org/ftp/arxiv/papers/1001/1001.3257.pdf
20. Korzaan, M., Brooks, N. and Greer, T. (2009) Demystifying personality and privacy: An empirical investigation into antecedents of concerns for information privacy. *Journal of Behavioral Studies in Business,1*, 1-17. Retrieved from http://www.aabri.com/manuscripts/09225.pdf
21. LaRose, R., Rifon, N.J. and Enbody, R. (2008) Promoting personal responsibility for internet safety.*Communications of the ACM, 51* (3), 71-76. doi:10.1145/1325555.1325569
22. Liu, C., Marchewka, J.T., Lu, J. and Yu, C-S. (2004) Beyond concern: A privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*, 127-142. doi:10.1016/j.im.2004.01.002
23. Maddux, J. E. and Rogers, R. W. (1983) Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19* (5), 469-479. doi:10.1016/0022-1031(83)90023-9
24. Mell, P. and Grance, T. (2011) The NIST Definition of Cloud Computing (Draft). *National Institute of Standards and Technology Special Publication 800-145*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
25. Miller, M. (2009) Cloud computing pros and cons for end users. Retrieved from http://www.informit.com/articles/article.aspx?p=1324280
26. Miller, K.W., Voas, J. and Laplante, P. (2010) In trust we trust. *Computer, 43* (10), 85-87. doi:10.1109/MC.2010.289
27. Morrow, S. (2011) Data Security in the Cloud. In *Cloud Computing: Principles and Paradigms (eds. R. Buyya, J. Broberg and A. Goscinski)*, John Wiley & Sons, Inc., Hoboken, NJ, USA. doi: 10.1002/9780470940105.ch23
28. Norman, P., Boer, H. and Seydel, E.R. (2005) Protection motivation theory. In: *Predicting Health Behaviour: Research and Practice with Social Cognition Models*. Open University Press, Maidenhead, 81-126. Retrieved from http://doc.utwente.nl/53445/1/K469____%5B1%5D.pdf
29. Onwubiko, C. (2010) Security issues to cloud computing. In *N. Antonopoulos and L. Gillam (eds.), Cloud Computing: Principles, Systems and Applications, Computer Communications and Networks*, Springer-Verlag, London. doi:10.1007/978-1-84996-241-4_16
30. Osterhaus, L. (2010). Cloud computing and health information. *B Sides*. Retrieved from http://ir.uiowa.edu/cgi/viewcontent.cgi?article=1014&context=bsides
31. Pennanen, K., Kaapu, T. and Paakki, M.K. (2006). Trust, risk, privacy, and security in ecommerce. *Proceedings of the International Conference on Electronic Business (ICEB) + Research Forum to Understand Business in Knowledge Society (eBRF) Conference,* Tampere, Finland.
32. Roberts, J. C. and Al-Hamdani, W. (2011) Who can you trust in the cloud?: A review of security issues within cloud computing. In *Proceedings of the 2011 Information Security Curriculum Development Conference* (InfoSecCD '11). ACM, New York, NY, USA, 15-19. doi:10.1145/2047456.2047458
33. Rogers, R. W. (1975) A protection motivation theory of fear appeals and attitude change1. The *Journal of Psychology: Interdisciplinary and Applied, 91*, 93-114. doi:10.1080/00223980.1975.9915803
34. Rogers, R.W. (1983) Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *J. Cacioppo & R. Petty (Eds.), Social Psychophysiology*. New York: Guilford Press.
35. Sangmi, C., Bagchi-Sen, S., Morrell, C., Rao, H.R. and Upadhyaya, S.J. (2009) Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication, 52* (2), 167-182. doi:10.1109/TPC.2009.2017985

36. Tian, L., Lin, C. and Ni, Y. (2010). Evaluation of user behavior trust in cloud computing. In *Proceedings of the International Conference on Computer Application and System Modeling (ICCASM 2010), 7*. doi:10.1109/ICCASM.2010.5620636
37. West, R. (2008). The psychology of security. *Communications of the ACM*, *51* (4), 34-40. doi:10.1145/1330311.1330320
38. Williams, J.G. & Kim, C. (1975). Opinion paper. On theory development in information science. *Journal of the American Society for Information Science, 26*, 1–9. doi:10.1002/asi.4630260102
39. Yao, M. Z., Rice, R. E.and Wallis, K. (2007) Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58* (5), 710-722. doi:10.1002/asi.20530
40. Youn, S. (2009) Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*, 389–418. doi:10.1111/j.1745-6606.2009.01146.x