Risk Perception and Cloud Computing Security

Gianfranco Elena
University of Glasgow, UK
(Department of Computing Science, PhD Program)
gianfrancoelena@gmail.com

Abstract.

Cloud computing technology offers great potential to improve civil military interoperability, information sharing and infrastructure resilience. Despite the surge in activity and the great benefits offered by cloud computing technology, security concerns about data availability, confidentiality, integrity and loss of governance have a great influence on risk management decision process. The massive concentrations of resources and data represent a more attractive target to attackers even if cloud-based defences can be more robust, scalable and cost-effective. The potential drawbacks are different than those for other IT systems since existing plans, policies, and practices were established prior to the large-scale introduction of cloud computing. The challenge that many organizations face is in understanding and weighing cloud computing's risks and advantages relative to existing legacy systems.

In this paper we investigate the role of risk perception related to IT innovation strategies. This study is motivated by a need to address a lack of understanding regarding risk perception of cloud computing technology. We aim to investigate which factors influence cloud computing risk perception in military and civilian organizations.

In our study we adopted the psychometric approach which has long been used to examine laypeople's perception of technological risks, activities and food hazards. In our case, psychometric approach was adapted to determine which cloud computing applications are likely to be acceptable to the military and civilian public and which cloud computing applications are likely not to be. We presented them a number of cloud computing applications and asked them to rate the risks involved on 5-point Likert scale.

We suggest that this information can improve our understanding about the role of risk perception in cloud computing risk analysis and provide valuable support to government organizations and corporates' cloud computing innovation strategies.

1. Introduction

Cloud Computing is perceived as one of the key technologies of the 21st century. This technology has a major potential to bring numerous benefits, however, it faces risks in terms of unintended economic and security impacts. Available research suggests that we do not fully understand cloud computing risks (Catteddu, 2011) and risk perception plays an important role in the risk assessment of cloud computing services. It seems likely that public risk perception of cloud computing will be crucial for the realization of technological advances (EU Commission, 2010). Therefore, risk perception and risk attitudes toward cloud computing should be taken into account at an early stage of technology development.

The psychometric approach has long been used to examine laypeople's perception of various hazards (Fischhoff et al., 1978). This research approach has been used to study a broad range of hazards, including technological risks, activities, and food hazards (Slovic, 1987). Participants assess, for example, how dreadful the hazards are, whether the risks are known to science, and whether people have control over their exposure to the hazard. The number of rating scales varies from study to study. The psychometric paradigm is designed to address the research question of why various hazards are perceived differently.

In the present research, the psychometric approach was adapted to determine which cloud computing applications are likely to be acceptable to the military and civilian public and which cloud computing applications are likely not to be acceptable. In most studies utilizing the psychometric paradigm, averages are taken across all participants, and the data matrix (hazards × rating scales) is submitted to a principal component analysis. As a result of this research approach individual differences are usually neglected (Siegrist et al., 2005).

In our study we investigated determinants of differences in risk perception. We looked at social trust when assessing the risks of a new technology (Siegrist & Cvetkovich, 2000). Research in technology domain showed that people who trusted institutions attributed more benefits and fewer risks to this technology (Siegrist, 2000; Tanaka, 2004).

In the present study, we examined the factors that contribute to risk perception of cloud computing applications in the military and civilians. The aim of this study is to investigate risk perception of different cloud computing applications creating "cognitive maps" of different risk perceptions. Cloud applications were described in short scenarios and participants assessed the risks and benefits associated with these applications. These assessments may identify the applications for which public debates will be most likely. Furthermore, results should indicate which factors have the greatest impact on the risk perception of a new and emerging technology.

2. Theory

Several studies have demonstrated that the psychometric model has a superior explanatory power (Sjöberg, 1996; 1997) but there is a discussion around the power with which the psychometric risk characteristics can actually explain risk perceptions and it neglects the impact of cultural factors on people's risk perceptions.

Numerous empirical investigations have been carried out on the cultural theory (Dake 1990; 1991; Wildavsky & Dake, 1990; Peters & Slovic, 1996) and the psychometric paradigm (Slovic, 1992; Gardner & Gould, 1989; Harding & Eiser 1984; Marris et al., 1997). In addition, a number of comparative analyses have been performed (Sjöberg 1996; 1997; Brenot et al., 1996; Marris et al., 1998). In general, these studies have sought to uncover and explain the proportion of variance in risk perceptions that each method can claim to account for, and then to test how accurate these claims are in order to dissect each method, revealing any limitations. Figures vary across the studies, but as Sjöberg (1997) reports, the consensus that has emerged across risk researchers, indicates that the psychometric approach can explain a greater proportion (about 20%) of the variance in perceived risks, than cultural theory (about 5%) does. Although considerable disagreement remains over absolute numbers (e.g. it is claimed that the psychometric paradigm can account for anything between 10% and 70% of the variance of risk perception), it is widely accepted that the qualitative risk characteristics of the psychometric paradigm explain a far greater, but nevertheless still modest, proportion of the variance in risk perceptions than either cultural biases, or socio-demographic variables, in cultural theory (Sjöberg 2000).

In this context, we decided that the best way to investigate risk perception of cloud computing technology is to use the psychometric methodology while trying to account for other important factors that might influence these risk ratings within the context of our participants work environments and professional backgrounds.

3. Method

3.1 Participants

The present study consists of an on line survey conducted in sixteen European countries. The questionnaire was developed according to well-known psychometric principles. A pilot test was performed to identify errors, avoid wrong design and predict possible problems. The survey was distributed to 285 potential participants. A total of 134 people took part in the research. Acceptance rate was 47%. 78,4 % (N=105) of the respondents were men and 21,6% (N=29) were women. The mean age was 37,97 (SD = 10,93; ranging from 18 to 65). Respondents indicated whether they had heard the term "cloud computing" before the survey. 92,6% of the respondents answered yes, and 7,4% answered no. 16 participants didn't complete the questionnaire and then 118 answers were analysed (Field, 2009).

3.2 Questionnaire

A brief explanation of cloud computing was provided, with the possible risk described as follows: "Cloud Computing Services are associated with new risks. Sensitive data are processed outside the enterprise and that brings to bypass the physical, logical and personnel controls that IT (Information Technology) departments exert over in-house programs. Customers are ultimately responsible for the security and integrity of their own data and they won't know exactly where their data are hosted and how the data environment is shared with other customers. Moreover, any vendor offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Finally, investigating inappropriate or illegal activity may be impossible in cloud computing and long-term viability be at risk since cloud provider could go broke or get acquired by a larger company." After this introduction, all 10 cloud computing applications and 3 non cloud computing applications were briefly described. Since benefits, but not risks, are specific for given applications, the benefits for each application were described. Information about generalized risks was summarized in the introductory section of the questionnaire. To obtain reference values, participants also evaluated three non cloud computing hazards (mobile phones, wireless devices and usb pens). Mobile phones are viewed as less risky than high-voltage transmission lines, but more risky than a TV transmitter (Siegrist et al., 2005). Therefore, mobile phones can be viewed as a medium risk. Wireless devices was chosen because WiFi is a widespread technology which implies the risk of losing personal information, and it might consequently serve as a lay model for evaluating cloud computing hazards. Finally, USB pen were selected because they are well known and their use is often correlated to malware infection and loss of data.

Participants were asked to rate the hazards on 10 5-point Likert scales. The dimensions utilized in earlier studies (Fischhoff et al., 1978) were adapted for the examination of cloud computing hazards. Some of the scales (e.g., old-new hazard) could not be used and were replaced by other scales (e.g., trust). The following rating scales were utilized:

1. What is the probability of IT security incident for your organization? (1 = very improbable; 5 = very probable)
2. Are you worried about risks for your organization? (1=not worried; 5=very much worried)
3. Do people take the risk voluntary and without any constraint? (1 = voluntary; 5 = involuntary)
4. Do people know the risk they are exposed? (1 = known precisely; 5 = not known)
5. How do you rate adverse security effects for your organization? (1 = not at all; 5 = very strong)
6. How do you assess control over risk? (1 = controllable; 5 = uncontrollable)
7. How much do you trust in governmental agencies responsible for protecting people IT security? (1 = no trust; 5 = much trust)
8. Using this technology is ethically justifiable to foster innovation and business efficiency? (1 = not justifiable; 5 = absolutely justifiable).
9. How beneficial do you consider this item to be for your organization as a whole? (1 = very low; 5 = very high).
10. How risky do you consider this item to be for your organization as a whole? (1 = very low; 5 = very high).

In addition to standard socio demographic variables, the questionnaire included items designed to measure general attitudes toward technology (e.g., "Technology is a danger for humans and their environment," "Technology makes life more comfortable"). Respondents were asked to express their agreement or disagreement with these items using a value between 1 ("don't agree at all") and 5 ("agree absolutely").

3.3 The Psychometric Risk Rating Scales

The questionnaire attempts to get a measure of the risk perceptions for broad categories of cloud applications, which were described in short scenarios to be realistic and specific to the cloud computing domain.

Specialised qualitative risk characteristic scales, and associated questions, were created. These were based on the psychometric instruments extensively used within the established paradigm (Fischhoff et al., 1978; Slovic et al., 1981). Particular attention was paid to the recent studies by Slovic et al. (1984(a); 1985) and Kraus & Slovic (1988), and, more specifically, a study conducted by Slovic, MacGregor and Kraus's (1987) that also took a scenario-based approach.

Eight characteristics were designed to measure three underlying dimensions of risk. The first is a general risk dimension capturing the severity, dread, and riskiness scales. The second is a general knowledge dimension capturing both knowledge characteristics. The third is a general control dimension capturing confidence, control, and trust characteristics. Factor analysis (or principle component analysis) was carried out to discover underlying dimensions or factors.

4 Results

4.1 Perceived Risks

Mean values for perceived risks and benefits for the military and civilians are given in Table I. "Documents in the Cloud" received the highest risk rating in the military sample while in the civilian sample, "Storage", “Documents in the Cloud” and “Identity Management” ranked as first. Overall, military assessed the risks associated with cloud computing applications as being much higher than civilian did.

Generally, overall the cloud applications taken into consideration, mean values for perceived benefits and trust received the highest risk rating in the military sample.

Table I. *Perceived Risk, Benefit, Trust (Mean and Std Dev.) of the Military and Civilian sample*

	Mean values for perceived Riks, Benefits, Trust											
Hazards	Military N=42		Civilian N=76		Military N=42		Civilian N=76		Military N=42		Civilian N=76	
	Benefit	SD	Benefit	SD	Risk	SD	Risk	SD	Trust	SD	Trust	SD
*Mobile Phones	3.548	0.916	3.520	0.950	3.238	0.906	2.724	0.918	3.048	1.011	2.408	0.926
Documents in the cloud	3.476	1.065	3.434	0.998	3.214	0.717	2.816	0.860	3.000	0.963	2.453	0.920
Software Apps in the cloud	3.405	1.211	3.293	0.997	3.048	1.058	2.605	0.801	3.000	1.012	2.461	0.824
Storage, Backup, Restore	3.238	1.144	3.197	1.071	3.195	1.054	2.895	0.932	2.929	0.997	2.539	0.774
Computing Power	3.098	1.091	2.987	1.125	3.024	1.000	2.303	1.020	3.049	0.835	2.587	0.824
*Wiress Devices	3.262	0.798	3.605	0.981	3.143	0.952	2.579	0.913	3.143	0.843	2.592	0.836
Identity and Access Mng	3.595	0.798	2.947	0.908	3.190	0.862	2.842	0.925	3.095	0.906	2.547	0.920
Monitoring and Auditing	3.476	0.773	3.145	0.934	2.881	0.861	2.342	0.740	3.071	0.867	2.632	0.907
Marketplace	3.000	1.148	2.789	0.899	2.857	0.952	2.329	0.823	3.095	0.878	2.697	0.864
Virtual Private Cloud	3.048	0.909	2.934	0.854	3.167	0.935	2.289	0.877	3.000	0.866	2.632	0.846
Email and Web Protection	3.714	0.708	3.303	0.980	3.190	0.773	2.474	0.791	3.143	0.899	2.487	0.872
Vulnerability Assessment	3.214	0.951	3.053	0.764	2.952	0.764	2.368	0.608	3.095	0.906	2.566	0.772
*USB pens and External HD	3.381	0.731	3.250	0.802	3.524	0.707	2.487	0.973	3.214	0.898	2.421	0.771

4.1.2 Analysis of the Aggregated Data of the Military Sample

The sample was reliable as Cronbach’s Alpha was 0.754. Kaiser-Meyer-Olkin Measure of Sampling Adequacy was 0.658 and Bartlett’s Test of Sphericity was 56,76 (p<0.001). A principal component analysis of the aggregated data for the military sample was conducted and a varimax rotation was performed. Inspection of the data indicated that outliers strongly influenced correlation coefficients. We decided, therefore, to compute rank correlations among the eight rating scales and to submit these rank correlations to a principal component analysis. Based on the scree-test plot we decided that three components, accounting for 86,72% of the variance, are necessary to explain the correlations among the eight rating scales. As Table II shows, the first of the two orthogonal components of the rotated factor loadings is highly correlated with perceived probability of security incidents, adverse security effects and worries about risks. This component is labelled “dread risk.” The second component is positively associated with knowledge of risk and trust while is negatively associated with voluntariness of risk. This component is labelled “Knowledge of the risk.” For further analyses, the factor scores of the 13 hazards were computed.

Table II. *Loadings from a Principal Components Analysis Over Eight Rating Scales Averaged Across Individuals (VARIMAX Rotated Solution) for the Military Sample*

Rotated Component Matrix[a]

	Component		
	1	2	3
Prob_Incident	**.946**	.173	.072
Adv_Effects	**.927**	.143	.011
Risk_Worries	**.905**	.141	-.253
Justifiable	**.668**	-.482	.380
Voluntariness	.098	**-.899**	-.035
Knowledge	.379	**.828**	-.243
Trust	.535	**.665**	.175
Control	-.026	-.011	**.968**

Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 4 iterations.

Multilinear regression analysis (SPSS) was used to examine how the factor scores related to the two principal components influence perceived risks. All predictors were simultaneously entered into the regression analysis. The proposed model was significant (F (3,9)=21,931, p=0.002) and explained 56% of the variance in perceived risks. The first factor, “dread risk,” was the most important predictor (β = 76, p < 0.001). The second factor “Knowledge” was marginally significant (β = 43, p < 0.01). The third factor was not significant (p>0.01).

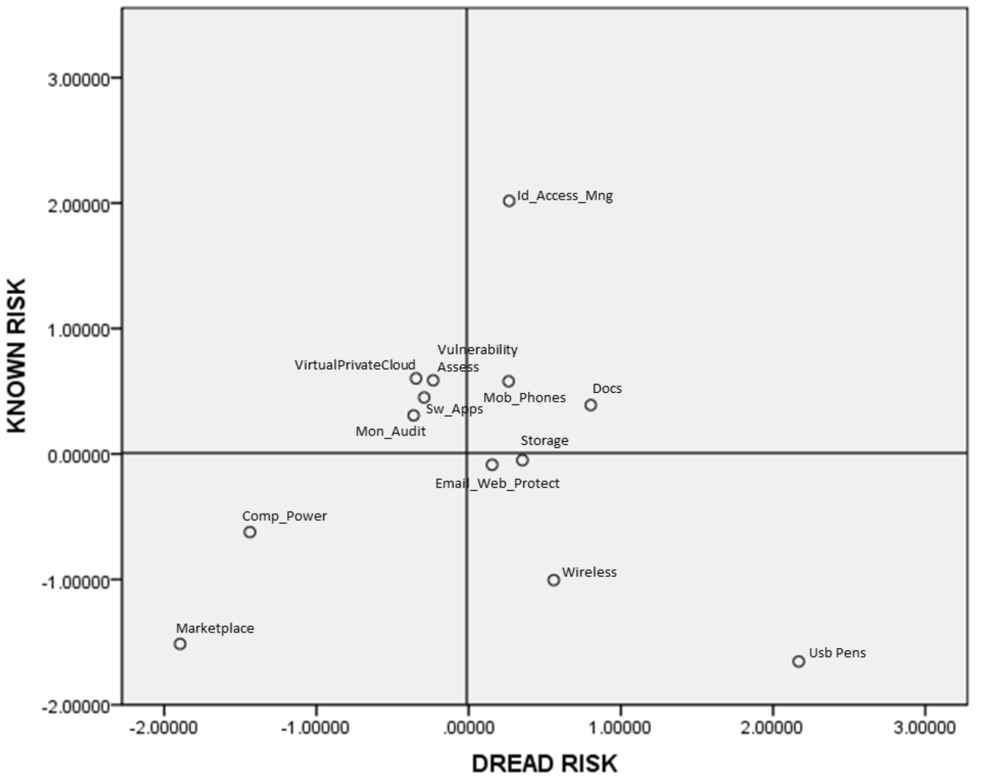

Fig. 1 *Location of the Cloud Computing hazards within the two component space for the military sample. It presents a two-dimensional plot of the cloud computing applications, using factor scores of "dread risk" and "Knowledge" as coordinates. Results indicate that the applications "Documents in the cloud", "Identity Access Management" and "Storage/Backup" have high loading on the factors Dread and Known Risk. These may be the applications most prone to be targets of public discussions about cloud computing technology.*

4.1.3 Analysis of the Aggregated Data of the Civilian Sample

The sample was reliable as Cronbach's Alpha was 0.616. Kaiser-Meyer-Olkin. Measure of Sampling Adequacy was 0.634 and Bartlett's Test of Sphericity was 57,98 p<0.001. Aggregated data for the civilian sample were submitted to a principal component analysis, and a varimax rotation was performed. Because outliers distorted the solution, rank correlations were analysed. Based on the scree-test plot we decided that three components, accounting for 80,96% of the variance, are required to explain the correlations among the eight rating scales. The factor loadings are shown in Table III. The rating scales probability of perceived probability of security incidents, adverse security effects and worries about risks had high loadings on the first component which was labelled as "dread risk." Knowledge, Justifiability and Control of the risk were positively correlated with the second factor. The second factor was labelled "Knowledge of the risk."

Table III. *Loadings from a Principal Components Analysis Over Eight Rating Scales Averaged Across Individuals (VARIMAX Rotated Solution) for the Civilian Sample*

Rotated Component Matrix[a]

	Component		
	1	2	3
Risk_Worries	**.944**	.070	-.027
Prob_Incident	**.937**	-.009	-.164
Adv_Effects	**.930**	-.107	-.012
Trust	**-.813**	-.515	.072
Justifiable	-.029	**.814**	.329
Control	.161	**.712**	-.408
Knowledge	-.004	**.690**	-.231
Voluntariness	-.091	-.116	**.921**

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 4 iterations.

A regression analysis (SPSS) was used to examine how the factor scores related to the three principal components influence perceived risks. All predictors were simultaneously entered into the regression analysis. The proposed model was significant (F (3,9)=11,58, p<0.01) and explained 40% of the variance in perceived risks. The first factor, "dread risk," was the most important predictor (β = 74, p < 0.01).

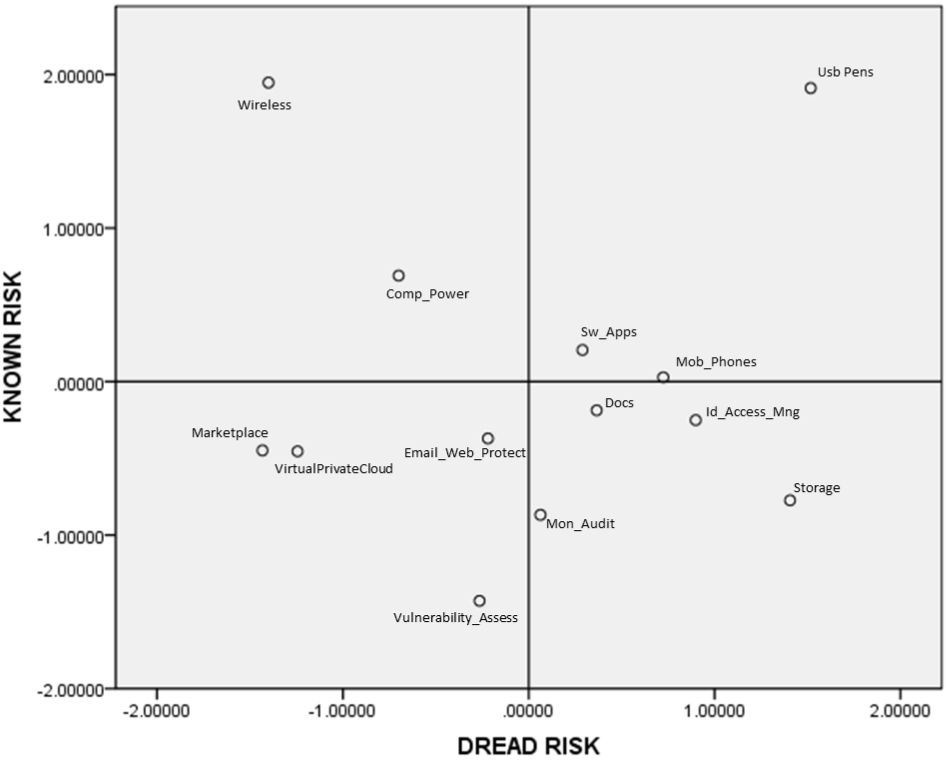

Fig. 2 *Location of the cloud applications hazards within the two-component space for the civilian sample.. It presents a two-dimensional plot of the cloud computing applications, using factor scores of "dread risk" and "Knowledge" as coordinates. Results indicate that the applications Identity Access Management, Documents in the cloud and Storage/Backup have high loading on the factors Dread and Known Risk. These may be the applications most prone to be targets of public discussions about cloud computing technology.*

4.1.4 Factors Influencing Individual Differences in Civilian's Risk Perception

Based on past research we hypothesized that trust and perceived benefits influence perceived risks. Civilian's assessments of trust, benefit and risks of the various cloud computing applications were highly correlated. All predictors were simultaneously entered into the regression analysis (SPSS). Results were partially in line with our hypotheses. Trust in government authorities and perceived benefits were not significant.

4.1.5 Factors Influencing Individual Differences in Military's Risk Perception

For the military sample all predictors were simultaneously entered into the regression analysis (SPSS). Results were partially in line with our hypotheses. Trust in government authorities (Beta=0.349; p<0.01), influenced risk perception of cloud computing applications.

4.1.6 Differences Between Military and Civilians

We examined whether the summated rating scales of perceived risks, benefits and trust are different for military and civilians. Military's risk assessments for cloud technology (M = 3.12; SD = 0.88; 95%-CI 2.85–3.52) were higher than civilian's risk assessments (M = 2.54; SD = 0.86; 95%-CI 2.29-2.89). Similarly, civilian people showed less trust in authorities (M=2.54; SD=0.85; 95%-CI 2.41-2.71) than military did (M = 3.07; SD = 0.91; 95%-CI 2.93-3.21). However, civilians perceived similar levels of benefits (M = 3.19; SD = 0.94; 95%-CI 2.79-3.61) as military (M = 3.34; SD = 0.94; 95%-CI 3.00-3.71).

5 Discussion

Cloud Computing could become a key technology of our century (European Commission, 2012). It has been suggested that more research related to security is needed to assure public support for cloud computing. How people perceive the benefits and risks associated with this new enabling technology must be taken into account in order to achieve effective risk assessment of cloud computing. The psychometric paradigm is commonly used to identify factors that explain risk perceptions of different hazards (Slovic, 1987). We adapted the psychometric method to examine public perception of cloud computing applications. Results show that military and civilians perceive various cloud computing applications differently. As in other psychometric studies, the response scales were highly correlated. Results of PCAs and regression analyses indicate that two factors, “Dread Risk” and “Known Risk”, explained most of the variance of perceived risks. The present research suggests, therefore, that it is problematic to examine general attitudes toward cloud computing applications.

How people react to cloud computing technology in the short or midterm depends on how industry and governmental agencies handle the issue. A social amplification process (Kasperson et al., 2003) could enhance the perceived risks of cloud computing hazards. Based on the results of the present study, cloud computing applications, for which such a social amplification process will most likely increase perceived risk, can be identified. Applications with high levels for dread risk and unknown risk are the most likely candidates. More specifically, applications in the Data/Storage/Backup in the cloud and Identity Access Management domains are most likely to become controversial topics among the cloud computing applications.

Even though we observed substantial mean differences for the various applications, the ratings were highly correlated. In other words, some people assess all cloud computing applications positively, whereas others assess cloud computing applications in a generally negative way. Therefore, we could further examine the question of why different persons perceive cloud technology differently. Military and civilians differ in their perception of risks associated with cloud computing hazards. The military perceive higher levels of risk have more trust in governmental agencies to protect people’s from cloud computing risks than the civilian does. Results of the present study are in line with previous research for other hazards (Kraus et al., 1992; Savadori et al., 1998, 2004). Results of the present research suggest that perceived benefit and trust in governmental agencies reduced perceived risks. Public concerns about cloud computing are reduced if people are familiar with the benefits of cloud computing and if measures are taken to enhance people’s trust in governmental agencies. The importance of trust for risk perception has been demonstrated in numerous studies (e.g., Siegrist, 2000).

How Government will regulate cloud technology adoption may, therefore, strongly influence laypeople’s and military’s risk perception.

Some limitations of the present research should be addressed. The present study provides a snapshot of how different groups of people perceive the risk of using some cloud computing applications in their work environment. However, risk attitudes toward cloud computing are not static. The actions of stakeholders and the manner in which the media report on cloud computing can influence risk perception of this enabling technology. Further social science research is needed, therefore, to better understand which factors might influence the risk perception and acceptance of cloud technology.

Generally, laypeople are still not familiar with cloud computing applications. Therefore, we had to describe the applications in some detail. Possible risks associated with cloud computing applications were addressed in the introductory section of the questionnaire because the risks associated with the various applications are very similar. Benefits associated with the applications, on the other hand, were mentioned in the short scenarios describing the cloud computing applications. It could be, therefore, that the people will assess the applications more negatively when benefits are less salient and possible risks of cloud computing applications are more salient. However, we would expect that this could influence the mean values, not the observed associations or patterns.

In the present research, we utilized the psychometric paradigm as a research framework. Some limitations of this approach have been described in some detail elsewhere (e.g., Siegrist et al., 2005). Future studies may wish to employ other research paradigms to examine public attitudes toward selected cloud computing incident scenarios.

REFERENCES

Brenot J., Bonnefous S. & Marris C. (1998). Testing the cultural theory in France. *Risk Analysis*; 18(6): 729-739.

Catteddu D., (2011), “Security and Resilience in Governmental Cloud”, European Network and Information Security Agency (ENISA), – available at http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

Dake K. , (1991). Orienting Dispositions in the Perception of Risk: An Analysis on Contemporary Worldviews and Cultural Biases, *Journal of Cross-Cultural Psychology*

Dake K. & Wildavsky A. (1991). Individual Differences in Risk Perception and Risk-Taking Preferences. *In: B.J. Garrick and W.C. Gekler (eds.) The Analysis, Communication and Perception of Risk*. Plenum Press: New York: 15-24.

Dake K. (1992). Myths of Nature: Culture and the Social Construction of Risk. *Journal of Sociological Issues*; 48: 21-37.

EU Commission, (2010). “Digital agenda for Europe”, available at http://ec.europa.eu/information_society/digital-agenda/publications/index_en.htm

ENISA, (2009). “Cloud Computing: Benefit, Risks and Recommendations for Information Security,” European Network and Information Security Agency (ENISA) report, accessed September 23, 2011, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment .

Field A. (2009). Discovering Statistics using SPSS for Windows. *Sage Publications*: London

Finucane M.L., Alhakami A., Slovic P. & Johnson S.M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioural Decision Making*; 13: 1-17.

Fischhoff B., Slovic P., Lichtenstein S. & Combs B et al. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*; 9: 127-152.

Gardner G.T. & Gould L.C. (1989). Public perceptions of the risks and benefits of technology. *Risk Analysis*; 9: 225-242.

Gould L.C., Gardner G.T., DeLuca D.R. & Tieman A.R. et al. (1988). Perceptions of technological risks and benefits. *Russell Sage Foundation*: New York,.

Kraus N. & Slovic P. (1988). Taxonomic analysis of perceived risk: Modelling individual and group perceptions within homogeneous hazard domains. *Risk Analysis*; 8(3): 435-455.

Marris, C., Langford, I., Saunderson, T., & O’Riordan, T. (1997). Exploring the “Psychometric Paradigm”: Comparisons between aggregate and individual analysis. *Risk Analysis*, 17, 303–312.

Marris C., Langford I.H. & O’Riordan T. (1998). A quantitative test of the cultural theory of risk perception: Comparison with psychometric paradigm. *Risk Analysis*; 18(5): 635-47.

Peters E. & Slovic P. (1996). The role of affect and worldviews as orienting dispositions in the perception and acceptance of nuclear power. *Journal of Applied Social Psychology* ; 26(16): 1427-1453.

Savadori, L., Rumiati, R., & Bonini, N. (1998). Expertise and regional differences in risk perception: The case of Italy. *Swiss Journal of Psychology*, 57, 101–113.

Sjöberg L. (1996). A Discussion of the Limitations of the Psychometric and Cultural Theory Approaches to Risk Perception. Radiation Protection Dosimetry; 68: 219-225.

Sjöberg L. (1997). Explaining risk perception: an empirical evaluation of cultural theory. *Risk Decision and Policy*; 2(2): 113-130.

Sjöberg L. (2000). Factors in Risk Perception. *Risk Analysis* ; 20(1): 1-11.

Slovic P., Fischhoff B. & Lichtenstein S. (1984a). Behavioural decision theory perspectives on risk and safety. *Acta Psychologica*; 56: 183-203.

Slovic P., Lictenstein S. & Fischhoff B. (1984b). Modelling the societal impact of fatal accidents. *Management Science*; 30: 464-474.

Slovic P., Fischhoff B. & Lichtenstein S. (1985). Characterising perceived risk. In: *R.W. Kates, C. Hohenemser & J.X. Kasperson (eds.).* Perilous progress: Managing the hazards of technology. Westview: Boulder, CO: 91-125.

Slovic P. (1987). Perception of risk. *Science*; 236: 280-285.

Slovic P., MacGregor D.G. & Kraus N.N. (1987). Perception of Risk from Automobile Safety Defects. *Accident Analysis & Prevention* ; 19: 359-73.

Slovic P. (1992). Perception of risk: Reflections on the psychometric paradigm. In: S. Krimsky & D. Golding (eds.). *Social theories of risk*. Praeger Press: New York: 117-152.

Slovic P. (2001). The Perception of Risk. *Earthscan Books: London*.

Siegrist M., (2000). The influence of Trust and Perceptions of Risks and Benefits on the Acceptance of Gene Technology", *Risk Analysis, Vol. 20,* No. 2

Siegrist, M., & Cvetkovich, G. (2000). Perception of hazards: The role of social trust and knowledge. *Risk Analysis*, *20*, 713–719.

Siegrist, M., Keller, C., & Kiers, H. A. L. (2005). A new look at the psychometric paradigm of perception of hazards. *Risk Analysis*, *25*, 211–222.