Andreea Cristina BENDOVSCHI, PhD Student
E-mail: Andreea_bendovschi@yahoo.com
Professor Bogdan Stefan IONESCU
E-mail: ionescub@gmail.com
Professor Iuliana Mariana IONESCU
E-mail: iuliana.ionescu@cig.ase.ro
The Bucharest Academy of Economic Studies

STATISTICAL INVESTIGATION INTO EXPLORING THE USE OF CLOUD COMPUTING TECHNOLOGY BY INCREASING THE USERS' TRUST

Abstract. *Trying to respond to the ever-changing needs of its users, cloud computing technology comes with a series of advantages that allow process optimisation and cost reduction; however the trust of cloud users is held back by challenges such as information security. This study aimed to determine how various aspects weigh in the users' trust in the cloud computing technology, with the final objective of identifying measures that can be taken to support the secure and trustful development of the cloud. Based on the statistical analysis of 571 questionnaires, the paper reflects on the aspects that weigh most in the users' trust in cloud computing technology, and assesses differences based on respondents' characteristics which are statistically tested using the Kruskal-Wallis test. The paper concludes with recommendations that would help the cloud community of users and suppliers address the needs and implications of the technology, in order for the cloud to reach its full potential.*

Keywords*: cloud computing, questionnaire, statistical analysis, Kruskal-Wallis test, trust, security.*

JEL Classification: O30

1. Introduction

As technology is continuously evolving, developing new concepts and reaching new peaks, companies are struggling to keep pace with the new trends in order to enable business transformation, cost cutting and process optimisation.

Cloud computing is far from being a new concept, and although more and more companies from all over the world choose to migrate their processes (Kumar, 2012) they still meet severe obstacles in the adoption decision.

Numerous definitions have been assigned to the cloud computing technology in the last decade (Foster et al., 2011; Buyya et al., 2008; Armbrust et

al., 2010; Low et al., 2011). NIST (2011) defines the cloud computing technology based on its main characteristics: concurrent, flexible, remote and on-demand access to a configurable network of shared technological resources (Mell and Grance, 2011). On the same note, Broberg, Venugopal & Buyya (2008) describe the cloud computing technology as an abstract collection of services accessible through the use of internet, and based on a parallel, distributed system of interconnected virtual machines (Broberg et al., 2008).

In order to respond to the users' needs and preferences, various models and types of cloud services have been deployed with time. Three main services were deployed at the beginnings of the cloud computing era (Kavis, 2014):

- **SaaS (Software as a Service)** represents a model in which the cloud provider manages and maintains web software and interfaces which are accessed by the user company and further managed internally, through its own network and infrastructure;
- **Paas (Platform as a Service)** is a model comprising of the platform (servers, operating systems, etc.) being managed by the service provider, while the user company manages the applications run through this platform;
- **Iaas (Infrastructure as a Service)** is a model in which the service provider manages the infrastructure (network, servers, etc.) while the user company manages and controls the operating systems and applications thus run.

However, with time other support models resulted, such as Risk Assessment as a Service or Security as a Service. These services have been deployed due to companies' demand to ensure the security of data managed through the cloud computing technology.

At the same time, several cloud models have been deployed; the public and community models use resources shared with other users, the private cloud provides exclusiveness to the available resources, while hybrid models combine characteristics of the aforementioned ones (Brar et al., 2014).

Although cloud computing technology brings along several opportunities of cost cutting, flexibility and process optimization (Damodaram and Ravindranath, 2010; Christauskas and Miseviciene, 2012; Miller, 2008; Weinman, 2012) companies adopting this technology also have to face a series of challenges, mainly focusing on security, ownership and responsibility sharing (Christauskas and Miseviciene, 2012; Diskiene et al., 2008; Galiniene and Marcinskas, 2007).

Authors believe that understanding how certain aspects weigh in the users' trust in the cloud computing technology can indicate measures that the cloud community should be focusing on in order to support the secure and trustful development of the cloud.

The study thus aims to explore ways in which the challenges of cloud computing can be addressed in order to increase the trust of existent and potential users.

2. Background and related work

Several studies addressed the main advantages and challenges that cloud computing technology brings along. CSA and ISACA surveyed 252 participants with extended cloud computing knowledge and experience, aiming to assess the greatest advantages and challenges (CSA and ISACA, 2012). The study shows that the cost reduction is the main driver influencing the adoption decision, followed by the agility of service, pay-as-you-go characteristic, time to market and increase of efficiency and productivity, while the greatest concern is the security issue, closely followed by data ownership, legal and contractual challenges, regulatory compliance, information assurance, supplier longevity and contract lock-in, performance standards and business continuity.

Cisco (2009) interviewed 244 CIOs and IT executives, concluding that 75% of them are mostly concerned by the security issue of the cloud computing technology (Cisco, 2009).A study performed by The Open Group (2011) also outlines the security issue as one of the main concerns potential user consider, but also identifies concerns related to governance, integration and process redesign (The Open Group, 2011).

The problem of security as a main concern of cloud computing users and potential adopters gave birth to a new type of cloud computing service model, Security as a service. As presented by P. Ram (2010), this model should be available on demand, and could help increase the users' trust in the way their data is managed and stored (Ram, 2010).

Ernst&Young's Global Information Security Survey (2012) showed that although companies are struggling with serious threats when handling sensitive data through cloud computing, 38% of the interviewees have not taken any mitigating measures to address the cloud computing related risks. However, the other 62% of the respondents chose to mitigate these risks through implementation of controls covering (Ernst&Young, 2012):stronger oversight on the contract management process for cloud service providers (28%), encryption techniques (28%), increased due diligence of service providers (25%), stronger identity and access management controls (22%), on-site inspection or assessment by your security/IT risk teams (16%), adjusted compliance monitoring processes (15%), increased auditing of cloud service provision (15%), adjusted incident management processes (15%), increased liability for cloud service providers in contracts (14%), contracting with a third party to test controls at a cloud service provider (13%), financial penalties in the case of security breaches (13%), more reliance on third-

party certification of cloud service providers (12%), financial penalties in the case of compliance and privacy issues (12%).

The idea that cloud computing technology relies on sharing of control and responsibilities over the data is most of the times the root of security and trust challenges faced by both customers and inter-connected service providers (Ernst&Young, 2012; Khaled and Qutaibah,2010).

3. Research methodology

The study was designed starting from the main challenges as identified by the aforementioned studies, and aimed to understand how aspects weigh in the perception of different categories of cloud computing existent and potential users.

3.1 Hypotheses

Although several studies have addressed the users' perception with regards to the cloud computing technology, none of the aforementioned studies attempted to understand discrepancies between respondents' characteristics, and instead only presented the generalised results. The authors believe, nevertheless, that significant differences can be found between the perceptions of users with different characteristics, which could be extremely useful in understanding the needs of each category. The study is therefore aiming to assess the existence and statistical significance of such discrepancies.

The following characteristics were included in the analysis: the respondents' gender, educational background, experience with the cloud computing technology, position in the company, business sector, company type and size of the IT Department.

3.2 Questionnaire design

Through reviewing the international literature summarised in the previous section, the authors identified recurring concerns which could be addressed by6types of measures, as follows:

- **Access rights**: confidentiality and integrity of information is ensured through appropriately restricting the logical access to data.
- **Security**: Security controls are in place for mitigating the risk of unauthorised access to the data managed/stored through the cloud computing technology.
- **Ownership and responsibility**: the more parties are involved in the process of managing/storing the data, the bigger the problem of ownership and responsibility in terms of information confidentiality, integrity and availability.
- **Liability**: as the use of internet knows no physical boundaries, and the use of cloud computing may involve the fact that data is physically stored in a different location (city, country, region, even continent) than the location it is used, the applicable norms, regulations and potential penalties need to be

addressed in order to better support the confidentiality, integrity and availability of information.

- **Continuity**: the continuity of service (through avoiding contract lock-in or vendor interoperability risks) as well as the business continuity (through appropriate incident management, backup and disaster recovery processes) is required for ensuring availability and integrity of information.
- **Performance**: IT governance, process redesign and performance standards should be considered to ensure an efficient adoption of cloud computing technology, thus enabling process optimisation and increase of the competitive advantage.

For each of the 6 categories, first-level hypotheses were further elaborated, as presented in Table 1.

Table 1. First level hypotheses

Category	**Users' trust would increase knowing that...**
Access rights	H1. Knowing that privileged access is appropriately restricted would increase the users' trust in the service.
	H2. Knowing that access to the data is periodically monitored would increase the users' trust in the service.
Security	H3. Encryption of data managed through the cloud computing technology would increase the users' trust in the service.
	H4. Periodic independent reviews would increase the users' trust in the service.
Ownership and responsibility	H5. Knowing they have a strong Service Level Agreement (SLA) with the service provider, clearly outlining the ownership and responsibility on data management and related controls would increase the users' trust in the service.
	H6. Transparency of service providers with regards to controls and availability for regular checks and audits would increase the users' trust in the service.
Liability	H7. Having strong, clearly set norms and regulations supporting data protection applicable to the service provider would increase the users' trust in the service.
	H8. Knowing that appropriate financial penalties may apply to the service provider in case norms and regulations are disobeyed would increase the users' trust in the service.
Continuity	H9. Knowing that service continuity is enforced (mitigating contract lock-in and vendor interoperability risks) would increase the users' trust in the service.
	H10. Knowing the service provider has appropriate business

Category	Users' trust would increase knowing that...
	continuity provisions (incident management, backup and disaster recovery) and effective controls would increase the users' trust in the service.
Performance	H11. Knowing an appropriate IT governance model is used for the services and data managed through the cloud would increase the users' trust in the service.
	H12. Knowing the service provider's performance and capacity standards are appropriate would increase the users' trust in the service.

3.3 Used methods and techniques

After analysing various research methods, authors selected a questionnaire-based study for data collection, under the main consideration that the analysed problem is a matter of human perception, thus the best approach would be the one involving as much direct contact/interaction as possible.

A questionnaire was elaborated, comprising of 14 questions focusing on measures that could address the challenges posed by the cloud computing technology and thus increase the companies' trust in this technology, and 8 demographic questions.

3.3.1 Population and sampling

As the study is focusing on the users of cloud computing working within the EU, the population was determined using statistical data provided by Eurostat. The labour force in the second quarter of 2015 among all EU countries is 245,534,300 (Eurostat, 2015). Applying a 95% confidence level and a margin of error within 5% of the total population, the sample size needed was determined using the following equation (Danktzker and Hunter, 2012):

$$n = \frac{(1.96)^2 * [p(1-p)]}{se} \quad (1)$$

Where: *n* is the sample size, *p* is the assumed population variance and s*e* is the standard error.

A sample size of 385 thus resulted as required for the results to be reliable. The sample was randomly distributed between all countries, business sectors, company sizes and respondents' gender. The questionnaire was elaborated using dedicated online software, and was distributed electronically, using email and social networks.

3.3.2 Timing, distribution and data collection

An electronic questionnaire was distributed among potential cloud computer users and cloud communities through the social media (email, LinkedIn).

The questionnaire comprised of 14 Likert scale questions ranging from 1 (not important) to 5 (very important), and 8 qualification questions regarding the individual (gender, cloud computing experience, educational background, position within the organisation) and the company (size, business sector, type of company and size of the IT Department).

3.4 Data analysis

Data cleansing was performed using MS Excel. During this step, data was analysed for consistency and completeness. All incomplete or invalid responses were eliminated from the research. A number of 517 valid responses were obtained during the survey period (19th November 2015 – 19th January 2016).

Once a consistent, complete dataset was obtained, the findings of the questionnaire were assessed for statistical significance using Minitab software with the Kruskal-Wallis test, illustrated through equation (2) (Anderson et al., 2010). This non-parametric test was chosen given the Likert scale type of responses of the questionnaire (ordinal data) which don't follow a normal distribution, the fact that almost all descriptive questions regarding the respondent background have at least 3 categories and that each category represents an independent random sample.

$$H = \left[\frac{12}{n(n+1)}\sum_{i=1}^{k}\frac{R_i^2}{n_i}\right] - 3(n+1) \quad (2)$$

Where k is the number of populations, n_i is the number of items in sample i, $\sum n_i$istotal number of items in all samples and R_i is the sum of the ranks for sample i.

With the Kruskal-Wallis test statistic, based on the sum of ranks for each of the samples, authors tested if the medians of two or more categories of respondents differ in each of the first-level hypothesis formulated at 0.05 level of significance, thus resulting in the following second-level hypotheses:

H0: the groups' medians are all equal in each of the first-level hypothesis

H1: at least one median is different in each of the first-level hypothesis

Figure 1 depicts the output for one of the tested first-level hypotheses with a descriptive question.

Kruskal-Wallis Test: H1. Authorized access vs. Educational Background

Kruskal-Wallis Test on Authorized access vs. Educational Background

Educational Background Experience	N	Median	Ave Rank	Z
No	209	4.000	208.9	-6.28
Somewhat	253	5.000	308.5	7.38
Yes	55	4.000	221.6	-1.96
Overall	517		259.0	

H = 54.71 DF = 2 P = 0.000
H = 63.91 DF = 2 P = 0.000 (adjusted for ties)

Figure 1. Kruskal-Wallis Test output for H1 vs. Educational background

The output shows the number of responses (N) for each category within the Response variable (Educational Background), their medians, the average ranking representing the average of the ranks for all observations within each sample used in computing the above H test statistic and the Z value indicating how the average rank for each group compares to the average rank of all observations.

In this example, the H statistic values have their p-value lower than 0.05, leading the authors to reject the null hypothesis and conclude that the medians are not all equal. Thus, the respondents'perception towards authorized access differs significantly depending on their educational background.

4. Results and discussion

4.1 The high-level view

The analysis was performed using the weighted average score assigned by respondents to each of the questions. The study revealed that knowing financial penalties may apply to the service in case norms and regulations are disobeyed ranked highest among all hypotheses, with a weighted score of 4.52, followed by a strong Service Level Agreement clearly outlining the split of responsibility (4.46), authorised access and interoperability (4.43), and encryption of data (4.42).

At the other end, knowing access is closely monitored (4.09), business continuity provisions (4.04) and IT governance (4.03) ranked lowest among all hypotheses. Detailed results are presented in Table 2.

Table 2. Reponses distribution by percentage

Hypothesis	Rank 1 (%)	Rank 2 (%)	Rank 3 (%)	Rank 4 (%)	Rank 5 (%)	Score*
H1: Authorised access	0	2	17	17	64	**4.43**
H2: Access monitoring	6	2	9	43	40	**4.09**
H3: Encryption	0	0	13	32	55	**4.42**
H4: Independent reviews	11	2	6	23	58	**4.15**
H5: Split of responsibility	0	2	7	34	57	**4.46**
H6: Transparency	2	11	9	23	55	**4.18**
H7: Data protection laws and regulation	2	3	17	23	55	**4.26**
H8: Financial penalties	0	2	4	34	60	**4.52**
H9: Interoperability	0	1	14	26	59	**4.43**
H10-1: Incident management	0	21	17	19	43	**3.84**
H10-2: Backup	0	13	19	13	55	**4.10**
H10-3: Disaster recovery	0	12	17	11	60	**4.19**
H11: IT governance	0	11	13	38	38	**4.03**
H12: Performance and capacity standards	0	2	23	30	45	**4.18**

**Score was determined using the Weighted Average model.*

The study revealed the fact that commercial and regulatory aspects (financial penalties applicable to the service provider, the split of responsibilities in the SLA, the interoperability between service providers) are more important for the potential users of the cloud computing technology than the technical aspects (access monitoring, business continuity, IT governance).

4.2 Assessing discrepancies and individual results

All questions were assessed against each category individually, and the statistical significance was assessed using p value. Results showed that although most of the categories present statistically significant discrepancies, such as the business sector, educational background and experience with the cloud computing technology of the respondents, characteristics such as gender or company size are not significant for some of the questions. Table 3 depicts the p value for each tested hypothesis per category.

Table 3. P value for each category

First-level hypothesis	P value per category						
	Gender	Cloud experience	Position in the company	Business sector	IT Dept. size	Company size	Education
H1	**0.003**	*0.086*	**0.000**	**0.000**	**0.000**	**0.000**	**0.003**
H2	*0.524*	**0.000**	**0.000**	**0.000**	**0.001**	**0.000**	*0.302*
H3	**0.000**	**0.000**	**0.000**	**0.000**	**0.025**	**0.000**	**0.000**
H4	*0.339*	**0.030**	**0.000**	**0.000**	**0.000**	*0.093*	**0.000**
H5	**0.006**	*0.082*	**0.000**	**0.000**	**0.000**	*0.057*	**0.004**
H6	*0.633*	**0.000**	**0.000**	**0.000**	**0.000**	*0.581*	*0.142*
H7	*0.120*	**0.000**	**0.000**	**0.000**	**0.000**	**0.008**	**0.001**
H8	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	*0.563*	**0.000**
H9	*0.577*	**0.000**	**0.000**	**0.000**	*0.929*	**0.048**	**0.019**
H10-1	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	*0.157*	**0.000**
H10-2	**0.014**	**0.000**	**0.000**	**0.000**	**0.000**	*0.356*	**0.000**
H10-3	*0.073*	**0.000**	**0.000**	**0.000**	**0.000**	*0.632*	**0.000**
H11	**0.010**	**0.000**	**0.001**	**0.000**	**0.000**	**0.001**	**0.000**
H12	**0.002**	**0.000**	**0.000**	**0.000**	**0.000**	*0.076*	*0.070*

The analysis continued with assessing the discrepancies between the categories which passed the statistical test, in order to understand the differences in the respondents' perceptions around cloud computing technology.

Results show that although no significant discrepancies can be found in terms of disaster recovery provisions, access monitoring, independent reviews, transparency, legislation and interoperability, discrepancies vary significantly between genders for matters such as authorised access, IT governance and

performance capacity management, encryption, SLA and penalties. The test also revealed that male respondents assigned a higher score to all these questions, thus outlining that male users of cloud computing would assess more attentively the cloud supplier's provisions before selecting a service.

Two main aspects were identified based on the cloud experience differences. Firstly, results outlined a direct link between the assigned score and the respondents' experience with the cloud computing technology, as the more experienced users are with cloud computing technology, the higher the scores they assigned.

Secondly, it was noted that while the inexperienced respondents view interoperability more important than the experienced users, highly experienced users place the most importance on the business continuity provisions (backup, incident management and disaster recovery), while the somewhat experienced users place more importance on access monitoring, transparency and encryption.

These results can be translated through a different perspective of the main needs and expectations users have from the cloud provider. For example, new users with little or no experience with the cloud computing technology, how it works and what could go wrong may imagine that their data stays in the cloud forever once they upload it there, without picturing a possibility for the data to be lost or corrupted beyond recovery. On the other hand, experienced users may believe that they could manage aspects such as access monitoring and interoperability as long as the cloud provider ensures data availability at all times.

In terms of the respondents' position in the company, all questions revealed statistically significant differences. Firstly, a general discrepancy was noted between employees and managers' ratings, with the latter assigning higher scores to most of the questions. This can be translated through the fact that greater responsibility brings greater concerns with regards to the information confidentiality, integrity and availability.

Results also show that managers and business owners are more concerned in technical aspects such as business continuity and encryption than employees, while legal and contractual aspects ranked more for employees than for the other categories.

All questions revealed statistically significant differences in terms of the business sector. Results show that while respondents working in financial services, management of companies and enterprises, retail and public sector scored higher than the others, while construction and exploitation industries scored the least.

This can be explained by the nature of data managed by the respondents on a daily basis. For example, people working in financial services and retail often manage confidential and personal data such as bank details or transactions information while the public sector manages citizens' personal data (address, phone numbers, etc.). On the other hand, such data type is rarely managed by

industries such as constructions or exploitation, where processes are not highly depending on the use of online transactions, internet-based software and personal data of third parties.

Perspectives regarding the size of the company and the size of the IT Department did not pass the significant test for most of the assessed questions. However, statistically significant discrepancies could be found in terms of authorised access, IT governance, access monitoring, encryption, legislation and interoperability.

Results revealed a general trend for respondents working in multinational companies to assign average scores to all these aspects, placing as a category between the SMEs' employees, which assigned the lowest scores, and the local companies with global presence, which ranked all these aspects the highest.

The only exception is the interoperability, which is more important to the multinational companies than for the other 2 categories. This can be explained by the challenge of finding operating models and IT resources that would fit different systems, architectures and databases as used by different locations.

Among all categories, the respondents' educational background outlined the greatest discrepancies, revealing an interesting link between the knowledge and the level of concern with regards to the cloud computing technology. As can be seen in Figure 2, respondents with a technical background (engineering, computer science) assigned all aspects a higher importance, followed by the finance/economics graduates, and lastly by respondents with other backgrounds (literature, foreign languages, etc.).

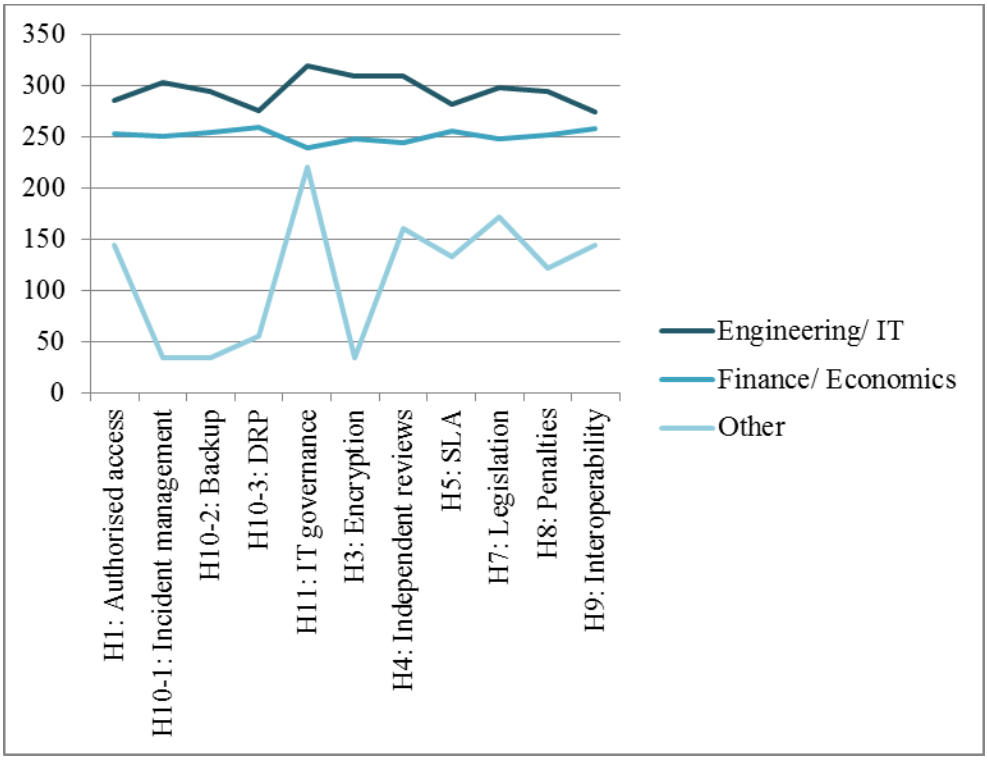

Figure 2. Average ranks per educational background categories

The result can be translated in the fact that the more connected to the technology and information security aspects respondents are, the more concerned they will prove to be when it comes to choosing a new technological way to manage the data.

On the same note, results show that while aspects such as business continuity, IT governance, encryption and independent certifications are assigned priority by the respondents with technical background, legal and contractual aspects are more important for respondents with a less technical background.

5. Conclusion and future research

Based on the high-level results of the research, these show that all 12 identified measures are essential in building trust into the broad use of the cloud computing technology, as the total weighted average score was no less than 4.03 for all questions. By limiting the analysis to a general level, results reveal the fact that commercial and regulatory aspects are more important to most of the respondents than the rather technical aspects, which could lead to 2 main implications. On one hand, the commercial and regulatory support is essential for users' trust in cloud computing to increase. Therefore, one of the main drivers to the development and

use of cloud computing technology could come from the national and EU authorities and independent organisations, through the elaboration of strong regulations, standards and best practices regarding the provision that would support the cloud users.

On the other hand, this could signal a general lack of awareness with regards to information security controls that go beyond the commercial and regulatory aspects. For example, the without appropriate business continuity provisions (data backup, disaster recovery and incident management) users' data could be lost and non-recoverable in case of a major incident or disaster. Also, an effective IT governance model could reflect a well-organised environment with adequate performance measurement, resource allocation and controls in place to ensure that IT delivers value. Access monitoring is also one of the least important measures for increasing users' trust in the cloud computing technology, however most of the times a cyber-attack, error or fraud takes place, this action is the most reliable in judicial or administrative proceedings (from internal investigations to the court of law). This is also supported by the fact that respondents with no experience in cloud computing technology or with no technical/IT background tended to rank all questions lower than the users with cloud experience or with a technical educational background.

However, through an in-depth analysis using Kruskal-Wallis test, results showed that this questionnaire can provide useful insights, allowing a better assessment of the users' perceptions and showing that generalisation may not always be the best approach to understand the needs of different user categories.

As the results showed the perception upon cloud computing technology varies with the respondents' experience and knowledge, different measures should be taken to address the concerns of each category.

For users with little or no experience with the cloud computing technology, and without a technical background, cloud computing may sound as an appealing option when the legal and contractual aspects offer protection and coverage. On the other hand, technical requirements will increase with the technical knowledge and experience of users, so that a fairly decent SLA will not be enough for people used to handling sensitive data on a daily basis, having a good technical knowledge or experience with the cloud computing technology. For these potential users, security controls implemented by the cloud provider would be essential in increasing the trust in the technology.

Nevertheless, everything comes with a cost, and additional security controls may reflect in the increase of service prices, whose justification may not be understood or agreed upon by some users or suppliers. On that note, authors believe that information security should not be optional, and as soon as there will be a universal demand for security, the cloud computing world will forever change.

Future research will be focusing on increasing the awareness of potential cloud computing users with regards to the threats their data may be exposed to, in order to better understand the implications of the cloud computing technology,

assess the data and security requirements, and design proper controls to ensure the confidentiality, integrity and availability of data.

REFERENCES

[1] **Kumar, A. (2012),*World of Cloud Computing & Security***; *International Journal of Cloud Computing and Services Science (IJCLOSER)*,volume1, pp. 253-58;
[2] **Foster, I., Zhao, Y., Raicu, I., Lu, S. (2009)**, ***Cloud Computing and Grid Computing 360-degree Compared****; Grid Computing EnvironmentsWorkshop*, volume 08, pp. 1-10;
[3] **Buyya, R., Yeo,C. S., Venugopal, S. (2008)**, ***Market-oriented Cloud Computing: Vision, Hype, and Reality for Delivering it Services as Computing Utilities****; CoRR*;
[4] **Armbrust, M., Fox, A., Griffith, R., Joseph, A., Konwisnki, A., Lee, G., Zaharia, M. (2010)**,***A View of Cloud Computing****; Communication of the ACM*, volume 23(4), pp. 50-58;
[5] **Low, C., Chen, Y., Wu, M. (2011),** ***Understanding the Determinants of Cloud Computing Adoption;*** *Industrial Management & Data Systems*, volume 111 (7), pp. 1006–1023;
[6] **Mell, P., Grance, T. (2011),*The NIST Definition of Cloud Computing - Special Publication 800-145. U.S. Department of Commerce****; Gaithersburg: Computer Security Division, Information Technology Laboratory, NIST*; Retrieved 15.02.2014, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf;
[7] **Broberg, J., Venugopal, S., Buyya, R. (2008),*Market-oriented Grids and Utility Computing: The start-of-the-art and Future Directions****; Journal of Grid Computing*, volume 6(3), pp. 255-276;
[8] **Kavis, M. (2014),** ***Architecting the Cloud: Design Decisions for Cloud Computing Service Models (Saas, Paas and Iaas)****; Wiley CIO;*
[9] **Brar, Y., Krishan, S., Mehta, A., Talwar, V., Choudhury, T., Vashisht, V. (2014),*An Advanced Security - A Two-Way Password Technique for Cloud Services****; International Journal of Computer Science and Mobile Computing*, volume 3(4), pp. 4-15;
[10] **Damodaram, A., Ravindranath, K. (2010),*Cloud Computing for Managing Apparel and Garment Supply Chains - An Empirical Study of Implementation Framework****; International Journal of Computer Science Issues*, volume 7(6), pp. 325-336;
[11] **Christauskas, C., Miseviciene, R. (2012),*Cloud Computing Based Accounting for Small to Medium Sized Business****; Inzinerie Ekonomika - Engineering Economics*, volume 23(1), pp. 14-21;

[12] **Miller, M. (2008),*Web-based Applications that Change the Way you Work and Collaborate Online****;*** *Que Publishing;*
[13] **Weinman, J. (2012),*Cloudonomics: The Business Value of Cloud Computing****;****Wiley;*
[14**] Diskiene, D., Galiniene, B., Marcinskas, A. (2008),** ***Management Attitude in the Context of Global Challenges: The Lithuanian Survey****; Transformation in Business& Economics*, volume 7(15), pp. 21 – 38;
[15] **Galiniene, B., Marcinskas, A. (2007),** ***Factors Determining the Quality of Business Valuation Services in the Transformation Context****; Transformation in Business& Economics*, volume 6(12), pp. 38-50;
[16] **CSA, ISACA (2012);*Cloud Computing Market Maturity Study****;*** Retrieved 12.02.2015 http://www.isaca.org/Knowledge-Center/Research/Documents/WSCC-Security-Considerations-Cloud-Computing_whp_Eng_0912.pdf;
[17**] Cisco, (2009);*The Cisco Powered Network Cloud: An Exciting Managed Services Opportunity****;*** Retrieved 30.01.2015;
http://www.hit.bme.hu/~jakab/edu/litr/Cloud/Cisco_Cloud_white_paper_c11-532553.pdf;
[18] **The Open Group (2011),*Cloud Computing Survey****;*** Retrieved 02.11.2014.https://www.opengroup.org/cloudcomputing/uploads/40/24144/Open Group Cloud Computing SurveyFINAL.pdf;
[19] **Ram, P. (2010),** ***Security as a Service (SaaS) as Securing User Data by Coprocessor and Distributing the Data***; *IEEE Trends in Information Sciences & Computing (TISC)*,volume 10, pp. 152-155;
[20] **Ernst&Young (2012),** ***Global Information Security Survey: Fighting to Close the Gap****;* Retrieved 11.11.2015.
http://www.ey.com/Publication/vwLUAssets/GISS2012/$FILE/EY_GISS_2012.pdf.
[21] **Khaled, M. K., Qutaibah, M. (2010),*Establishing Trust in Cloud Computing****;*** *IT Professional*, volume 12 (5), pp. 20–27;
[22] **Bernstein, D., Deepak, V. (2010),** ***Intercloud Security Considerations****; Proceedings of the Second IEEE International Conference on Cloud Computing Technology and Science (CloudCom '10)*, 2010, pp. 537–544;
[23]***Eurostat labour force database***. Retrieved 02.09.2015.
http://ec.europa.eu/eurostat/statistics-explained/index.php/EU_labour_force_survey_-_methodology;
[24]**Danktzker, M. L., Hunter, R. D. (2012),** ***Research Methods for Criminology and Criminal justicehttp://www.hit.bme.hu/~jakab/edu/litr/Cloud/Cisco_Cloud_white_paper_c11-532553.pdf;****Jones & Bartlett Learning;*
[25**] Anderson, D. R., Sweeney, D. J., Williams, T. A., Freeman, J., Shoesmith, E. (2010),*Statistics for Business and Economics – Second Edition***; *Cengage Learning.*