International Journal of Human Capital and Information Technology Professionals
Volume 7 • Issue 3 • July-September 2016

Cloud Storage Privacy and Security User Awareness:

A Comparative Analysis between Dutch and Macedonian Users

Adriana Mijuskovic, South East European University, Tetovo, Macedonia
Mexhid Ferati, Oslo and Akershus University College of Applied Sciences, Oslo, Norway

ABSTRACT

There are many factors influencing the user awareness level of privacy and security concerns when storing data on the cloud. One such factor is the users' cultural background, which has been an inspiration to many studies comparing various cultures. Along those lines, this paper compares the user awareness level between Dutch and Macedonian users, which has not been investigated before. An online study was conducted to measure users' attitude towards privacy and security of data in the cloud-based systems. The research process was conducted by delivering an online survey to Computer Science students and employees working in different software companies in the Netherlands and Macedonia. The comparative analysis indicates that there are differences in user's attitude towards storing private data in the cloud. The results of this paper demonstrate that Dutch compared to Macedonian users in general have higher level of awareness regarding the privacy and security of cloud storage.

KEYWORDS

Cloud Storage, Cloud Users, Privacy and Security Risks, User Awareness

INTRODUCTION

The increasing amount of data in various digital forms and the desire to have access to it from various devices has increased the importance of cloud storage. The advantage of having data on a cloud primarily stems from the need of having them available across multiple devices we usually use. Moreover, the uploaded data serve as a solid backup in case the device is damaged or lost. Especially with the rise of using mobile phones, the data storage and sharing has reached a high expansion level and became a need for every user (Guilloteau & Mauree, 2012). Because of this, the number of people considering cloud as an alternative storage is increasing immensely. For example, only Dropbox's 400 million users save 1.2 billion files to the cloud every 24 hours[1]. These data are of various nature with some being considered private, despite the fact that cloud storage is associated with a range of severe and complex privacy issues (Svantesson & Clarke, 2010).

Data privacy and security are two dimensions that become relevant with the introduction of cloud storage. Studies reveal that those are judged as the biggest threats when having user data in the cloud storage (Svantesson & Clarke, 2010). Privacy is the basic human right and the cloud service providers (CSPs) should take it in consideration within their policies (Pearson & Benameur, 2010). Privacy stands for protection and suitable use of user's personal information. For organizations, the

DOI: 10.4018/IJHCITP.2016070101

privacy includes application of laws, policies and standards by which the Personally Identifiable Information (PII) of individuals is managed. Regulations of data privacy exist in many countries and are applied when PII is stored and published on the cloud (Guilloteau & Mauree, 2012). Similarly, the security concern is also one of the major hurdles linked to cloud storage. The CSPs enforce data security by using different types of mechanisms such as firewalls and virtualization (Ruivo, Santos & Oliviera, 2015).

These mechanisms, however, do not fully protect against threats of unauthorized data access from outsiders (Shahzad, 2014). The privacy and security issues are considered when the data is collected, stored, processed and shared. The risk becomes even higher when the services are personalized based on user's location, calendar and social networks. Most of these services have a profiling and embedded tracking with mechanisms that can tailor the environment based on individual user's behavior (Pearson & Charlesworth, 2010). When users' data is moved to the cloud, it can be: 1) accessed by or sent over third parties, 2) used for unintended purposes, 3) can become subject to data protection laws for protection of customer's data and 4) not deleted when not needed anymore (Henze, Großfengels, Koprowski, & Wehrle, 2013). Users might not always be aware of these facts.

To understand this, studies have been conducted to investigate the level of user awareness concerning privacy and security of the data stored on the cloud (Horrigan, 2008; Ion, Sachdeva, Kumaraguru, & Čapkun, 2011). These studies reveal that users' awareness is generally low, and that the cultural differences play a great role in user attitudes towards the cloud storage. Considering the importance of the culture, in this paper we investigate the difference in awareness level between Macedonian and Dutch users, two very diverse cultures in terms of the dimensions described by Hofstede and Hofstede (2005) that can be easily compared on author's website[2]. Macedonia is not listed as a country on the website, but we compare it to Serbia, which in many aspects is very similar to the Macedonian culture. Based on these dimensions, we anticipate that Dutch users will be generally more aware than Macedonian users. More specifically, we hypothesize the following:

H1: Dutch users have higher awareness regarding the existing privacy and security risks when storing data in the cloud compared to Macedonian users.
H2: Dutch users store less sensitive data files in the cloud systems compared to Macedonian users.
H3: Dutch users are more familiar with the cloud service providers' rights regarding retaining copies of files and terms of disabling users' account compared to Macedonian users.

People gaining awareness of these issues is important so that in situations when users' expectations are not met and their privacy rights are violated, they have the right to sue the companies (Pearson & Charlesworth, 2009). Therefore, this paper attempts to identify users' awareness level about privacy and security regulations for most widely used cloud systems: Google Drive, Dropbox and OneDrive. In the following sections of this paper the authors present the literature review followed by the methodology used to collect and analyze the data. Afterwards, findings from the gathered data are presented and discussed. At the end, the paper is concluded with some ideas and directions for future efforts.

LITERATURE REVIEW

Most widely used cloud storages offer similar services that are comparable between each other. These systems share almost the same advantages, but also similar issues about privacy and security, such as, data loss, data replication, and unauthorized data delivery to third-party companies (Chu et al., 2013). There are many studies investigating various aspects of privacy and security, such as: explaining in detail the privacy and security weaknesses linked to cloud storing (Jivanyan, Yeghiazaryan, Darbinyan, & Manukyan, 2015; Zhao, Rong, Jaatun, & Sandnes, 2012); evaluating enterprise security risks

and cloud computing adoption (Joint, Baker, & Eccles, 2009); devising security guidelines and best practice recommendations (Jansen & Granse, 2011); or providing solution to encrypt the data before being sent to the cloud (Jivanyan et al., 2015; Kamara & Lauter, 2010). However, in limited numbers are the studies that investigate the user awareness concerning privacy and security in the cloud.

Studies of privacy awareness have been conducted in other areas besides cloud, such as: smartphones, Wi-Fi, and social media networks. Some of these studies show that users generally lack knowledge or are not particularly concerned about the privacy issues. For example, a study by Barkhuus and Dey (2003) shows that people are not very concerned about their privacy when using location-based services. Another study reports that users lack understanding of important privacy risks when using Wi-Fi (Klasnja et al., 2009). This study suggests that one effective way to improve awareness about Wi-Fi risks is to show users which aspect of their data is being transmitted. In the social media networks, studies conducted by Ho et al. (2013) and Goettke and Christiana (2007) reveal that many users are not aware of the privacy threats linked to social media networks and that these sites are not providing a flexible interface to help users protect their data. These studies are very concerning, because due to the lack of user awareness and proper privacy protection tools, huge quantities of user data, including personal information, pictures and videos are quickly falling into the hands of authorities, strangers, recruiters and even the public at large (Aimeur, Gambs & Ho, 2009).

Other studies reveal users' concerns regarding privacy. Study by Chin, Felt, Sekar, and Wagner (2012) shows that 60% of smartphone users are concerned that using mobile payments could put their financial and personal security at risk. Similarly, Ben-Asher et al. (2011) surveyed smartphone users and found that people consider information on their phones sensitive (e.g., photos and contacts) and worry about physical attacks on their phones.

A study conducted by the Pew Research Center surveyed the privacy concerns' level of American Internet users (Horrigan, 2008). In that survey, 63% of the American participants said they would be very concerned if the cloud storage provider retained copies of their files they had deleted. Additionally, 49% of participants said they would be concerned if the provider gave their files to law enforcement agencies when asked.

Many studies consider the importance of culture when addressing the issues of privacy and security. For example, Ion et al (2011) studied the privacy concerns and expectations from populations of two distinctive cultures (India and Switzerland) and observed the cultural differences that affect their expectations from the cloud. The results of that study indicate a difference in the attitude towards storing sensitive data in the cloud between Indian and Swiss users. The Swiss users were more aware about the lack of guarantees and they practice to store less sensitive data in the cloud. They also consider the government monitoring of cloud-stored data as a privacy infringement, while the Indian users consider it as an important act in protection against terrorism. Similarly, the study conducted by Krasnova and Veltri (2010) shows that Germans, compared to Americans, have lower privacy concerns, which according to another study this may be linked to low Power Distance Index (Milberg, Smith, & Burke, 2000).

The Power Distance Index (PDI) and five other indexes have been defined and studied by Hofstede, Hofstede & Minkov (2010). In their book, authors report a study of different cultures conducted in seventy countries over a period of thirty years. Led by these cultural differences with respect to people's attitude towards privacy and security, we conduct our study to compare the difference between Dutch and Macedonian users.

METHODOLOGY

Data Collection and Procedure

In order to investigate the level of users' awareness about privacy of data in the cloud systems, qualitative and quantitative data collection methods were combined. Referring to several other articles (Horrigan, 2008; Ion et al, 2011; Quah & Röhm, 2013; Danaher & Chong, 2014), which

investigated similar issues, the researchers found that the most suitable research method would be an online survey. Therefore, in this study the researchers have chosen to use a questionnaire that was composed of closed- and open-ended questions.

The questionnaire was used to investigate the awareness level of Macedonian and Dutch users about existing privacy and security risks when storing data in the cloud. It was delivered online through Facebook and LinkedIn to all users from Macedonia and the Netherlands and all participants were given detailed information about the main purpose of this study. The survey included 25 questions; 5 were open-ended while 20 questions were closed-ended questions. The main purpose of this online survey was to get comparative data about the awareness level of both Macedonian and Dutch users concerning the existing privacy and security risks when storing data in the cloud.

Participants

A total number of 66 participants were included in this study, where 38 respondents were from Macedonia and 28 were from the Netherlands. Seventeen respondents from Macedonia and 13 from Netherlands were employees at software companies. The number of Macedonian students majoring in Computer Science was 21, while 15 students where from the Netherlands. The greatest number of respondents (69.7%) belonged to the 20-29 age group, 19.7% belonged to the 30-39 group, 7.6% were 40 or older and only 3% of all respondents were 19 years old or younger. Most of the participants were male (81.8%).

Data Analysis and Method

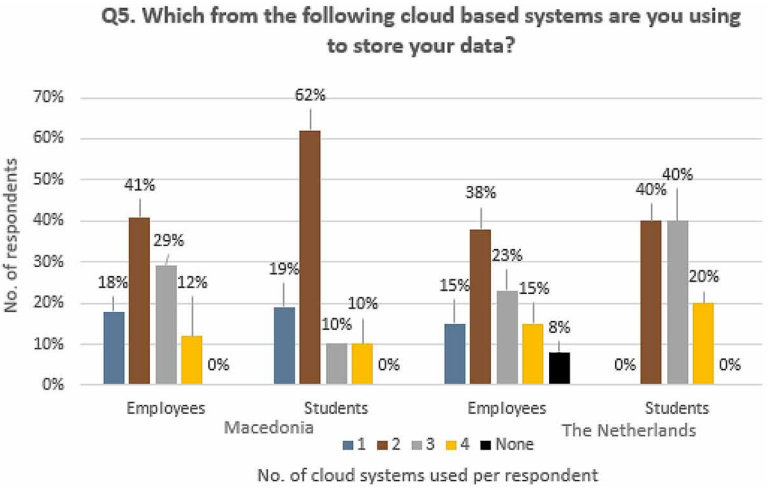
The main purpose of this study was to measure the level of users' awareness about privacy and security weaknesses for cloud-based systems such as Dropbox, Google Drive and OneDrive in the Republic of Macedonia and the Netherlands. This study includes research and comparative analysis of data about the awareness level of Macedonian and Dutch users regarding privacy and security risks. The next step involved analyzing the answers collected from the quantitative questions and the results were retrieved by using queries, formulas and graphs. The quantitative data analysis was done by using Excel.

RESULTS

In this section, the main findings concerning the extent of Macedonian and Dutch users' awareness about the proposed cloud privacy and security issues are presented. Users' answers regarding Q5: *"Which cloud systems are you using?"* were grouped in five categories; users who use 1, 2, 3, 4 or none of the cloud services. The options were the following: *GoogleDrive, Dropbox, OneDrive, iCloud, SygarSync, Spideroak, Box.Com, none* and *other*. Figure1 shows that most of the respondents, 62% of the Macedonian students and 40% of the Dutch students use two cloud-based systems. Only 41% of the Macedonian employees and 38% of the Dutch employees use two cloud systems. These results indicate that both sample groups comparably use few cloud-based systems with Google Drive and Dropbox being the most preferable. More precisely, the indication is that the Macedonian users (especially students) use two cloud systems more than the Dutch users.

The answers that contribute towards the main goal of this study are linked to questions 7–25 from the questionnaire. Fifty-nine percent of the Macedonian employees and 31% of Dutch employees have noted that they know five to nine security weaknesses when answering the multiple choice question *Q13*: "*Which of the following privacy and security weaknesses have you heard of or you know about?"* The provided answers were: *Lack of Control, Shared Environment, Physical Security, Storage Security, No Privacy on Sharing, Unauthorized sharing, NonHTTPS shortened URL, sharing of Trash Files, Regulatory Compliance* and *Indiscriminate Accessing URL.* Only 10% of the Macedonian students and 27% of Dutch students knew about 5 to 9 security weaknesses. The percentage of users who are aware about 4 security weaknesses is very low from both Macedonian

Figure 1. Number of used cloud systems per respondent. The two respondent groups have shown that they use mostly two cloud-based systems



and Dutch groups of respondents. An interesting finding is that none of the Macedonian students have chosen the answer "none", in contrast to 33% from the Dutch students. These results indicate that the Macedonian employees are more aware about higher number of security weaknesses than the Dutch employees. In general, there is a low percentage of the Dutch and Macedonian students who are aware about 5 to 9 security weaknesses, although the responsiveness from the Dutch students is higher than the Macedonian students. Details are shown in Figure 2.

Another aspect that we wanted to explore was to discover the level of concern regarding retaining copies of files that are stored in a specific cloud system after the user deletes them. Based on the results obtained and graphically presented in Figure 3, it may be noticed that there is a high percentage of students from Macedonia and the Netherlands who have stated the answer: "I would be concerned". Even 71% of the Macedonian students and 53% of the Dutch students have stated that they will be concerned if the cloud service provider retains copies of their files after being deleted. These numbers indicate that the Macedonian students compared to Dutch students are more aware regarding the concerns' about retaining of users' files by the CSPs. While on the other hand, 38% of Dutch employees have chosen this answer and therefore they are more aware than the Macedonian employees (29%). Ultimately, it can be inferred that the Macedonian students are even more aware than the Dutch employees regarding the security weaknesses of the cloud.

Very small percentage of users of all groups from both countries have provided "I would be highly concerned" as an answer to Q7. Twenty-four percent of the Macedonian employees and 14% of the Macedonian students have chosen the response "I would be highly concerned", while only 15% of the Dutch employees and 7% of the Dutch students have chosen the same response (refer to the results provided in Figure3).

Further, we investigated user's knowledge about certain rights maintained by the cloud service providers based on the results given in Figure 4. The majority of Macedonian employees (47%) have responded that the cloud service providers have the right to disable the user's account only in special cases. A high percentage of the Dutch employees (46%) have stated that the CSPs have the right to disable the user's account, but only with a notification provided in advance. Indeed, the correct answer is that the cloud service provider may disable the user's account at any time and for any reason with or without any prior notice. The responsiveness for this answer was quite low, as only 33% of Dutch students and 5% of the Macedonian students gave this response. Thirty-one percent of the Dutch employees gave the correct response, while none of the Macedonian employees was correct.

Figure 2. Students' awareness level about most of the provided cloud security weaknesses is higher than the employees' awareness level

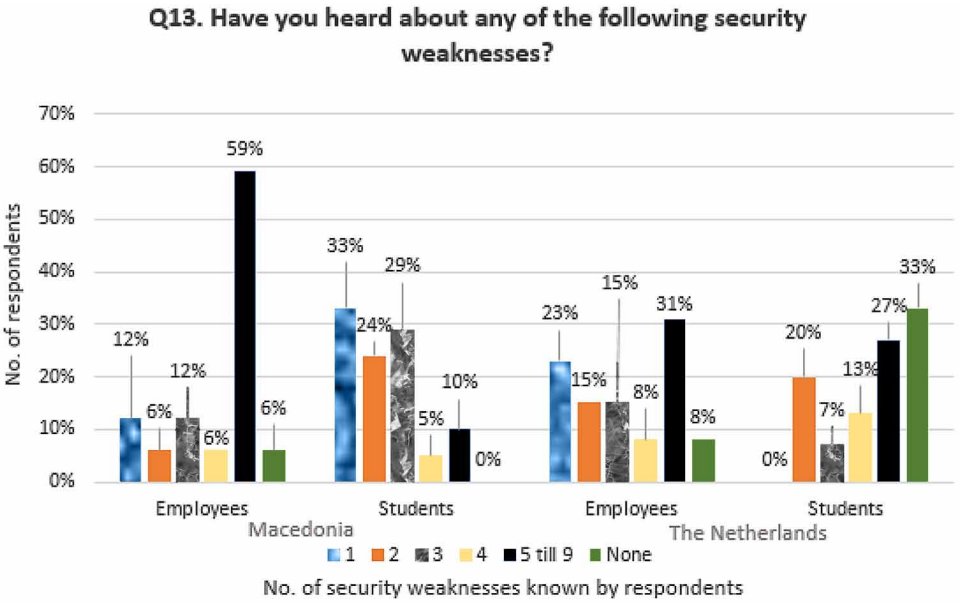
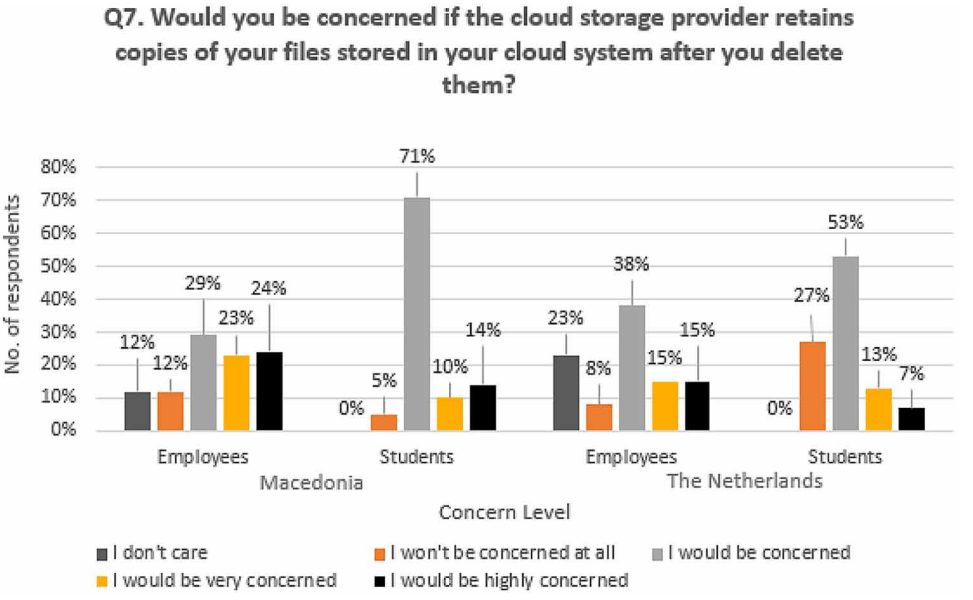


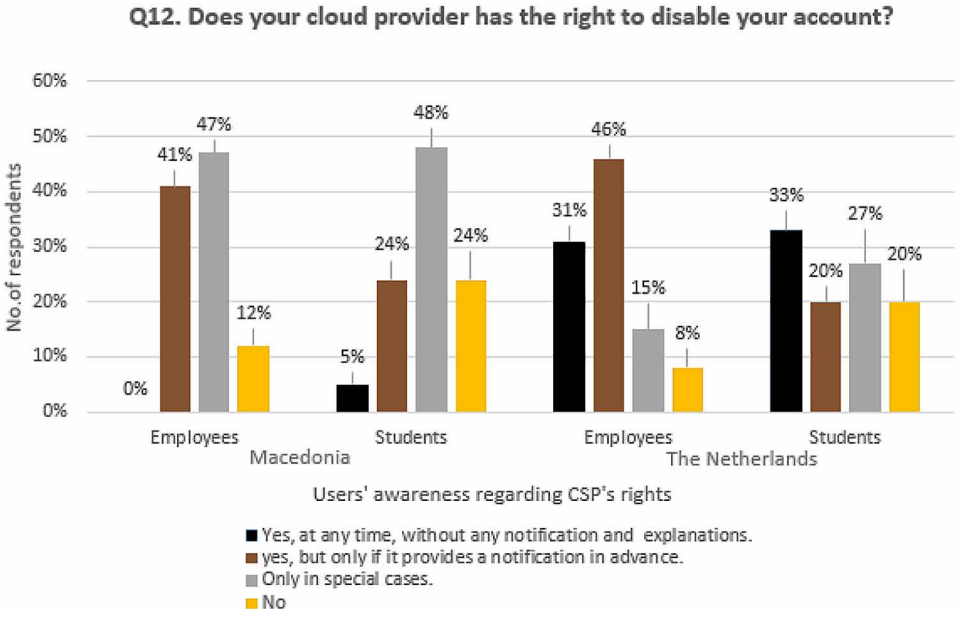
Figure 3. Concern level of users about CSP's retention of deleted files



Therefore, it can be inferred that Dutch users (employees and students) compared to Macedonian users know more about the rights of CSPs regarding disabling of users' accounts.

Concerning the awareness of privacy risks, Figure 5 shows that 47% of Dutch students and only 14% of the Macedonian students are aware about three privacy risks when storing data in the cloud.

Figure 4. Users' awareness regarding the CSP's ability to disable user's account



Therefore, it may be inferred that the Dutch students are more aware than the Macedonian students regarding the privacy issues. When referring to the employees group, it may be noticed that both Macedonian employees (35%) and Dutch employees (38%) are equally aware about three specific privacy risks when using the cloud. An interesting finding is that the number of Macedonian employees who are aware about three privacy risks is the same with the number of Macedonian employees who are not aware about any of the provided privacy risks. Therefore, it can be implied that Dutch respondents (both students and employees) are more aware than the Macedonian respondents about the privacy issues of the cloud.

In order to examine more in-depth whether the Macedonian or Dutch users are more aware regarding storing private data in the cloud, we conducted an in depth analysis of *Q8 "Which from the following sensitive data files are you storing in your cloud systems."*Figure 6 shows that the Macedonian students (76%) tend to store more private photos compared to Dutch students (20%). The results for Dutch and Macedonian are similar. These results indicate that the Macedonian students compared to Dutch students are less aware regarding the risks of storing sensitive private data in the cloud.

The data obtained from the respondents' answers to *Q10" Does your cloud service provider has the right to see or modify your stored files within your cloud account?"* show that the Macedonian users, both employees (65%) and students (57%) do not know whether the cloud service provider has the right to view or modify users' data files. On the other hand, the percentage of Dutch users who have chosen the same answer *"I don't know*" is lower; 46% of the Dutch employees and 40% of the students group (Figure 7). Therefore, it may be inferred that the Dutch users are more aware about the CSPs' rights to see or modify user's data files in the cloud.

Interesting responses were collected from question *Q11 "When you delete a file from your cloud account, what do you think will happen?"* The percentage of employees' responses is quite similar between Macedonian (29%) and Dutch employees (38%), but students' responses from both groups considerably differ. Only 14% from the Macedonian students responded that copies of the files will still exist for few weeks in the cloud, which is considerably lower than the 66% of Dutch students

Figure 5. Users' awareness regarding privacy risks when storing data in the cloud

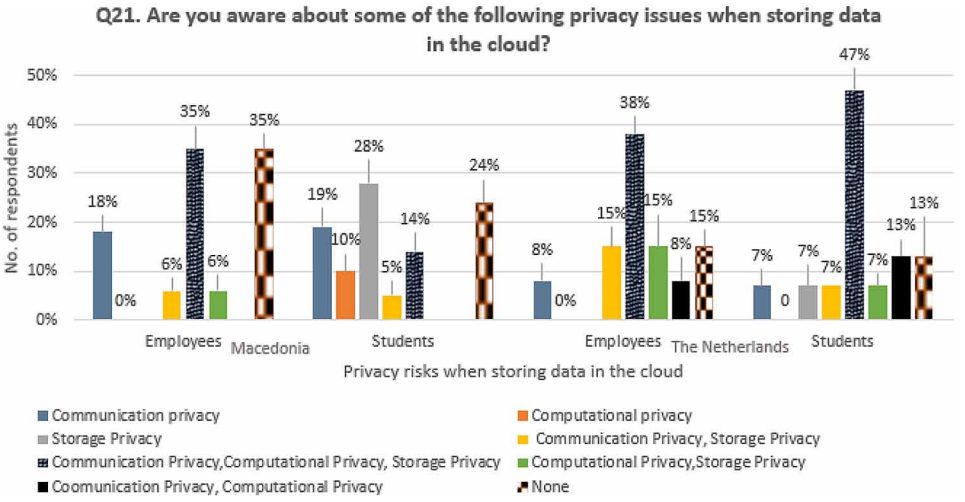
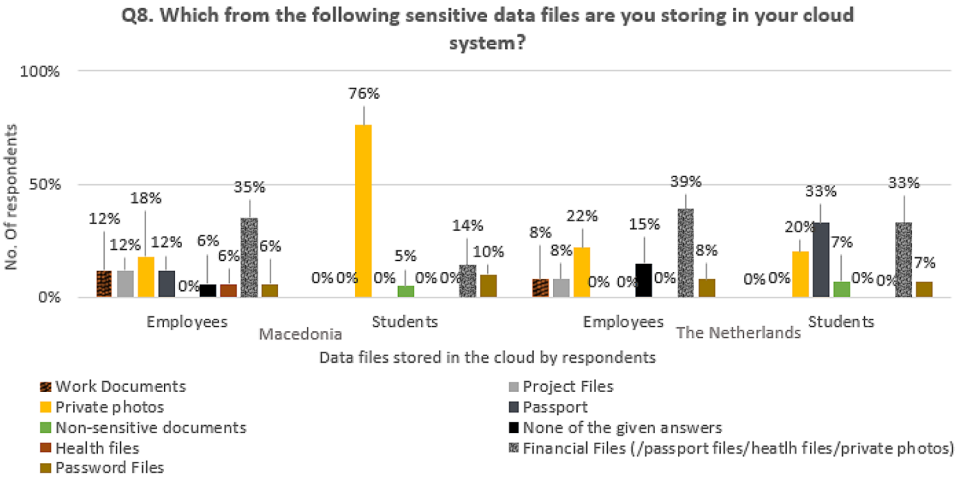


Figure 6. Preferred data files stored in the cloud by students and employees from Macedonia and The Netherlands



who provided the same answer. From these results shown in Figure 8, it may be derived that the Macedonian students are less aware compared to Dutch students about what happens after the files are deleted from the cloud systems. The correct response to this question is that copies of the files will still exist after a few weeks in the user's cloud system.

The results from *"Q18. Which from the following cloud service providers options you would take into consideration?"*, show that there is almost no difference between the responses of employees and students from both countries (Figure 9). The majority of Macedonian students (57%) and Dutch students (60%) would prefer to pay for cloud services that will provide privacy and security protection of their data files. The same answer was also preferred by the employees from both countries, Macedonia (59%) and the Netherlands (62%). Overall, around 40% of all respondent groups would prefer to use a free version of a cloud storage system, which does not provide any privacy or security protection of users' data. This could indicate that the majority of Macedonian and Dutch users are

Figure 7. User awareness about the rights of cloud service provider to view or modify users' data

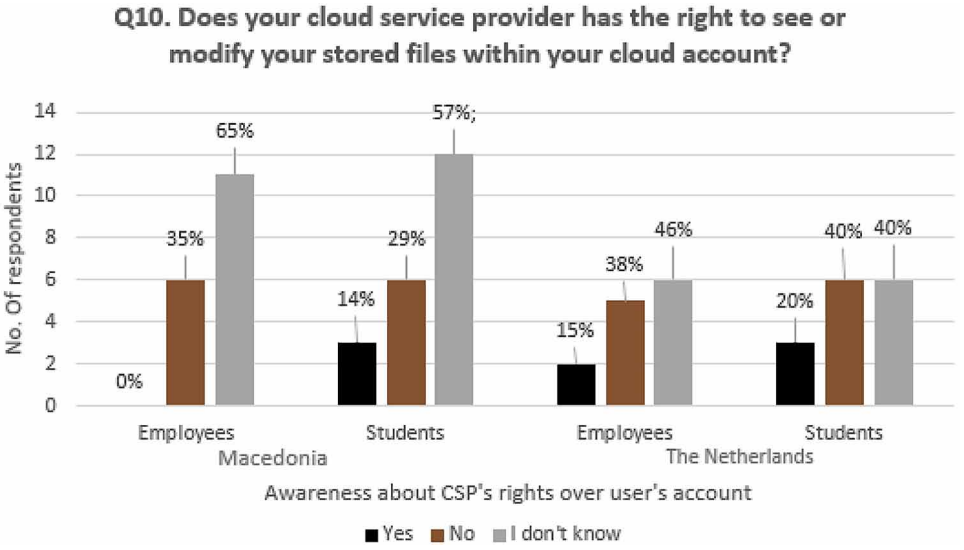
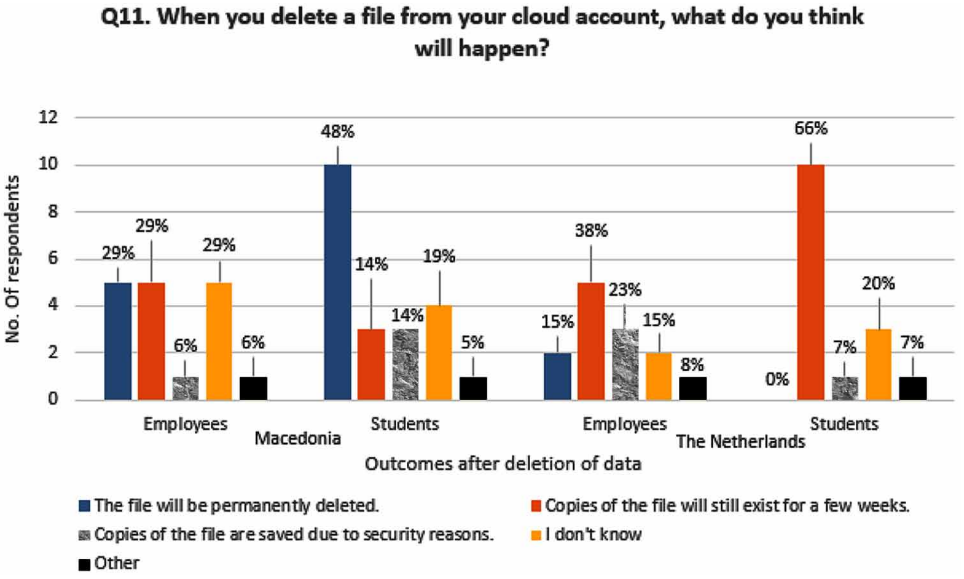


Figure 8. User awareness about what happens after deletion of data from the cloud system



aware that it is a better option to use a paid cloud storage service that would ensure privacy and security of users' data.

Responses gathered from "*Q19. Do you currently pay for cloud storage?"* are quite interesting because the majority of respondents have stated that they currently do not pay for cloud storage services (Figure 10). Even 86% from Macedonian students and 67% from the Dutch students are not currently paying for cloud storage. Additionally, there is almost similar percentage between the Macedonian employees (82%) and the Dutch employees (77%) who are not paying for cloud. This is

Figure 9. Cloud server options chosen by the respondents

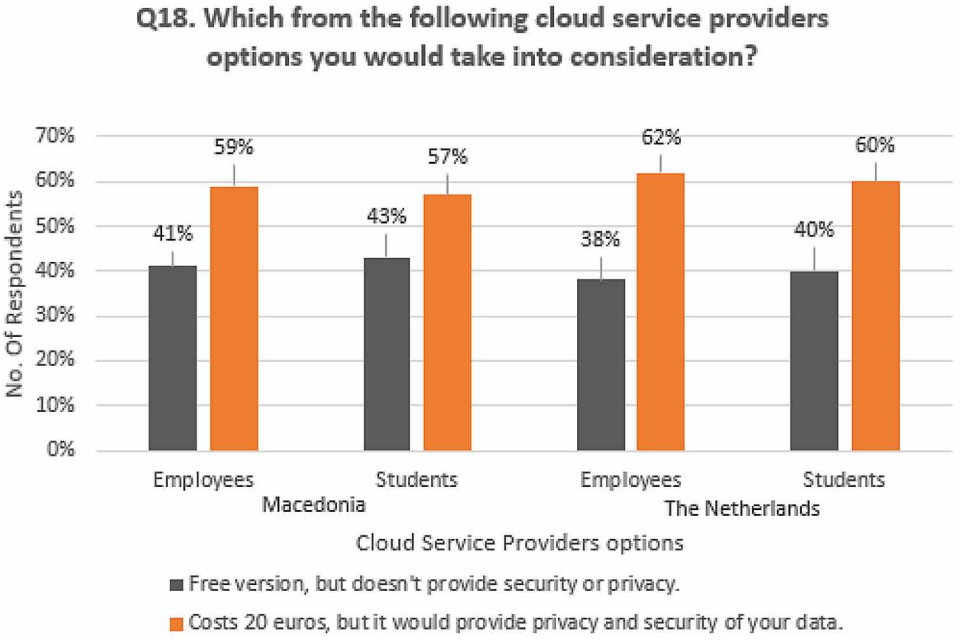
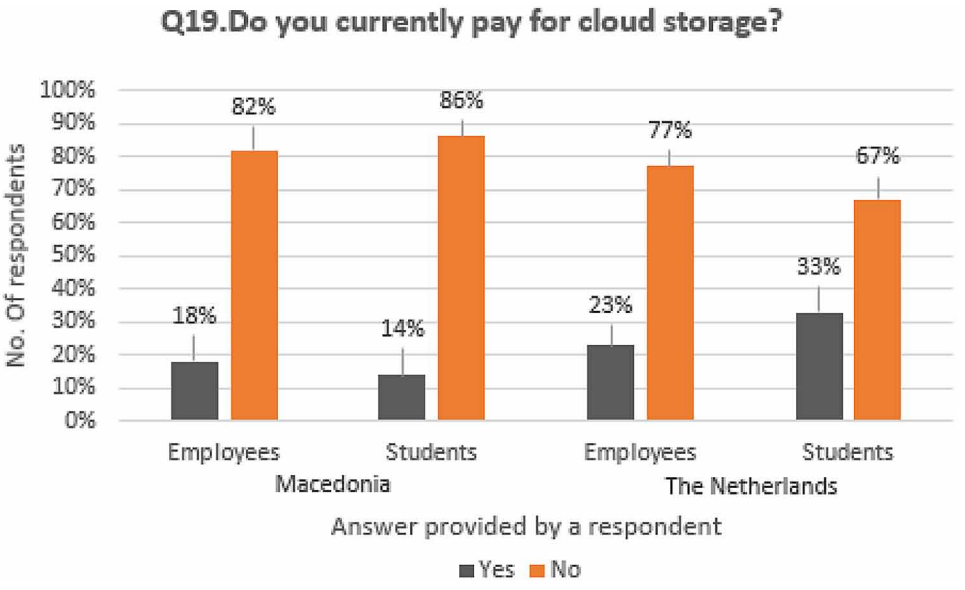


Figure 10. Users paying for cloud storage



an indication that on average all users will pay 20 euros for storage for increased privacy and security, but greater percentage of them do not pay for the services.

This is an interesting finding, which needs further investigation, but one possible reason could be that users assume that they will gain no privacy or security protection even if they pay. Another reason could be that the pricing of cloud storage right now is only linked to the increased storage, which people do not want or need.

Figure 11 reveals important data about privacy principles of the cloud and includes several answers: *Choice Consent and Control, Scope/Minimization, Access and Accuracy, Security safeguards, Challenging compliance, Limiting use-disclosure and retention, Accountability, None and other*. The findings show that the Macedonian students (62%) and only 20% from the Dutch students are aware about only a single privacy policy. Only 6% of the Macedonian employees and 10% of the Macedonian students are aware about the existence of five privacy policies. On the other hand, there are no Dutch students and employees who are aware about five privacy policies. The majority of Dutch students (53%) are not aware about any of the provided privacy policies that guarantee privacy of data in the cloud. These results indicate that Macedonian compared to Dutch users are more aware about privacy policies of the cloud systems.

The answers listed for the privacy regulation laws in Q24 were the following: *The EU's data protection directive (95/46/EC), COPPA, GLB, HIPPA, none* and *other.* Based on the results shown in Figure 12, both student groups from Macedonia (90%) and the Netherlands (80%) are similarly aware about a single privacy regulation law. The same applies for the Macedonian employees (59%) and the Dutch employees (69%). Only 6% of the Macedonian employees are aware about five privacy regulation laws for protecting data in the cloud, while none of the Dutch students and employees are aware of that many regulation laws. These results reveal a certain consistency in users' response, which shows users being aware of only one privacy regulation law.

DISCUSSION

The results of this study show that two hypotheses (H1 and H2) are partially accepted and one (H3) completely accepted. The first hypothesis stated that the Dutch compared to Macedonian users are more aware about existing privacy and security risks when storing data in the cloud. Based on the results shown in Figure 5 the Dutch compared to Macedonian students have higher awareness level

Figure 11. Privacy policies for data in cloud

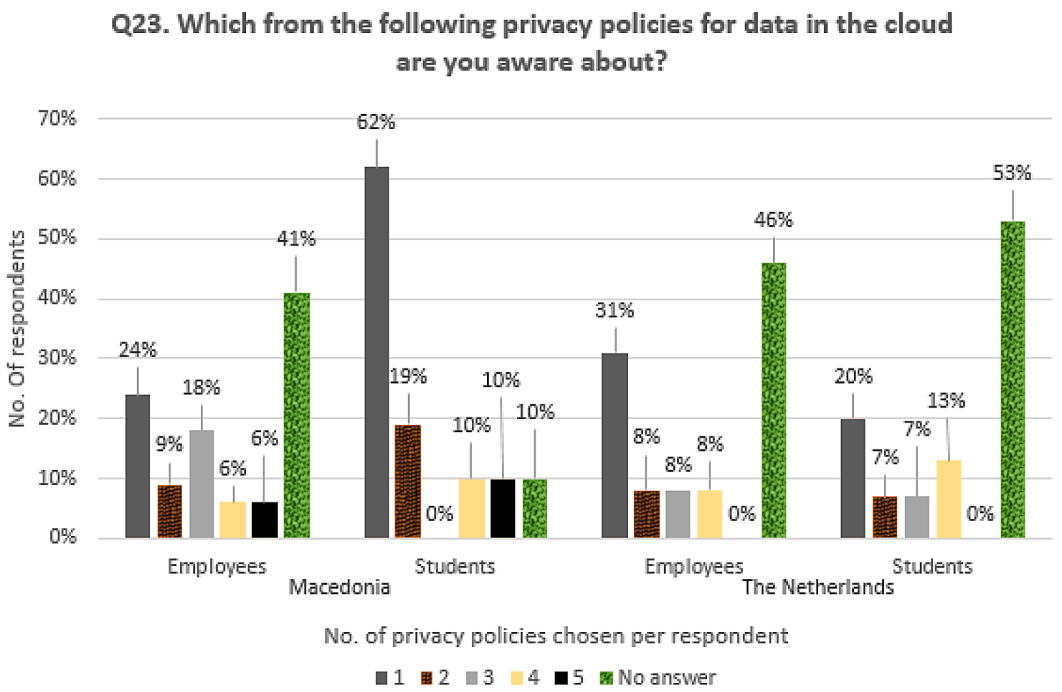
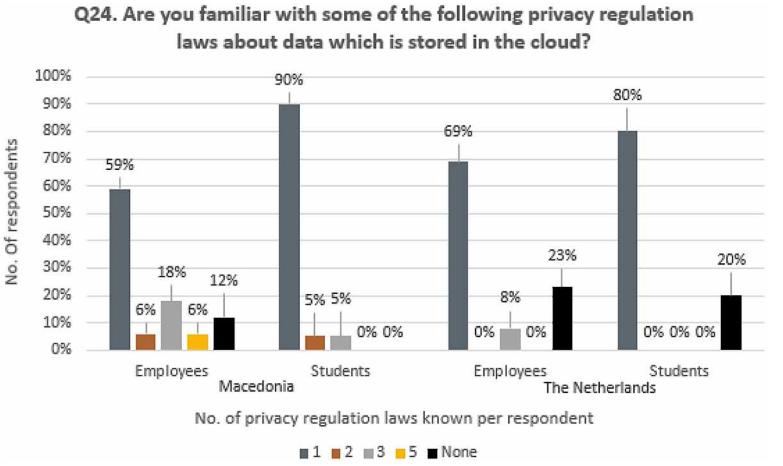


Figure 12. Privacy regulation laws for data in the cloud



regarding existing privacy issues when using the cloud. Figure 2, however, shows the opposite for the employees; Macedonian employees are more aware about higher number of security weaknesses than the Dutch employees are. Similarly, according to Figure 3, higher percentage of Macedonian compared to Dutch students are more concerned if the CSPs retain copies of deleted files. When referring to the employee groups, both Dutch and Macedonian respondents are equally concerned about the same topic. Consequently, it can be concluded that the first hypothesis can be partially accepted.

The second hypothesis stated that Dutch users store less sensitive data in the cloud compared to Macedonian users. This is true only for students, since employees of both countries practice similar behavior considering storing sensitive data on the cloud (see Figure 6). Hence, we conclude that this hypothesis is also partially accepted.

The third hypothesis is fully accepted based on the findings that the Dutch users are more aware about the CSPs' rights regarding using users' data and disabling of users' accounts. A reliable support for this hypothesis are the data results from Figure 7 and Figure 4 showing that Dutch users (students and employees) are more aware than the Macedonian users. Further support is shown in Figure 8, which shows that Dutch users are more aware that copies of the file deleted by the user will still be available on the cloud for few more weeks.

The results show that for six questions Dutch users (students and employees) generally express higher awareness compared to Macedonian users. Only when answering the first question, the Macedonian users showed higher awareness than the Dutch users. In all other cases, results were not showing favor for any of the groups.

Comparing only the employees, in nine questions Dutch showed higher awareness than Macedonian users, who on the other hand showed higher results only in two questions. Similarly, Dutch students showed higher awareness in seven questions, while Macedonian students in four. In all other cases the employee groups from both countries showed equal awareness about the privacy and security issues when storing data files in the cloud.

Overall, when comparing the Dutch employees' awareness to Dutch students' awareness, the results clearly showed that the Dutch employees have higher awareness about more privacy and security topics (9 questions) than the Dutch students (7 questions). When comparing students to employees in Macedonia, the students have higher awareness about more questions (4), than the Macedonian employees (2).

The significance of this study lies in revealing the difference of the awareness level between Dutch and Macedonian users. Such results may be related to Milberg et al (2000) study, which shows

that the cultural values differ to some certain degree across many countries and highly influence the society's responses. In that study, it was also explained that the cultural values may be linked to the individuals' privacy concerns and awareness. According to Milberg, the cloud users who live in high "individualism" countries (in our study - The Netherlands), would have higher level of awareness and concern regarding the privacy and security risks when storing data in the cloud. When mentioning individualism, we refer to the belief that every person has the right of a private life. There are countries where the individualism is of lower importance (e.g. Macedonia), where there is a higher influence of the organizations' practices and policies that might intrude person's private life.

One of the major reasons why the Dutch users have higher awareness level about privacy and security risks than the Macedonian users can be based on findings provided by Hofstede et al (2010). One of the major findings which is linked to the privacy and security concern level is that the countries with high PDI exhibit lower level of trust and in our study it was shown that the Dutch users have definitely lower level of trust when using the cloud systems. The reasons behind the low level of trust (higher privacy and security concerns level) can be understandable since the CSPs hold rights that can expose the users' data files to high privacy and security risks. In another study (Quah & Röhm, 2013), the Australian respondents believed that the cloud computing made it more difficult for organizations to find a way to protect customers' data and the greatest concern was regarding the risk of losing control over data locations and data unauthorized access. The lower privacy and security concern level of the Macedonian users can be referred to several similar studies. Similar results are found in study by Ion et al (2011), which showed that there is an alarmingly high percentage of users from Switzerland and India, who are not aware that the CSPs obtain the right to modify user data and disable user accounts at any time. This outcome is derived as a result of the fact that users do not read privacy policies and terms of service of the cloud services they use. Different privacy and security concern level could also be related to several different factors, such as individuals' previous education, cultural background and psychological aspects (Stone, Gueutal, Gardner, & McClure, 1983).

CONCLUSION

In this paper, we explored Macedonian and Dutch users' awareness level of existing security and privacy weaknesses when using the cloud-based services. Regardless of cloud systems' popularity, studies show that there are many privacy and security weaknesses in the cloud. Concerning this, the results of this study indicate that the cloud storage users are generally aware of existing privacy and security issues, however they lack detailed knowledge about existing issues and solutions to those issues. Dutch users in general showed higher awareness compared to Macedonian users and this is because of the different cultural values these societies hold.

The limitation of this study is that the number of the Macedonian participants (38) was higher than the number of Dutch participants (only 28), and that we only received 66 responses in total. Further research on identifying new measures and frameworks to protect users' data in the cloud is necessary. Some of the possible measures that researchers should explore are: 1) The effect of changing the content and the presentation of privacy policies in increasing user awareness concerning privacy and security threats, and 2) To determine if cloud services provide better visibility into security settings by adopting stronger authentication mechanisms, such as two-factor authentication, access log visualization, etc. Furthermore, this study should increase awareness level of users when exposing private data in the cloud and establish the comparison of the concern level about privacy and security risks between the Macedonian and Dutch users due to the existing differences between the cultural values.

REFERENCES

Aimeur, E., Gambs, S., & Ho, A. (2009). UPP: user privacy policy for social networking sites. *Proceedings of the Fourth International Conference on Internet and Web Applications and Services ICIW'09*. (pp. 267-272). IEEE. doi:10.1109/ICIW.2009.45

Barkhuus, L., & Dey, A. K. (2003). Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In INTERACT (Vol. 3, pp. 702-712).

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011). On the need for different security methods on mobile phones.*Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (pp. 465-473). ACM. doi:10.1145/2037373.2037442

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 1). ACM. doi:10.1145/2335356.2335358

Chu, C. K., Zhu, W. T., Han, J., Liu, J. K., Xu, J., & Zhou, J. (2013). Security concerns in popular cloud storage services. *IEEE Pervasive Computing / IEEE Computer Society [and] IEEE Communications Society*, *12*(4), 50–57. doi:10.1109/MPRV.2013.72

Danaher. M & Chong, C. J. (2014). User Concerns on Cloud Security - A UAE Perspective. *International Journal of Computer and Information Technology*, 3(6), 1264 - 1267.

Goettke, R., & Christiana, J. (2007). Privacy and online social networking websites (Special Topics in Computer Science Computation and Society: Privacy and Technology). *Computer Science*, 2007, 199r.

Guilloteau, S., & Mauree, V. (2012). Privacy in Cloud Computing. ITV-T Technology Watch Report.

Henze, M., Großfengels, M., Koprowski, M., & Wehrle, K. (2013). Towards data handling requirements-aware cloud computing. *Proceedings of the 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom)* (Vol. 2, pp. 266-269). IEEE. doi:10.1109/CloudCom.2013.145

Ho, A., Maiga, A., & Aïmeur, E. (2009). Privacy protection issues in social networking sites. *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications AICCSA '09*. (pp. 271-278). IEEE. doi:10.1109/AICCSA.2009.5069336

Hofstede, G., Hofstede, G. J., & Minkov (2010). *Cultures and organizations: Software of the Mind*. New York, NY: McGraw Hill.

Horrigan, J. (2008). *Use of cloud computing applications and services*. Pew Internet & American Life Project.

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011). Home is safer than the cloud!: privacy concerns for consumer cloud storage.*Proceedings of the Seventh Symposium on Usable Privacy and Security* (p. 13). ACM. doi:10.1145/2078827.2078845

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing (NIST special publication 800).

Jivanyan, A., Yeghiazaryan, R., Darbinyan, A., & Manukyan, A. (2015). Secure Collaboration in Public Cloud Storages. In Collaboration and Technology (pp. 190-197). Springer International Publishing. doi:10.1007/978-3-319-22747-4_15

Joint, A., Baker, E., & Eccles, E. (2009). Hey, you, get off of that cloud? *Computer Law & Security Report*, *25*(3), 270–274. doi:10.1016/j.clsr.2009.03.001

Kamara, S., & Lauter, K. (2010). Cryptographic cloud storage. In *Financial Cryptography and Data Security* (pp. 136–149). Springer Berlin Heidelberg. doi:10.1007/978-3-642-14992-4_13

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009). When i am on wi-fi, i am fearless: privacy concerns & practices in everyday Wi-Fi use.*Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1993-2002). ACM. doi:10.1145/1518701.1519004

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences (HICSS)* (pp. 1-10). IEEE.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, *11*(1), 35–57. doi:10.1287/orsc.11.1.35.12567

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. *Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 693-702). IEEE. doi:10.1109/CloudCom.2010.66

Pearson, S., & Charlesworth, A. (2009). Accountability as a way forward for privacy protection in the cloud. In *Cloud computing* (pp. 131–144). Springer Berlin Heidelberg. doi:10.1007/978-3-642-10665-1_12

Quah, A. M. Y., & Röhm, U. (2013). User awareness and policy compliance of data privacy in cloud computing. *Proceedings of the First Australasian Web Conference* (pp. 3-12). Australian Computer Society, Inc.

Ruivo, P., Santos, V., & Oliveira, T. (2015). Success Factors for Data Protection in Services and Support Roles: Combining Traditional Interviews with Delphi Method. *International Journal of Human Capital and Information Technology Professionals*, *6*(3), 56–70. doi:10.4018/IJHCITP.2015070104

Shahzad, F. (2014). State-of-the-art survey on cloud computing security Challenges, approaches and solutions. *Procedia Computer Science*, *37*, 357–362. doi:10.1016/j.procs.2014.08.053

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *The Journal of Applied Psychology*, *68*(3), 459–468. doi:10.1037/0021-9010.68.3.459

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Report*, *26*(4), 391–397. doi:10.1016/j.clsr.2010.05.005

Zhao, G., Rong, C., Jaatun, M. G., & Sandnes, F. E. (2010). Deployment models: Towards eliminating security concerns from cloud computing. *Proceedings of the 2010 International Conference on High Performance Computing and Simulation (HPCS)* (pp. 189-195). IEEE.

ENDNOTES

1 https://www.dropbox.com/news/company-info_
2 http://geert-hofstede.com/countries.html_

APPENDIX

Survey Questions

Cloud Storage Privacy and Security User Awareness: A Comparative Analysis between Dutch and Macedonian Users

The purpose of this research is to obtain an extended and adapted version of my previous research paper regarding its publication in IJHCITP.

* Required

1. What is your age? *

-19 or younger
- 20 to 29
- 30 to 39
- 40 or older

2. What is your gender? *

- Female
- Male

3. In which country do you live? *

- Macedonia
- The Netherlands

4. What is your occupation? *

- Computer Science student
- Employee at a software company

5. Which from the following cloud based systems you are using to store your data? (Choose all that apply)

- Google Drive
- Dropbox
- One Drive (formerly Sky Drive)
- iCloud
- Sugar Sync
- Spider Oak
- Box.Com
- None
- Other:

6. What is the main reason for using the specific cloud based system/systems?

7. Would you be concerned if the cloud storage provider retains copies of your files stored in your cloud system after you delete them? *

- I don’t care
- I won’t be concerned at all
- I would be concerned
- I would be very concerned
- I would be highly concerned

8. Which from the following sensitive data files are you storing in your cloud system? *

- Financial Files
- Passport
- Health history files
- Password lists
- Private photos
- None of the provided answers
- Other:

9. Which one from the provided answers you consider it as a more secure storage? *
- Cloud storage
- Local storage
- Both
- None
10. Does your cloud service provider has the right to see or modify your stored files within your cloud account? *
- Yes
- No
- I don't know
11. When you delete a file from your cloud account, what do you think will happen? *
- The file will be permanently deleted.
- Copies of the file will still exist for a few weeks.
- Copies of the file are saved due to security reasons.
- I don't know
- Other:
12. Does your cloud provider has the right to disable your account? *
- Yes, at any time, without any notification and explanations.
- Yes, but only if it provides a notification in advance.
- Only in special cases.
- No
13. Have you heard about any of the following security weaknesses? *
- Lack of Control
- Shared Environment
- Physical Security
- Storage Security
- No privacy on Sharing
- Unauthorized sharing
- NonHTTPS shortned URL
- Sharing of Trash Files (nonDead URL)
- Regulatory Compliance
- Indiscriminate accessing URL
- None
- Other:
14. Would you be able to explain some of the security weaknesses that are mentioned above? *
15. Are you familiar with some of the following security solutions for protection of data in the cloud? *
- Simple encryption
- Secret Sharing
- Secure Multiparty Computation
- Fully Homomorphic Encryption
- Processing non-decrypted data
- None
- Other:
16. What do you know about some of the data protection solutions for the cloud mentioned in Q.15? *
17. Do you know which from the following cloud service providers have an Advanced Encryption Standard for data security protection? *
- GoogleDrive
- Dropbox

- iCloud
- OneDrive
- I don't know
- Other:

18. Which from the following cloud service providers options you would take into consideration?
- Free version, but doesn't provide security or privacy.
- Costs 20 euros, but it would provide privacy and security of your data.

19. Do you currently pay for cloud storage?
- Yes
- No

20. Please state your reasons to your previous answer?

21. Are you aware about some of the following privacy issues when storing data in the cloud? *
- Communication privacy (privacy of data while in transit from client to cloud server)
- Computational privacy (privacy of data being processed at an untrusted cloud server)
- Storage privacy (privacy of archival data at cloud server)
- None
- Other:

22. Please state your reason about your choice from the previous question? *

23. Which from the following privacy policies for data in the cloud are you aware about? *
- Choice Consent and Control
- Scope/minimization
- Access and accuracy
- Security safeguards
- Challenging compliance
- Limiting use- disclosure and retention
- Accountability
- None
- Other:

24. Are you familiar with some of the following privacy regulation laws about data which is stored in the cloud? *
- The EU's data protection directive (95/46/EC)
- COPPA
- GLB
- HIPPPA
- None
- Other:

25. The EU's data protection directive (95/46/EC) provides: *
(only one valid answer is possible)
-The users with certain basic rights with respect to their personal data and at the same time demanding "service and data controllers" to follow rules about processing or user's data.
- Rules which limit the cloud service providers' rights in the way of abusing user's data
- Protection of user's data only if the user chooses an option for additional data security within the cloud service
- I don't know
- Other: