User Awareness of Existing Privacy and Security Risks when Storing Data in the Cloud

Adriana Mijuskovic, Mexhid Ferati

Abstract: *Many studies have ranked the security and privacy of cloud-based systems to be a major concern for their adoption by companies, however, there are not many studies investigating users' awareness level about these issues. An online study was conducted to study users' attitude towards privacy and security of data in the cloud-based systems. The research was conducted by delivering an online questionnaire to Computer Science students and employees working in software development companies. The results showed that users in general are aware of existing privacy and security risks when storing data in the cloud, but they lack knowledge when asked to describe those risks and threats in detail. This study indicates a necessity to increase the privacy and security awareness to cloud users about the risks when storing their data in the cloud.*

Key words*:* ***Cloud storage, User awareness, Privacy and security risks***

INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be provisioned and released with minimal management effort or service provider interaction [15]. It is a new term in the Information Technology, which can be also defined as a large pool of accessible virtualized resources. With the appearance of Internet connectivity and the rise of using mobile phones, the data storage and sharing has reached a high expansion level and became a need for every user [3]. Great examples of cloud-based systems that are already used for a long time are Google Mail, Google Docs, and Yahoo Mail.

Privacy is the basic human right and the cloud service providers (CSPs) should take it in consideration within their policies [9]. Privacy stands for protection and suitable use of user's personal information. Cloud computing is associated with a range of severe and complex privacy issues [13]. For organizations, the privacy includes application of laws, policies and standards by which the Personally Identifiable Information (PII) of individuals is managed. The greatest threat which implies that privacy should be taken into consideration is when the data is collected, stored, processed and shared. The privacy risk is 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 behaviour [9].

The security concern is one of the major hurdles for preventing the adoption of cloud systems. The CSPs enforce data security by using different types of mechanisms such as firewalls and virtualization. These mechanisms do not fully protect against threats of unauthorized data access from outsiders as a result of low transparency [12]. Cloud storage systems deliver novel security and privacy threats which might slowdown the process of its adoption. The biggest challenge for software engineers is to design cloud services which will decrease the security and privacy risks. Furthermore, it is needed improvement on laws that will place geographical and other restrictions on data collection, processing and transferring PII [11]. In situations when users' expectations are not met and their privacy rights are violated, they have the right to sue the companies [10]. Therefore, we attempt to identify users' awareness level about privacy and security regulations for most widely used cloud systems: Google Drive, Dropbox and OneDrive.

PROBLEM STATEMENT

One of the greatest issues that customers have when using cloud-based services is related to users' privacy and security. Regulations of data privacy exist in many countries and are applied when PII is stored and published in the cloud [3]. When sensitive customer's data is moved to the cloud, privacy and security concerns arise. In such situation the uploaded data 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 [4]. To investigate users' awareness, we report findings for a study conducted by gathering data using questionnaires. Although, there were similar studies regarding this topic, such as [5] and [6], none of these studies were considering students and employees as participant groups, and they were not conducted in the Republic of Macedonia. Based on the identified issues, our study investigates users' awareness level about the privacy and security risks of using cloud-based services, such as, Dropbox, Google Drive and OneDrive in the Republic of Macedonia. In the following sections of this paper we present our 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, we conclude the paper with some ideas and directions for future efforts.

LITERATURE REVIEW

Google Drive, Dropbox and OneDrive offer similar services, which are comparable between each other. These systems share almost the same advantages, but also similar issues about privacy and security of data storage such as: data loss, data replication, and unauthorized data delivery to third-party companies [1]. There is an EU-US cooperation on cyber security in order to strengthen the cyber security risk management in energy, transport and finance sectors. Based on the EU-US Summit, held on 26th of March in Brussels, Belgium, the United States and the EU agreed to boost effectiveness of the Mutual Licence Agreement. Their main goal is to provide data protection and enable certainty when data is transferred for commercial purposes [16].

Some of the articles reviewed in paper [1] were focused on explaining the mentioned concepts of security weaknesses, but they did not provide information about user's awareness. One study evaluates enterprise security risks and cloud computing adoption [8], while another study devises security guidelines and best practice recommendations [7]. A study conducted by the Pew Research Center surveyed the privacy concerns' level of American Internet users [5]. 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 will be concerned if the provider gave their files to law enforcement agencies when asked.

In [6] the authors 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 indicated 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.

All these studies, however, fail to reveal to what extent, users are aware of privacy issues, their expectations, and how these concerns would alter their behavior towards online cloud storage services.

METHODOLOGY

Data collection and Procedure

In order to investigate the level of users' awareness about privacy of data in the cloud systems, we have combined qualitative and quantitative data collection methods. Referring to several other articles [5], [6], [14] and [2], which investigated similar issues, we found that the most suitable research method would be an online survey. Therefore, in this study we have chosen to use a questionnaire that was composed of closed- and open-ended questions. The questionnaire was delivered online and included 15 questions; 4 were open-ended while 11 questions were closed-ended questions. Participants were selected based on whether their occupation was a student or an employee at a software company. The chosen participants were contacted through a private message on Facebook and LinkedIn with detailed information about the purpose of this study.

Participants

A total number of 28 participants were included in this study, 14 of them being employees in IT companies, while the rest were Computer Science students; all from Macedonia. Most of the respondents (students and employees) were 20 to 29 years old. Thirteen students and 7 employees were 20-29 years old, while 6 employees and one student were 30-39 years. Only one employee was older than 40.

Data Analysis and Method

The main purpose of this research was to measure the level of users' awareness about privacy and security weaknesses, policies and solutions for cloud-based systems such as Dropbox, Google Drive and OneDrive. The qualitative data collected from open-ended questions was organized and categorized by identifying certain patterns which involved assigning codes to users' responses. The next step involved grouping of answers in categories and the final results were retrieved by using queries. The qualitative data analysis was done using NVivo, while the quantitative data analysis was done using Excel.

RESULTS AND DISCUSSION

In this section, we present the main findings concerning the extent of users' awareness about the proposed cloud privacy and security issues. Users' answers regarding Q5: *"Which cloud systems are you using?"* were grouped in 4 categories; users who use 1, 2, 3 or 4 cloud services. Fig. 1 shows that most of the respondents, 8 (43%) students and 6 (43%) employees use 2 cloud-based systems. Only 2 (14%) employees and 1 (7%) student use 4 cloud systems. These results indicate that both sample groups comparably use few cloud-based systems with Google Drive being the most preferable.

The answers which contribute towards the main goal of this study are linked to questions 9–15 from the questionnaire. Sixty-four percent of employees and 36% of students selected *storage security* as their answers to the multiple choice question *Q10*: "*Which of the following privacy and security weaknesses have you heard of or you know about?".* The least chosen issue was *sharing of trash files*, since none of the employees and only one student (7%) mentioned it. Fig. 2 shows that employees compared to students are more aware about *storage security* issues. On the other hand, students compared to employees are more aware about *lack of control*, *shared environment*, *physical security*, *NonHTTPS shortened URL* and *sharing of trash files*. Additionally, both participant groups are equally aware about *no privacy on sharing* and *unauthorized sharing*. Based on these results, we may conclude in general that students are more aware about privacy and security weaknesses compared to IT employees. This interesting finding, requires further investigation, since our natural expectation was that employees should have more knowledge about privacy and security risks related to cloud systems.

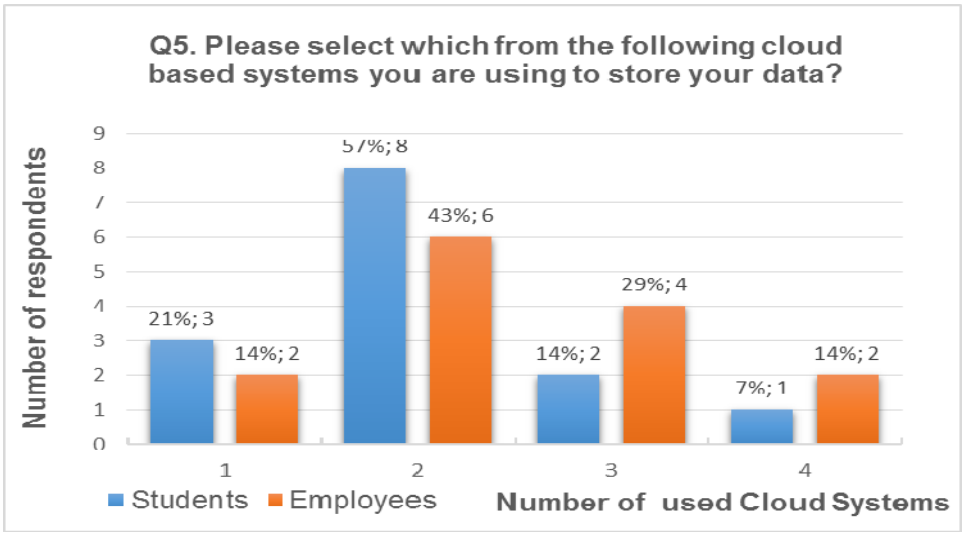

Fig.1. Number of used cloud systems per respondent. The two respondent groups have shown that they use mostly 2 cloud-based systems.

The respondents' answers to Q11: "*Would you be able to explain some of the security and privacy weaknesses that are mentioned above?"*, were grouped in 4 categories: *aware of risk existence*, *define 2 security and privacy issues of using cloud systems*, *wrong answer* and *did not respond*. The results showed that only 2 (14%) employees briefly defined some privacy and security issues and same number of students are aware of the privacy and security risks. These results imply that the employees and students alike do not have satisfactory knowledge about the mentioned issues in Q10, although on average they chose many issues (detailed in Fig. 2).

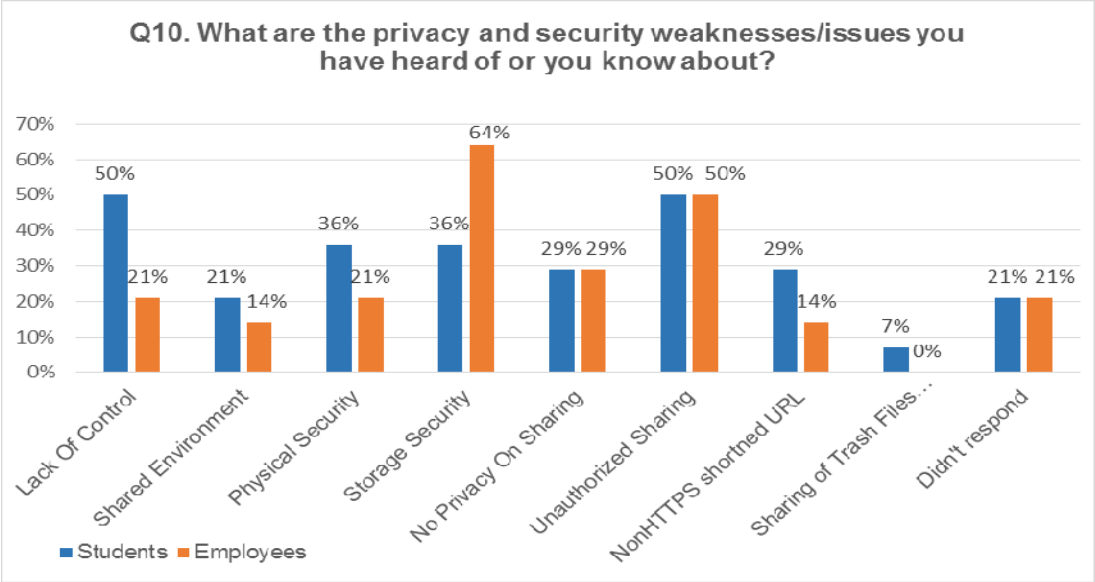

Fig. 2. Students' awareness level about most of the provided cloud privacy and security weaknesses is higher than the employees' awareness level.

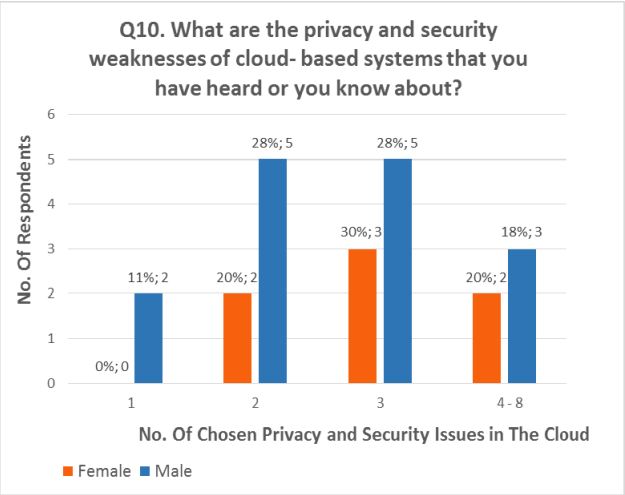

Fig. 3. Males and females have similar knowledge concerning security weaknesses of cloud-based systems.

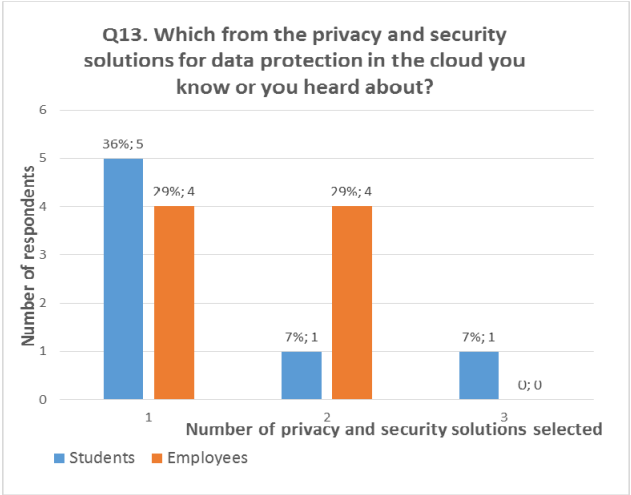

Fig. 4. Number of solutions selected by students and employees.

The answers to Q10 revealed an interesting finding concerning participants' gender. Fig. 3 shows that most of the respondents (28% male and 30% female) recognized three privacy and security issues. Two issues were recognized by 28% of male and 20% of female respondents, while 18% of male and 20% of female respondents recognized more than four issues. These consistent values between males and females indicate that the gender has no effect concerning awareness related to cloud privacy and security issues. Another interesting finding is that only one third of students and employees reported about their knowledge of solutions for data protection in the cloud (Fig. 4.)

All these findings indicate a pattern that to an extent cloud service users are aware of privacy and security issues when storing their data, although they are less aware of solutions related to these issues. Similar results are found in [6], 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. In another study [14], 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.

CONCLUSIONS AND FUTURE WORK

In this paper we explored users' awareness level about security and privacy weaknesses when using cloud-based services. Regardless of cloud systems' popularity, studies show that there are many security weaknesses in the cloud. Concerning this, the results of this study indicate that the cloud system users are aware of existing privacy and security issues, however they lack detailed knowledge about existing solutions to these issues. The online survey used was sent to total number of 50 persons, however, only 28 responded positively, which presents the great limitation of this study.

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.

REFERENCES

[1] Chu, C-K., Zhu, W.-T., Han, J., Liu, J.K., Xu, J., Zhou, J.: Security Concerns. In Popular Cloud Storage Services, IEEE Pervasive Computing (2013)

[2] Danaher. M, Chong. C. J: User Concerns on Cloud Security- A UAE Perspective. In: International Journal of Computer and Information Technology (2014) ,Vol. 03 – Issue 06,p. 1264 - 1267

[3] Guilloteau, S., Mauree, V.: Privacy in Cloud Computing. ITU-T Technology Watch Report, Geneva (2012), p 1-12

[4] Henze, M., Großfengels, M., Koprowski, M., Wehrle, K.: Towards data handling requirements- aware Cloud Computing. In: 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom); vol. 2. (2013) p.266-269

[5] Horrigan, J. B.: Use of cloud computing applications and services. In: Pew Internet & American Life project memo (2008)

[6] Ion, I., Sachdeva, N., Kumaraguru, P., Capkun, S.: Home is Safer than the Cloud!: Privacy Concerns for Consumer Cloud Storage. In: Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburg, PA, USA, ACM (2011), p. 13-1

[7] Jansen, W., & Grance, T.: Guidelines on Security and Privacy. In: Public Cloud Computing, National Institute of Standards and Technology Gaithersburg, MD 20899-8930 (2011)

[8] Joint, A., Baker, E., Eccles, E.: Hey, you, get off of that cloud?. In: Computer Law & Security Review 25(3), Barlow, Lyde & Gilbert LLP. Elsevier Ltd. (2009) 270-274

[9] Pearson, S., Benameur, A.: Privacy, Security and Trust issues in cloud computing. In: Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference. Bristol, UK (2010) p.693-702

[10] Pearson, S., Charlesworth, A.: Accountability as a way forward for privacy protection in the cloud. In: Jaatun MG, Zhao G, Rong C, editors, CloudCom 2009, Beijing Jiaotong University, China. Vol. 5931/2009. Springer. (2009) p.131 - 144

[11] Pearson, S.: Taking Account of Privacy when Designing Cloud Computing Services. In: Proceeding CLOUD '09 Proc. of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, Washington, DC, IEEE Computer Society (2009) 44-52

[12] Shahzada, F.: State of the Art Survey on Cloud Computing Security Challenges, Approaches and Solutions In: The 6th International Symposium on Applications of Ad hoc and Sensor Networks (AASNET'14), aKing Fahd University of Petroleum and Minerals, Dhahran, KSA. Vol. 357 – 362

[13] Svantesson, D., Clarke, R.: Privacy and consumer risks in cloud computing. In: Computer law and security review 26.4 (2010) 391-397

[14] Quah, A. M. Yi: User Awareness and Policy Compliance of Data Privacy in Cloud Computing. In: Proc. of the 1st Australasian Web Conference (AWC 2013), Adelaide, Australia.

[15] Willie, M.:Cloud Computing Service Metrics Description. In: National Institute Of Standards and Technology

[16] Joint Statement, EU-US Summit (March 2014), Brussels, Belgium.

ABOUT THE AUTHORS

Adriana Mijuskovic, Masters student, Contemporary Sciences and Technologies, South East European University, Phone: +38971736226, E-mail: am18316@seeu.edu.mk.

Mexhid Ferati, PhD, Contemporary Sciences and Technologies, South East European University, Phone: +389 44356157, E-mail: m.ferati@seeu.edu.mk.

The paper has been reviewed.