Chapter 44
Cloud Storage Privacy and Security User Awareness: A Comparative Analysis Between Dutch and Macedonian Users

Adriana Mijuskovic
South East European University, Macedonia

Mexhid Ferati
Oslo and Akershus University College of Applied Sciences, 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.

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

DOI: 10.4018/978-1-5225-8897-9.ch044

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

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 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 &

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/cloud-storage-privacy-and-security-user-awareness/228763

Related Content

Instructing AI Ethics and Human Rights
Katharina Millerand Muhammet Demirbilek (2022). *Applied Ethics in a Digital World (pp. 59-72).*
www.irma-international.org/chapter/instructing-ai-ethics-and-human-rights/291431

Wearable Devices: Ethical Challenges and Solutions
Marc L. Resnickand Alina M. Chircu (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 694-712).*
www.irma-international.org/chapter/wearable-devices/228751

Digital Equity: Responding to the Reality of the Digital Divide
Patrick Flanagan (2022). *Applied Ethics in a Digital World (pp. 74-83).*
www.irma-international.org/chapter/digital-equity/291433

Privacy-Preserving Aggregation in the Smart Grid
Georgios Karopoulos, Christoforos Ntantogianand Christos Xenakis (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 1800-1817).*
www.irma-international.org/chapter/privacy-preserving-aggregation-in-the-smart-grid/228810

Factors Influencing Information Security Policy Compliance Behavior
Kwame Simpe Ofori, Hod Anyigba, George Oppong Appiagyei Ampong, Osaretin Kayode Omoregie, Makafui Nyamadiand Eli Fianu (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance (pp. 152-171).*
www.irma-international.org/chapter/factors-influencing-information-security-policy-compliance-behavior/253668