Linnéuniversitetet
Kalmar Växjö

The effect of computer science on the use of cloud storage

Author: Loic_Galland
Supervisor: First_Name Surname
Semester: Autumn 2018
Discipline: XXXX
Course code: 1DV510

Abstract

As the world moves towards a life surrounded by data and computers, data created everyday are rising significantly. Users needs to send their data to onlines storages called cloud storage. In this report, the different type of dangers of storing private information and the different way to limit those risks are presented. The possible threats fall into three catagories: trust, Service availibility and Data Loss. There is also two different ways of limit the risks: encryption and two-factor authentificator. These techniques are essencial to create a safer environment for the user's private information which allow to make the users feel more secured and protected. Further research in this field should be aimed at the creation of new ways protect private data as hackers are finding more and more creative ways to access those.

Keywords

Cloud Storage, Privacy, Cyber Attack, Encryption

Table of Contents

1 Introduction

Since the computer entered our lives and changed our ways of living and working, researchers had to find a way to store our digital data. They created all sort of technology and machines such as hard drives, flash drives, CD-ROMs. However, as the technology improved over the years, scientists were trying to create a way to store our digitals data without using any physicals machines such as hard drives. This is how the cloud storage came to life. The U.S International Data Corporation proclaims that in 2013 4.4 zettabytes (1 zettabyte is equal to 2^{70} bytes) of data have been created so far and that by 2020 around 44 zettabytes of data will be created **[1]**. This is going into an expenontial growth and it does not seems to slow down.

There is five main attributes that charectirize cloud storage according to the U.S. National Institute of Standards and Technology (NIST) **[2]**. Theses main attributes describe a cloud system in a general way. The first attribute is the on-demand self-service feature which allow the users to use the storage capacities and computing performance without the intervention of any human being. The user can store any type of data such as pictures, documents and many more. The second attibute is the broad network access. The users can access their data from almost every devices such as phones, computers, tablets and many more. All the data can also be accessed anywhere in world as long as the user have access to any kind of internet connection. The third attribute is the shared ressources feature. It allows its users to create clouds with multiple persons have access to the account. In addition, users can even share pictures, documents or any type of data to other users by sharing to them. The fourth attribute is the elasticity. It is easy and user-friendly to send data or to receive it. The cloud also have the ability to store a lot of data and give the feeling to the user that the storing capacities are infinite. The user could get this feeling due to the abscence of physical storage. The fifth attribute is the price for the user. Using the cloud storage will save money to the user as they would not have to buy any physical storage such as hard-drives. It will also reduce the amount of space used for storage for the user as data will be stored on servers online.

However, even though cloud storage looks like a promising technology that can appeal to a big number of peoples, a lot of individuals are questioning whether this technology is safe enough to be trusted to keep their personals information. After the cyber-attacks on August 31, 2014 on the iCloud of Apple **[6]** where private pictures from celebrities were leaked on the internet. The hacker responsible for this leak is still unknown. However, it appears that celebrities were targetted and the hacker managed to gain access to the Icloud of the victims from an unknown way. A few days after the attack Apple confirmed that the celebreties' accounts had been hacked. Because of this incident people started to have doubts about the reliability of this technology. A few days after the attack Apple confirmed that the celebreties' accounts had been hacked.

1.1 Aim and Research Questions

The aim of this report is to evaluate if the cloud storage technology is safe enough for user to save their digital personal information online.
To achieve this aim, I will answer to the following questions :

- What are the possible danger of stroring information with cloud storage technology?
- What can the user do to limit the risks?

2 Result

The amount of data created every year have exponentially increase over the last few years. Due to all of this changes it has become harder and harder to protect every single data that is stored on the cloud. This section will show the differents threats of cloud storage and the user can limit those threats.

2.1 Possibles threats to privacy of the cloud storage.

2.1.1 Trust

Trust has an important place in the user life. When users upload their data and private informations on the cloud, they expected that the service will keep their information private. Such trust is hard to aquire, especialy on the internet where do not know for sure who we are talking with or who work for the company that is offering the cloud storage service. According to Nesrine K. and Maryline L. **[3]** the two different place where the trust is needed to limit the risk of exposure would be the company outsourcing certain task to someone else and the multi-tenancy accounts.

2.1.1.1 Outsourcing

Due to the enormous amount of data that is stored on the cloud storage, companies need to outsource certain task to other companies. For example, the company that offer the cloud storage service can use servers from others company to store the data **[4]**. The problem of doing it for the user would be that trusting the company would not be enough. The user need to trust the company's choice to which company they decided to use for outsourcing certain tasks. This implies that there will always be a chance that private data is made public by those outsourcing companies.

2.1.1.2 Multi-tenancy

Another issue of trust on the cloud storage technology could be with the multi-tenancy accounts **[4]**. The cloud in that case is used and shared between multiple users. Therefore, data from different customers might be placed onto the physical machines. One individual which the information is stored on that physical machines could corrupt the machine and therfore get access to all the data that it contains. Companies usualy store the data of multiple customers on the same machines to reduce cost. However, it brings another possible danger for the user to have private data turn public. It does require a lot of knowledge on programming or even how the cloud storage company operates. For instance, which servers are they using and what type of physical machines. Therefore, these types of attacks are less common but are still a possible threat for the privacy of the user.

2.1.2 Service Availability

Another major issues with this technology is the service availability **[5]**. It can appends that sometimes the service is not accessible due to maintenance or ongoing issues. During that time the user cannot access to their private data. If the user really need to get that information quickly but the service is not available, they will have no other choice than wait until it is available again for use.

2.1.3 Data Loss

One of the reason that people are using the cloud storage technology is because they want to keep their data safe and reachable. However, sometimes it can happen that the data get lost or disappear for number of reasons **[4]**.

2.2 How to limit the risks

As seen before, there is a lot of risks that can happen with the cloud storage if the storage account is not protected correctly. In addition, there is also some ways to reduce the risk of getting data leaked on the internet.

2.2.1 Encrypt Everything

Most of the time when a user gets his information leaked it is easier that his/her computer got hacked first or the hacker somehow found out the password **[9]**. To limit the risk of this happening the user encrypts the data on his computer. By encrypting all their data, users will be the only one to have access to their data. If hackers will get the encrypted data, they will not be access the real picture or information that the user protected. Users will need to use a predefined password composed of symbols, letters and number to open their information.

According to APA Practice Organization **[7]** there is three different type of encryption. The first one is the full-disk encryption. It creates a protection of the full system (computer). The user need a password to be able to unlock all his data at once. The computer will ask for the password after turning on the computer. The second type of encryption is called virtual-disk encryption. It creates an encrypted container that acts like a flash-drive. To able to access the “container” the user will need to enter the password previously configured. This add an extra safety from the full-disk encryption and therefore both password should be different to limit the risk of private data becoming public. The third type is the file/folder encryption. It consists of protecting a folder or a file with password so that only the user will be able to get the information inside. Therefore, users could for instance secure Eclipse to protect their programs or even Microsoft Word. When someone will try to open any of the protected application or folders they will need to enter the password that have been previously set.

With the three methods combined, the user limit significantly the risk of someone else accessing their private data. Therefore, if their computer gets stolen or hacked the criminals would not be able to get any personal information without having a lot of knowledge in hacking or programming. The limit the risk even further, the user should use three different strong passwords (including symbols, letters and numbers) for the three different technics of encryption.

2.2.2 Two-Factor Authentication

In certain situation, encrypting all the data is not enough to stop hackers. If they manage to find the password for each encrypting method, then they will have access to everything and will be able to private information from the cloud. Therefore companies like Google created an additional security to protect the cloud or information online. This is called the two-factor authentication **[8]**.

If the user connects from a new device and enter his/her password to log in, they will be asked to enter a token as well. Most often now, users can get the token from a text message on their phones. It is composed of six digits and token will be valid for a short period of time (usually 30 seconds).

Therefore, if the hacker finds the password, they will not be able to access the information on the cloud as they will need to also get the token from the phone of the user. This will reduce the risk significantly as it is harder for hackers to hack someone phone and get the token from the text.

3 Discussion

Every day, enormous amounts of data are being created which force the users to buy more and more physical storage such as hard-disks. However, these technics will take a lot of place and therefore individuals and companies start using service that will store their data online which is called cloud storage.

However, this technology also comes with privacy threats such as trust **[3]**, Service availability **[5]** and Data loss. The user can lose control over the data that he/she stored on the cloud storage. After trusting the company responsible for the cloud storage, the user also need to trust the enterprise’s choice concerning the outsourcing companies they are using. The user might not be available all the time either due to maintenance of the website or even ongoing issues.

To limit those risks the users needs to encrypt his/her data **[9]**. They can either do a full-disk encryption, virtual-disk encryption or even file/folder encryption **[7]**. This will help the user by giving them additional protection for their private data.

The implication of these encryption techniques is that they provide an additional safety for the user to reduce the risk of private data turning public. Therefore, it is harder for hacker to get access to this private information. Although, theses techniques are adding more safety for the privacy of the users, the hackers will get smarter and smarter and therefore new safety measures will need to be created.

4 Conclusion

The aim of this report was to investigate the different danger or threats that users could experience when storing private information on cloud storage. Another aim of this report is to investigate the possible ways of reducing those risk.

Cloud storage is becoming an important part of the concern from the users and therefore a lot more techniques will be created to protect the privacy of its users.

References

[1] – Cyclone Interactive, The Digital Universe of Opportunities: Rich data and the increasing value of the internet of things, IDC, 2014.

[2] - M. Peter and G. Tim, The NIST Definition of Cloud Computing: *Computer Security*, Gaithersburg: NIST, 2011, p. 2.

[3] – K. Nerine and L. Maryline, Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographies Mechanisms: *Computer communication*, Vol. 111. 2017, pp.120-141.

[4]- X. Zhifeng and X. Yang, Security and Privacy in Cloud Computing: Vol.15(2). IEEE Communications Surveys & Tutorials, 2013, pp.843-859.

[5] – M.A Alzain, E. Pardede, B. Soh, J.A. Thom, Cloud Computing Security: *From single to multi-clouds*. Hawaii: Proceedings of the Annual Hawaii International Conference on System Sciences, 2012, pp.5490-5499.

[6] – O. Laurele, "Reminder that privacy does not exist online and legally, there's not much we can do about it", Golden Gate University School of Law, October 2014. [Article]. Available: https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1030&context=ggu_law_review_blog [Accessed: Dec. 11, 2018]

[7] - APA Practice Organization. (2014, Spring/Summer). ABCs and 123s of encryption. Good Practice, Spring/Summer, 10 –18.

[8] – Google, "2-Step Verification", Google. [Online]. Available : https://www.google.com/landing/2step/ . [Accessed: Dec. 11, 2018]

[9] – L. D. Samuel, Emerging Ethical Threats to Client Privacy in Cloud Communication and Data Storage: Vol.46, Iowa: University of Iowa, 2015, page 154-160.