The Future of Cloud Computing and Data Security

Anthony Cong Nguyen, 13

July 7, 2012

ABSTRACT

In the traditional computing model, a user's data is stored on a hard disk drive or USB flash drive that the user carries around with them, and generally, this is the only copy the user has of their data. The cloud offers new and exciting ways that computing in the near future can be improved. However, the great accessibility of this data comes at a cost of extra issues that users must consider, regarding ownership, access, and security of their data. As more and more individuals store more and more different types of private and public information in cloud spaces, new laws and social attitudes toward information will develop naturally; we need to be ethical as we move toward this future.

LIST OF KEYWORDS

Cloud computing, data security, internet technologies, privacy issues, copyright laws, businesses, data backup

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

INTRODUCTION

In the next five to ten years, cloud computing will be one of the big changes in how people view computers and their personal online and offline data. Because internet connections are now faster, and people want to access their files from anywhere, people will move more data into the cloud. Companies such as Dropbox, Apple, and Microsoft, as well as file sharing sites such as MegaUpload or Rapidshare, are holding on to massive amounts of user data. This change will offer people many more ways to collaborate with one another and to share information like never before. However, users now need to be able to trust these tech companies with the data they are storing online. They need to trust that these companies will keep their data safe from deletion, or from being edited without their permission, or shared with unintended individuals. Users need to trust that these companies will behave ethically with their data. They need to know what rights they have as consumers, and they need to be told in plain English before they begin to use these services. These are all potential issues that should be thought about now, rather than later, when it may be too late.

Figure 1 - Rapidshare Logo

WHAT IS CLOUD COMPUTING?

There is no one definition of the term "cloud computing" that is agreed upon by all people, however, for the purposes of this discussion, the NIST (National Institute of Standards and Technology of the U.S. Department of Commerce) definition will be used.

The definition goes: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Three service models of cloud computing within this definition are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [1]. Simply put, cloud computing refers to accessing of powerful computing resources through the internet. Examples of these three models will be presented in this section. Principally, this paper will discuss applications relating to data storage, both for consumers and for larger corporations, but this section will briefly discuss other applications of cloud computing.

Figure 2 - NIST Logo

Several Examples of Business Applications of Cloud Computing

Large businesses have many technology needs that can be met by cloud computing. One of the biggest advantages of using cloud computing is avoiding the costs of purchasing servers and hiring people to maintain them. It does not make sense for a small local business to purchase 5-10 computers that will quickly become obsolete to manage their client data, when they could buy in to a commercial Platform as a Service (PaaS) cloud instead. Oftentimes, these PaaS are run on a pay-per-terabyte pricing plan where you pay for what you use. This would also decrease the number of IT employees needed to manage the system, because there are less physical devices to service. In 2010, Netflix moved their movie streaming service over to Amazon's EC2 cloud, which is an Infrastructure as a Service (IaaS) provider [2]. They have over one petabyte of information stored on Amazon's S3 cloud platform. As of today, Netflix is the largest source of

Figure 3 - Amazon Web Services consists of many different services, including EC2, which powers Netflix

North American internet traffic, 24.87% of all net traffic [3]. This is in part because broadband internet speeds have been increasing, to the point where a user can watch a movie without having to download the entire film beforehand; Netflix offers video streams with data use up to 2.3 GB/hr, and people have the internet speeds to take advantage of it [4]. Netflix has become so confident in its business model, that in 2011 they split their services into three groups of customers, those with streaming only, those with DVD only, and those with access to both; the streaming only group is the largest subscriber group, with 19.1 million users. These statistics show how far two different types of cloud computing penetrates into the lives of the American public.

Home User Application of Data Storage Services

We will examine Software as a Service by looking at Microsoft's SkyDrive offering and Dropbox's offering for data storage. Both SkyDrive and Dropbox allow users to store any kind of files, such as word documents, PowerPoint presentations, pictures, videos, or music, online for access from different physical locations. Instead of carrying around a flash drive with hundreds of different files from different years of work, the same data could be stored online where any device with internet access can access it. Dropbox, which began operating its service in 2008, now has 100 million users. Dropbox also uses Amazon S3 as the means to store user data [5]. When a user signs up for Dropbox, they are provided 2 GB of free online storage, which can be accessed through any web browser, or through client applications running on Windows, Mac, Linux, or other mobile devices. Any device with the client application installed syncs the

Dropbox folder to the device, and all the data from the folder. By having different folders within your online Dropbox, there are quick ways to share files with other people [6]. This can be applied in many ways, for example, to share pictures, or documents that different people are working on in a group, or to deliver information by a method other than email. In addition to those previously mentioned features, SkyDrive also has integrated into it Microsoft's Office Web Apps, which is an example of Software as a Service (SaaS), which allows users to edit Word, Excel, and PowerPoint files in the web browser; the software runs in the browser and is hosted on Microsoft's servers, in the cloud [7].

Figure 4 - Dropbox Logo

BASICS OF INFORMATION SECURITY

What is information security? The term information security means

(1) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
(C) availability, which means ensuring timely and reliable access to and use of information. [8]

It is important to realize that without practicing information security, your data is not safe. Conventional virus infections can sometimes leave people's computers completely useless. Phishing exploits steal passwords from people every day. Many people do not realize the severity of losing a password for a website online; since people use the same password for different services, losing a password to an email account also likely means losing access to

online banking or bill paying services, or allowing someone access to websites that might have your social security number on them. An online password is one of the most important pieces of information a person owns.

Personal Examples

To make a comparison with conventional security, the basics of security include locking house and car when they are not occupied, keeping your wallet with ID and set of keys together at all times, and avoiding places known to be dangerous, especially at night. Likewise, in terms of information security, some basic ideas involve keeping a laptop with sensitive documents locked and secure, perhaps in a briefcase when not in use, or providing personal information such as address or phone number to websites that do not in their privacy policies make clear what the data will be used for. Much like how you would not sign a legal contract without reading through it carefully first, you should not install any software or sign up for a service using personal information without knowing exactly what you are agreeing to. Figure 5 is an example of an external hard disk that has hardware and software based encryption, so that a password is needed to access the data. In addition, it is important to make sure that your operating system and antivirus are fully updated and patched, with the latest security settings that are made to deal with security holes as they are found. When logging into email or other sites requiring password authentication from a public computer, make sure that the browser you are using supports encryption, or it is more likely that the password data may be intercepted during the submission, and of course, log out when done. Any suspicious websites that are not known to be reputable

Figure 5 - Hard Disk with Encryption Technology

are likely to have viruses or other means for hackers to try and log into your personal accounts, and so must be avoided at all costs. However, these are all just the basics that each person should observe. Security is never perfect, so any preventative measures taken help contribute to being more secure.

Business Examples

A small business that is not in the cloud, such as a local movie rental shop, might still have 15 or 20 computers that store lots of information related to cataloging, storing, and renting out movies. While it will not jeopardize national security if this information is hacked into, it is still important to implement good practices for security here. Business must backup their data regularly. Home users should be in this practice as well, but if businesses do

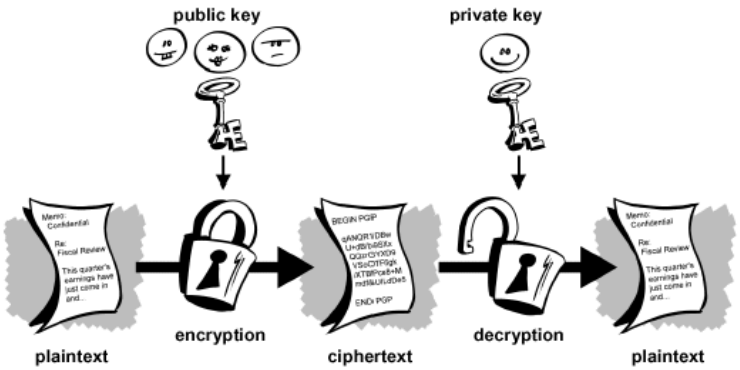

Figure 6 - Public/Private Key Encryption

not, they stand to lose lots of money if their systems fail and they lose both information and uptime. This in turn would lead to a drop in customer confidence; customers cannot pay for services that are not available. For businesses that are working live, not only are backups necessary, but these businesses need a seamless way to transition from operating on the working environment to the backup. For businesses that are working with more valuable data, encryption technology is a must. There are many different types of encryption technology available, and since hackers are constantly at work at breaking crypts, up to date standards of encryption must be used. Businesses must consider these issues as they do any kind of data management.

ETHICAL CONCERNS ABOUT HOW DATA SECURITY AND INTEGRITY AFFECT THE CLOUD

If we, as individuals and businesses, are to store our data to not be stored on machines we own ourselves, but instead on computers owned by big corporations such as Amazon, Microsoft, or Google, we need to be able to trust that these companies that they will keep our data private, and safe from data loss. According to Lori M. Kaufman of BAE Systems, some minimum capabilities that are needed to satisfy confidentiality, integrity, and availability are:

- A tested environment schema to ensure that the shared storage environment safeguards all data
- Stringent access controls to prevent unauthorized access to the data
- Scheduled data backup and safe storage of the backup media [8]

Kaufman's points bring up legal concerns that are not immediately obvious. For example, if you store your bank account username and password onto Dropbox, and the information gets stolen, is Dropbox fully responsible? Does Amazon share some of the blame, because the data is stored via their S3 service? Furthermore, while services such as Dropbox, SkyDrive, and Google Drive sync a copy of the user's data to the cloud while keeping a copy on the local machine, other services do not. And for websites such as Reddit and Foresquare that depend fully on cloud companies powering them, outages can be horrendous. Very recently, Amazon had server downtime in the U.S. East region of service, which was caused by power problems and other bugs [9]. According to a report from a 2009 IEEE conference, cloud

Figure 7 - IEEE Logo

vendors need to have stronger service level agreements (SLAs) that specify many details about their service, including: Definition of Services, Performance Management, Problem Management, Customer Duties and Responsibilities, Warranties and Remedies, Security, Disaster Recovery and Business Continuity, and Termination [10]. This report also lists many different considerations that customers should ask before engaging in cloud usage; the report is more applicable for businesses, but there are also considerations that individuals who are using cloud data storage should consider. For instance, how secure is the encryption scheme being used, and can all of my data be fully encrypted? What happens in the event of a natural disaster, or the company going bankrupt? What protections are underway to make sure my files are not being altered in transmission [10]? If companies do not provide a minimum effort toward these issues, when they are providing a service where so much is at risk, they cannot be said to be acting ethically.

CONCLUSION

The future of computing is the cloud, and we must be careful that we do not take it lightly. Even right now, clouds such as Amazon Web Services are powering huge amounts of the internet, including but not limited to Netflix's online film streaming services, as well as powering the data storage behind Dropbox, which now has over 50 million users. We should make sure that we think through security as we use our computers online and offline. As we begin to store more and more data online, in the cloud, we must also take the necessary extra steps that come with the cloud, in order to ensure our data security.

BIBLIOGRAPHY

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Gaithersburg, 2011.

[2] "Netflix Selects Amazon Web Services to Power Mission-Critical Technology Infrastructure," 7 May 2010. [Online]. Available: http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1423977&highlight=. [Accessed 5 July 2012].

[3] "Global Internet Phenomena Spotlight Netflix Rising," Sandvine Incorporated, Waterloo, 2011.

[4] "Netflix - TV Shows & Movies. How Does it work?," Netflix, [Online]. Available: https://signup.netflix.com/HowItWorks. [Accessed 5 July 2012].

[5] "Dropbox - Where does Dropbox store everyone's data?," Dropbox, [Online]. Available: https://www.dropbox.com/help/7/en. [Accessed 5 July 2012].

[6] "Dropbox - Features - Simplify your Life," Dropbox, [Online]. Available: https://www.dropbox.com/features/. [Accessed 5 July 2012].

[7] "Office Web Apps," Microsoft, [Online]. Available: http://office.microsoft.com/en-us/web-apps/. [Accessed 5 July 2012].

ABOUT THE AUTHOR

Figure 8 - Anthony Nguyen

Anthony Nguyen is a 3rd Year Electrical Engineering student at the University of California, Los Angeles. He works part-time at the Bruin Online office as a Student Tech Consultant and in his free time participates in the Vietnamese Student Union's annual Vietnamese Culture Night as part of the traditional dance group. He is planning to graduate with his B.S. in June 2014 and pursue his M.S. immediately afterwards.

POWERPOINT SLIDES

Cloud Computing and Data Security for Personal Use

Anthony Nguyen, 13
07/05/2012

Table of Contents

- What is Cloud Computing?
- Data Storage Use Scenarios
- What is Data Security?
- Data Security vs. Traditional Security
- How does the cloud affect Information Security?
- Copyright Issues

What is cloud computing?

- Cloud computing refers to many different technologies that enable users to access different kinds of resources through the internet
- Examples of Data Storage in the cloud include Dropbox, SkyDrive, Google Drive
- Other cloud applications include Netflix, Hotmail/Gmail/Yahoo Mail, or Amazon EC2
- Due to time constraints, we will discuss only Data Storage applications of the cloud

Data Storage Use Scenarios

Use Scenarios continued

- Comparison of pricing and platform support between the different data storage competitors

Dropbox SkyDrive Google Drive

- Potential issues that may arise from storing data online compared to storing the data offline

What is Data Security?

- Data Security encompasses many different practices and technologies that users should employ to keep their personal data from being tampered with, stolen, or lost

Data Security vs. Traditional Security

Lock computer/phone when not idle	Lock house or car before leaving
Don't let emails pile up when on vacation	Don't let mail pile up while on vacation
Avoid suspicious websites and use good judgment, esp. when tired	Avoid areas known for gang violence or crime, esp. at night
Don't agree to software agreements without reading them	Don't sign contracts without reading them
Employ encryption schemea for sensitive data, such as banking passwords or credit card information	
Perform routine backups of all non-disposable data, and backup more often for more critical, changing data	

How does the cloud affect conventional information security?

- Issues that arise from the physical location of stored data
- Issues of Data Ownership Legality

Copyright Issues

FBI WARNING

Federal Law provides severe civil and criminal penalties for the unauthorized reproduction, distribution or exhibition of copyrighted motion pictures, video tapes, DVDs or video discs. Criminal copyright infringement is investigated by the FBI and may constitute a felony with a maximum penalty of up to five years in prison and/or a $250,000 fine.

DO NOT COPY THIS TAPE!

Summary

- The cloud as a means of data storage offers much more flexibility to users who want to access their data anywhere, anytime they have internet
- That said, there are concerns that must be taken into account as people begin to use these new technologies, to keep their data secure

READABILITY