Cloud Computing

Security Practices for General User

The cloud is composed of an extensive bulk of computers owned by a third-party in remote location(s). The Internet provides a bridge between personal data and the cloud, enabling users to upload, download and modify data from any device and anywhere. People or companies can rent data storage or processing power from the cloud when needed, and then "return" it when no longer needed. This greatly reduces investments in large hard drives, or time spent deleting old data folders to make space for new data. Soon, there will be no need for frequent use of physical storage devices such as USB thumb drives to exchange data.

Most cloud service providers offer computer applications as alternatives for large amounts of software. This can reduce the budget for software licenses given that a cloud service provider offers the applications for a fixed fee, enabling everyone in an office to have access to many applications, all in one portal.

Through the cloud, sharing and collaborating with others on a project is seamless and easy. For example, a Power Point presentation for class could be simultaneously worked on by several group members. Students can share and modify study guides from anywhere in the world. Plus, giants like Amazon, Google, and Microsoft are fighting for a piece of this pie –which technically means they are fighting over who owns most of the Internet- making the cloud accessible for anyone's budget (price battle lowers the price). Most clouds even offer enough free space for personal data, including recurring backups -- all free of charge.

Examples of Popular Cloud Service Providers

Dropbox offers free 2GB storage space. Users can upload files via their software client or over web interface. It has 256-bit AES encryption and two-step verification security features. Also, it provides business plan for companies who need sharing files over the Dropbox.

Similar to Dropbox, Box offers free space up to 10GB as basic plan. Users can upload files via the software client or web interface. Business users can consider paying the monthly fee for unlimited storage depending on their business needs.

Google Drive not only provides storage to users but also online applications such as Google Doc. User can edit their online files without the pre-installing any software on their computers. 15GB free basic storage is offered to new registered users. For users with Android phone, Google offers additional free storage space. It also provides mobile phone data backup solution which can be accessed anywhere anytime using the Internet.

While iOS devices such as iPad, iPhone, iPod and Macintosh computers are getting more popular, iCloud from Apple offers a basic plan of 5GB free storage space. Even for users who do not have any Apple devices, they can just register for an Apple ID to enjoy this free service. The main feature of Apple iCloud is mainly for the consistency of files and configuration settings across all Apple devices. For example, once user creates or updates schedule over their Calendars of iCloud, all devices using the same Apple ID will be updated when connected to the Internet.

Similar to Apple, Microsoft offers 15GB free storage spaces through OneDrive. Users can even get 3GB more when activating the camera roll backup from Microsoft devices. However, different with Google Drive, if a user would like to edit files directly from OneDrive, the user would need to pay Office365 in advance. Microsoft also has special plans for users to get unlimited storage space[1].

Microsoft locks paid OneDrive accounts – monitor behavior and content
22nd April 2014

Microsoft locks out paid users from their OneDrive account and denies access to their files for 24 hours. Users are complaining on the Microsoft forums about receiving messages that their account is temporarily blocked. Accounts are blocked for various reasons, including what Microsoft calls 'suspicious activity', 'large volume of traffic' or violations of the Microsoft services agreement or code of conduct.

Users are presented with the following message when they try to login to their account.[2]

Amazon Web Services (AWS) not only offers storage capacity but also the following cloud applications which are useful for business applications:

- AWS Trust Advisor
- Amazon Mobile Analytics
- Amazon Cognito
- Amazon DynamoDB and more…

The first registered user can enjoy 12-month of free tier access to AWS cloud services.

Free storage space is definitely the commercial way of attracting new users to register for cloud services. Different cloud service providers offer similar plans by providing cloud storage and related services. Nowadays, smartphone registration is another good avenue for users to increase their cloud space without extra pay.

Benefits Using Cloud

The usage of cloud becomes popular for many good reasons. Notwithstanding the frequently use case of sharing bulk data which email system imposes size limitation, the following are other advantages of using cloud services:

- **Elasticity of Resources**

Where workload and capacity of IT systems cannot be easily predicted, cloud is a suitable platform that more computing computer can be acquired or de-provisioned dynamically according to the business and resource requirements

- **Data access from anywhere**

Data is not no longer restricted on a personal computer or confined within an internal network. It can be made available and shared with many others simultaneously, whenever there is Internet access.

- **Cost Saving**

The "pay-as-you-go" and "one-time-payment" models make the cloud accessible without purchasing powerful computer systems with expensive storage space. Likewise, users can pay at his or her discretion to use "more" virtual drives, memory and CPUs when needed and "return" it when it is not necessary.

- **Quick Deployment**

Once the cloud service is chosen and paid for, it only takes a couple of minutes to implement. On the contrary, in-house servers can take weeks or months for proper installation (getting OS and software license and patching, setting up firewalls, authentication programs and backup systems).

- **Software Usage**

The installation, license and update of software become the responsibility of cloud service provider. Moreover, the usage of software can be accessed by any devices with Internet access.

- **Data Backup**

Data backup is no longer a hassle to users. It becomes part of the chores performed by the cloud service provider. Users are however recommended to create one more backup copy to local drive for contingency purpose.

- **Security system**

The security system of cloud service providers is probably better than what an average individual or a small to medium company can build. Nevertheless, users

iCloud Data Breach: Hacking And Celebrity Photos
2nd September 2014

A group posted a proof of concept script on the popular code repository called Github that would allow for a user to attempt to breach iCloud and access a user account. This script would query iCloud services via the "Find My iPhone" API to guess username and password combinations. The problem here was that apparently Apple AAPL +2.94% was not limiting the number of queries. This allowed for attackers to have numerous chances to guess password combinations without the fear of being locked out.[3]

should take note the potential security concerns and follow the recommended practices as described later in this newsletter.

- **Team Collaboration**

Team work becomes more convenient as group papers, conferences and presentations can be worked on simultaneously by different team of students or staff.

Security Concerns & Recommended Practices

Before diving into "the next big thing", users should be aware of the security concerns when using cloud. The upmost concern is that when data is uploaded to the cloud, it is "shared" with a third-party, which is the cloud service provider you have entrusted with your data. What if the service provider corrupts the data due to technological errors? What if the service provider goes out of business? What if the service provider releases access of data to law enforcement for national security reasons? What if hackers break into the service provider storage area? All these concerns are beyond user's control.

The counterargument to this disadvantage is that cloud service providers live and die by their reputation, thus, they have state of the art security systems; systems that small companies or households would probably never be able to afford.

The following are other security concerns and recommended practices when using the cloud:

- **Possible Downtime**

Without Internet access, it is impossible to access cloud service and data. In addition, when cloud service providers schedule maintenance, or unfortunately suffer from server outages or service attack that cause service interruption, users will not be able to access the cloud services. The global service outage of Microsoft Azure on 19th August 2014 is a good example[4].

Data backup to local drives is still an important practice for users utilizing cloud services.

- **No Sensitive Data**

If you, your classmates and/or co-workers use online e-mail, online photo albums (Flicker) or music services (Pandora and Spotify), you are already using the cloud.

For really personal or sensitive data, think twice before uploading to the cloud. There was already a notorious data breach incident about celebrity nude photos on iCloud.

From a risk management perspective, you should ask yourselves what kind of data cannot be afforded to be compromised in the worst scenario. Prudent decisions should then be made not to store such data in the cloud.

If there is a need to use the cloud to store personal and sensitive data, add your own layer of encryption to the data before uploading to the cloud, and ensure that you own your own encryption key.

Cloud Common Usage:

People are usually uploading data not only to one specific cloud platform but also to others. For example, files kept at Dropbox which are most frequently used can be backed up to Google Drive. Also, data and configurations of smartphone devices could be backed up to the cloud, such as iPhone to iCloud.

Survey Stats at a Glance
26th August 2014

- *66% of respondents said their organization's use of cloud resources diminishes its ability to protect confidential or sensitive information.*
- *62% said they believed the cloud services in use by their organizations are not thoroughly vetted for security before being used.*
- *71% said they would not receive immediate notifications involving the loss or theft of customer data.*
- *51% said on-premises IT is equally or less secure than cloud-based services.*
- *55% responded that they don't believe their IT leader is responsible for ensuring their information is secure.*[5]

- **Prone to Attack**

Having centers full of private or sensitive data is appealing to hackers; thus, hacking attacks could be fairly common. Poor design and implementation of security by the cloud service providers can easily result in data breach incidents.

Check carefully what security features are implemented by the cloud service providers. Examine what data encryption is used on the cloud platform, how data is protected during uploading and downloading, and the authentication channel. Choose cloud service providers with reputable name with no precedence of security incidents.

- **Software Features**

For Universities' usage, administrators should make sure that cloud members can be easily added and deleted depending on the academic year.

Also, check carefully the correct package of cloud applications with the intended features before paying for usage. Sometimes cloud applications may miss some features which would be otherwise available when buying the software separately.

Tips for Students and Staff

In corporate environment, users are normally governed by corporate IT security policy and the computing devices are typically standardized with hardened security configurations.

But in Universities, students and staff are allowed to use own computing devices. And security governance is more relaxed compared to corporate environment.

A lot of the attacks these days are targeting end users. Once a user's computer is compromised, the data stored in the cloud can be subsequently retrieved by the hacker. So University students and staff are advised to develop the following good computing habits when using the cloud:

- Exercise safe browsing habits - if a web site looks shady, it usually is shady. Don't further click on links or downloads;
- Use devices that you trust to connect to the cloud, i.e. minimize the use of public computers which do not fulfil the security standard;
- Enable and use two-factor authentication if available from cloud service providers;
- Choose different passwords and credentials for University IT systems and public cloud services;
- Change passwords regularly;
- Log off sessions when finished;
- Don't open or click on links in strange or unsolicited e-mail;
- Install anti-malware software on computing devices.

The Hong Kong Government has created a web site to educate the public about cloud usage, useful tips and checklists regarding cloud usage can be found from http://www.infocloud.gov.hk/.

The Importance of Safe Passwords[6]

Regardless if data is stored in-house or in the cloud, it is important that passwords for different sites should be kept different and securely protected. This way, if anything is ever compromised, hackers will not have access to other accounts using the same password. Likewise, it is a good practice to change the cloud access passwords regularly.

References

1. "OneDrive now with unlimited storage for Office 365 subscribers." 27 October 2014. Web. 11 November 2014
2. "MYCE News" 22 April 2014. Web. 29 Sept 2014
3. "Forbes" 2 September 2014. Web. 29 Sept 2014
4. "Microsoft Cloud Service Azure Experienced Global Outage" 19 August 2014. Web. 11 November 2014
5. "Government Technology – Data Breaches in the Cloud: Who's Responsible?" 26 August 2014. Web. 29 Sept 2014
6. "Your Dropbox Account May Have Been Hacked (UPDATE: Dropbox Says No)" 14 October 2014. Web. 16 Oct 2014

Copyright Statement

All material in this document is, unless otherwise stated, the property of the Joint Universities Computer Centre ("JUCC"). Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.

A single copy of the materials available through this document may be made, solely for personal, non-commercial use. Individuals must preserve any copyright or other notices contained in or associated with them. Users may not distribute such copies to others, whether or not in electronic form, whether or not for a charge or other consideration, without prior written consent of the copyright holder of the materials. Contact information for requests for permission to reproduce or distribute materials available through this document are listed below:

copyright@jucc.edu.hk
Joint Universities Computer Centre Limited (JUCC)
c/o Information Technology Services
The University of Hong Kong
Pokfulam Road, Hong Kong