Accessing Permanently Deleted Data on the Cloud

ROHAN GUPTE

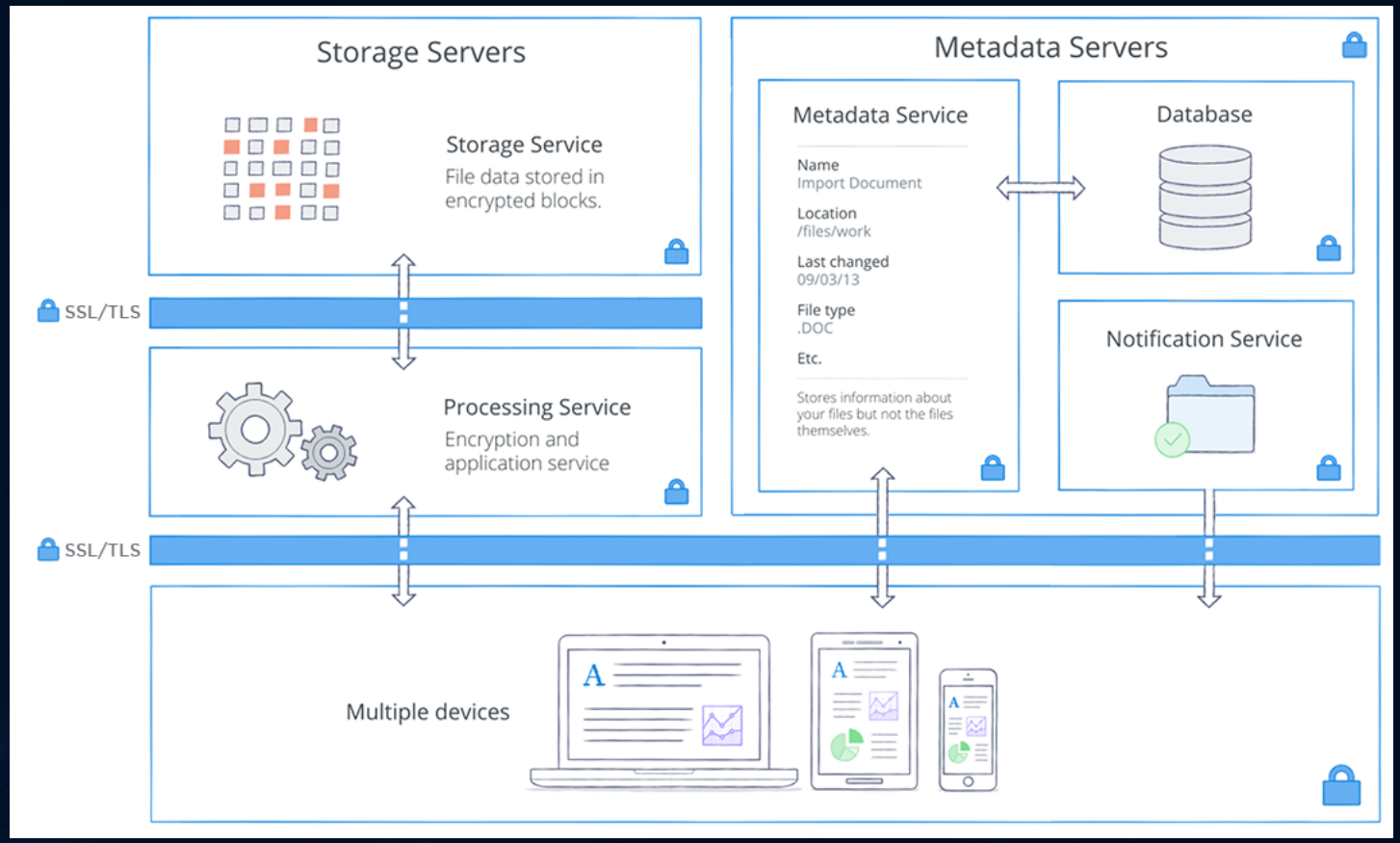
What is Cloud Computing

- Information stored with an external service
- The external service has a multitude of servers on which they store the users information
- Allows for ubiquitous access of information

Cloud Storage Security

- File data is broken up into blocks
- Each block is encrypted and stores in different servers
- Advanced Encryption Standard (AES) is the most commonly used encryption protocol
- When accessing cloud information on local machine, the cloud transfers information using SSL/TLS protocol

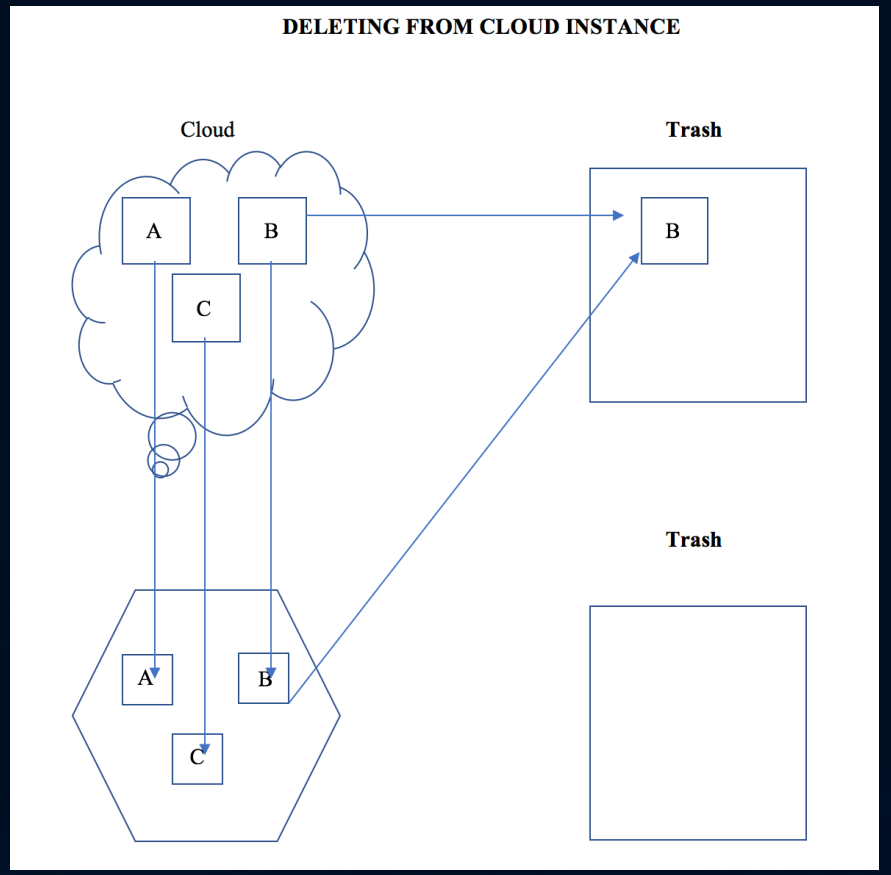
Encryption Process



Deleting Files on the Cloud

- When a files is deleted from the cloud it is placed in the trashcan
- The file will stay in the trash for a certain amount of time depending on the cloud computing service
- The file will be permanently deleted after the allotted time has expired or if the user manually permanently deletes the file.
- There are two different methods of deleting information from the cloud

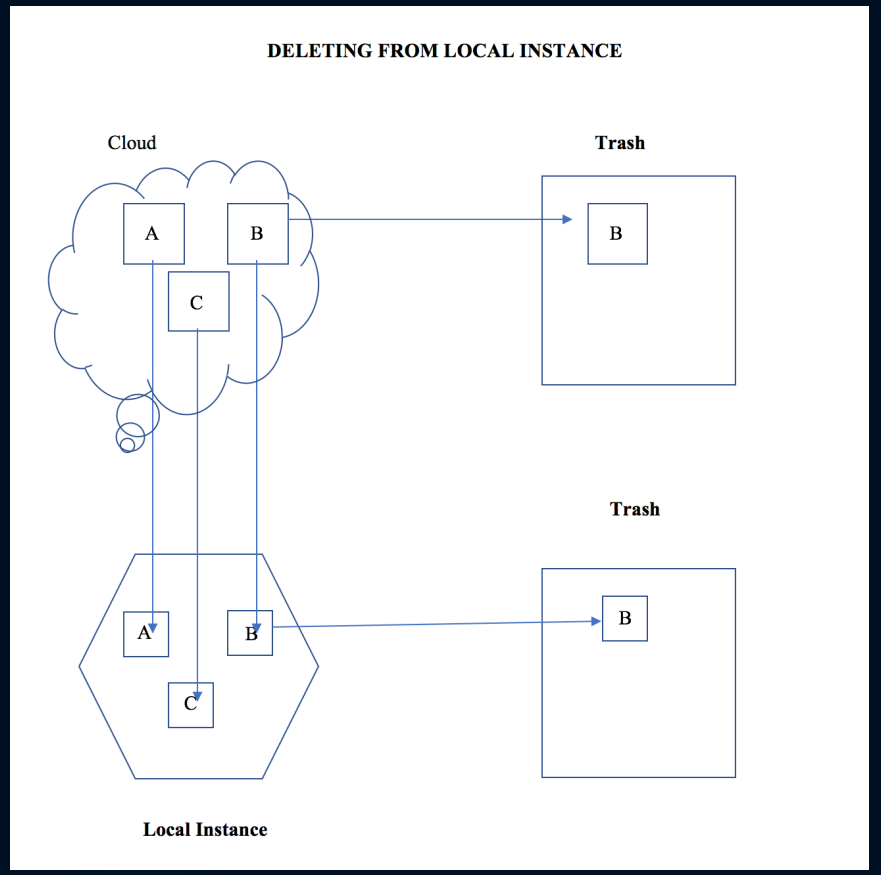
Deleting Files From the Cloud via the Cloud Service



Deleting Files From the Cloud via the Cloud Service (Cont)

- Files which are deleted form the cloud service side only end up in the trashcan of the cloud service
- No file in trashcan of local instance

Deleting Files from the Cloud via Local Machine



Deleting Files from the Cloud via Local Machine (Cont)

- When a file is deleted from the local machine, that file is placed in both the trashcan of the local machine and the cloud server
- The user must permanently delete the files from both the local machine

What happens to the Permanently Deleted Data on the Cloud

- When the data is deleted on the cloud , the service provider keeps the data for a few days on their servers.
  - The files are kept on a very secure server, with heavy security protocols

What happens to the Permanently Deleted Data on the Local Machine

- The file is still on the machine, but hidden
  - The bytes which the file was written on still exist until other data overwrites those bytes

Data Backups – Friend?

- Cloud companies keep a back up of the users information on their servers
- In many cases Backups are helpful as they can have information that you may have accidently deleted and need back

Or Foe????

- Backups can also be accessed by hackers if the user does not take the proper security measures
- Many incidents have occurred with leaked information from users' cloud accounts

How Information on the Cloud is leaked

- Most time users do not have secure enough passwords for their cloud accounts, thus hackers can easily access their account
- Also users' are not aware that their information was not permanently deleted
  - Usually the data is in the trashcan which the hacker can restore and obtain the information

Apple iCloud leaks

- Many users' are not aware that Apple stores the last 3 backups on their servers
- This was brought to light as many celebrities' personal iCloud accounts were hacked into
  - Users thought they deleted their photos, but only one back up had been completed
  - Hackers were able to search through multiple backups and find sensitive photos

Dropbox Mishap

- In 2017, a bug in the Dropbox code let deleted files appear back in the users accounts
- Some of these files were believed to have been deleted almost 6 years ago
- Could have been very dangerous is a user's account had been compromised

How can our information be better protected

- Information Security is a two-way street
- Both the Cloud Computing services and users have a responsibility to use most effective security measures

Cloud Computing Company's Duty

- They have a duty to provide the safest and most secure data storage platform
  - Storing valuable information of millions of individuals
- Ensure that if a bug occurs to quickly find a patch for it
  - Such as the Dropbox bug

User's Duty: Research

- Must ensure that they do research on the cloud computing company they wish to use
- Understand how Cloud Computing Companies store information and if they encrypt their information
- Understand how often backups are uploaded and how many backups are kept by the company
- Understand what happens to the data when it is deleted

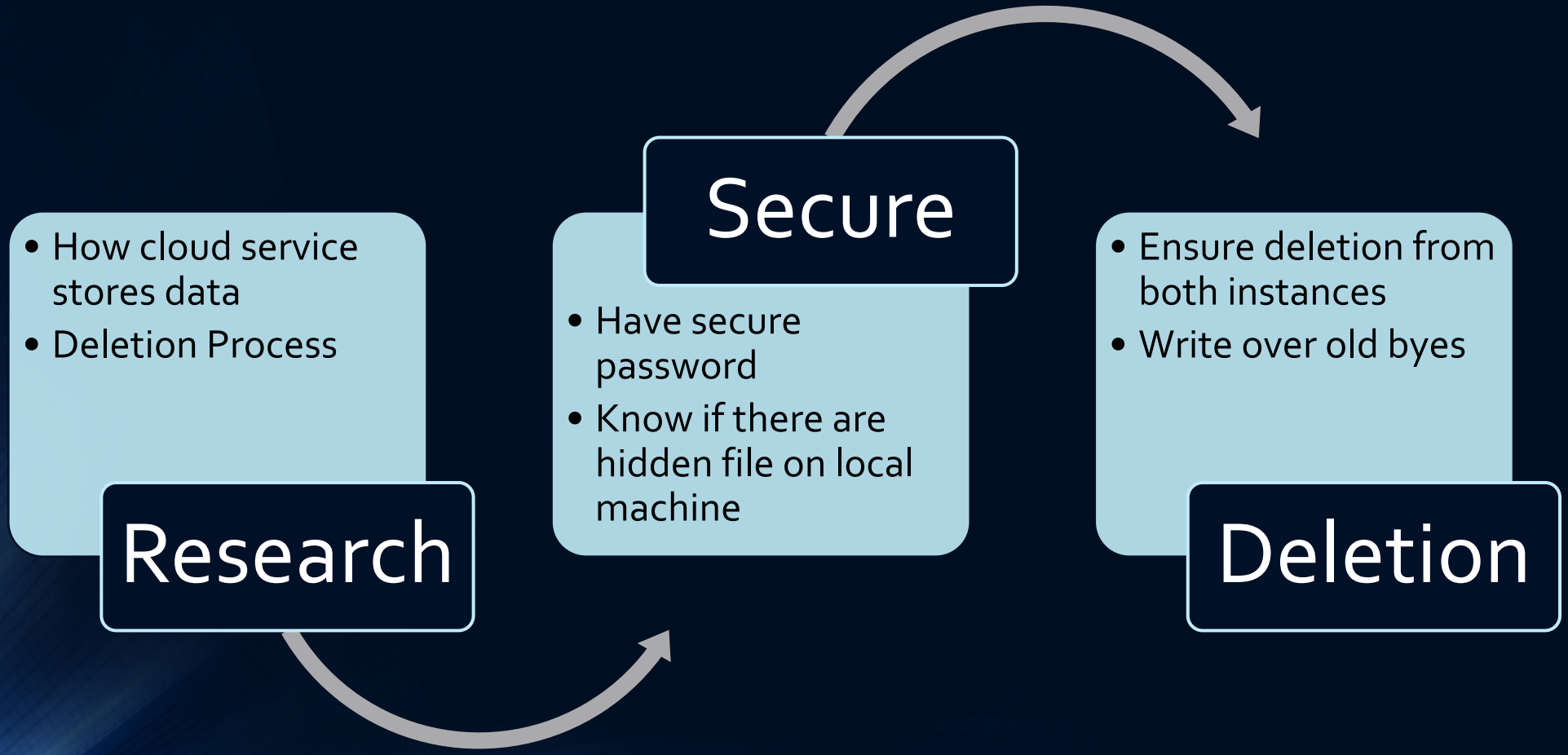
User's Duty: Proper Security Measures

- Ensure a strong and not easily guessable password
- If deleting from the local instance, permanently delete from both the cloud service and local machine
  - Use software to write over the bytes on which your permanently deleted data was previously on
    - If your local machine is accessed, hackers can not find these files

Finding Hidden Files

- In many cases files that have been deleted and are hidden can be found using the command on mac os:
  - defaults write com.apple.finder AppleShowAllFiles -boolean true ; killall Finder
- Cloud Companies such as Dropbox keep a hidden folder of cached files on the users local machine.
  - Can be found with the command above and be permanently deleted

Title and Content Layout with SmartArt




Thank
you!!