Legal & Ethical Issues of Cloud Storage

M.Cromie, F.Leishman, E.Malinovskis, A.McDonald & M.Paterson

School of Computing Science, University of Glasgow

Introduction

...

Figure 1: A simple diagram illustrating the basic concepts of cloud storage

Leaks

- Cloud storage leaks are becoming increasingly common.
- But who's fault is it when data is stolen? The user or the storage company?
- A recent example would be the iCloud photo hack resulting in private pictures of celebrities being stolen. This was made possible by a combination of weak passwords and security vulnerabilities of iCloud being exploited.
- Ethical issues could be raised when users believed that their iCloud accounts were secure, despite security vulnarablities of iCloud this data was leaked.
- Another ethical issue with this is that some users were unaware that their data was uploaded on the cloud, with automatic backups enabled without their explicit permission.

Sharing Data

- What is to stop employees from accessing, reading, sharing or selling user data?
- This is a very difficult issue, with a fine line between what is acceptable to be used by the storage company.
- An example of this is one of Dropbox's terms that they have full access to all data uploaded to their service, allowing them full ownership.
- This raises severe ethical concerns, with users questioning the reasons behind this policy.
- The new revision of the General Data Protection Regulation aims to help the protection of private data, in order to stop this happening.
- This will be aimed at targetting cloud storage companies, as the law will enforce strict controls on personal data; harsher security requirements and even harsher penalties for companies that breach these laws.

Backup

- Backups are made regularly by the storage company to prevent loss of user data.
- These back ups are usually stored off site, to keep data safe.
- Users have little or no control over access to the backup data (both remote and physical).
- Backup service provided is often "Best effort" and the providers do not take over any liability associated with data loss or misplacement.
- This raises potential ethical issues, with the user trusting the storage company to make regular incremental back ups and the company failing to do so.
- This is often signed into a contract, which users should research before selecting a provider.

Encryption

- Data stored on the cloud is not as secure as many people believe.
- As a solution encryption shouldbe utilised to further protect the information.
- However, encryption is not without its flaws. Who encrypts the data? Who has access to the keys?
- Some storage companies provide services for users to encrpyt the data but the companies will retain access of the keys[1].
- This is a critical issue for businesses storing customer data on the cloud, as they could be violating the Data Protection Act should they be enabling unauthorised people to view potentially sensitive information.

Conclusion

- In conclusion, we have shown there are a great deal of legal and ethical issues associated with storing data on the cloud.

References

[1] Wenjin Hu, Tao Yang, and Jeanna N Matthews. The good, the bad and the ugly of consumer cloud storage.

ACM SIGOPS Operating Systems Review, 44(3):110–115, 2010.