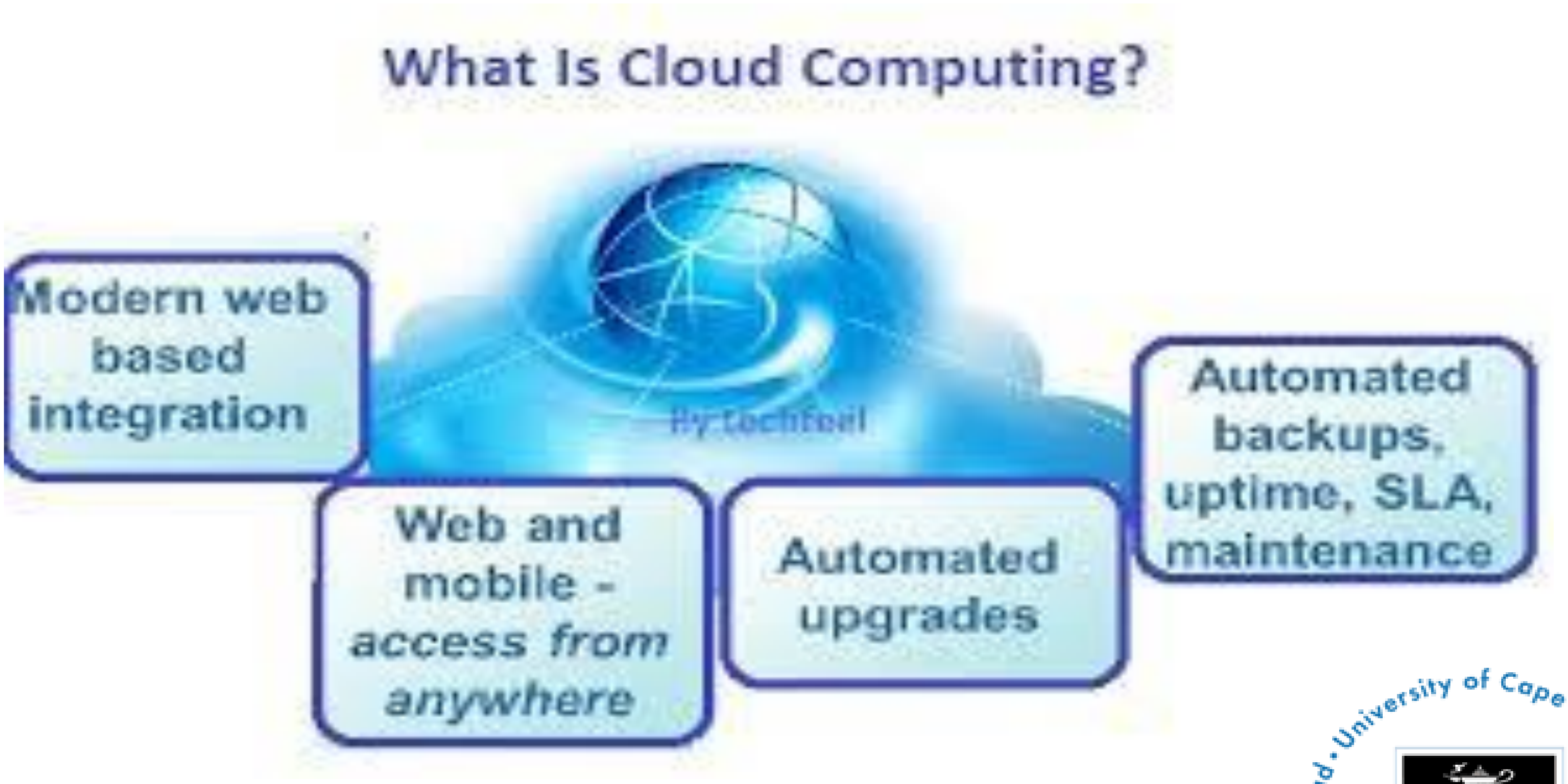
Security challenges with cloud storage

JOEL CHIGADA

University of Cape Town

Cloud computing



What Is Cloud Computing?

Modern web based integration

Web and mobile - *access from anywhere*

Automated upgrades

Automated backups, uptime, SLA, maintenance

Outline

- Introduction
- Objectives of study
- Defining cloud computing
- Types of cloud storage
- Security challenges in cloud storage
- Methodology
- Findings
- Recommendations
- Conclusion
- References

Introduction

OrganisationsOrganisations of all types operate in an increasingly dynamic global village characterised by rapid technological developments and innovation in information communication technology (ICT). The major ICT developments have given birth to cloud computing technologies which have attracted a great deal of attention from many quarters Including authors, consultants, technology analysts and companies. Organisations that take advantage of the dynamism in ICT developments are able to create new products and business models, thus remaining relevant and competitive in the market. Though cloud computing offers attractive economic and flexible solutions to businesses, the issues of security in cloud storage is a major cause for concern. Security in cloud storage is no doubt one of the critical issues that face organisations dealing with vast amounts of data and information that should be stored. Security on cloud storage has to deal with data leakage; cloud credentials; snooping; key management and performance. Organisations are therefore likely to adopt a careful approach to cloud computing storage.

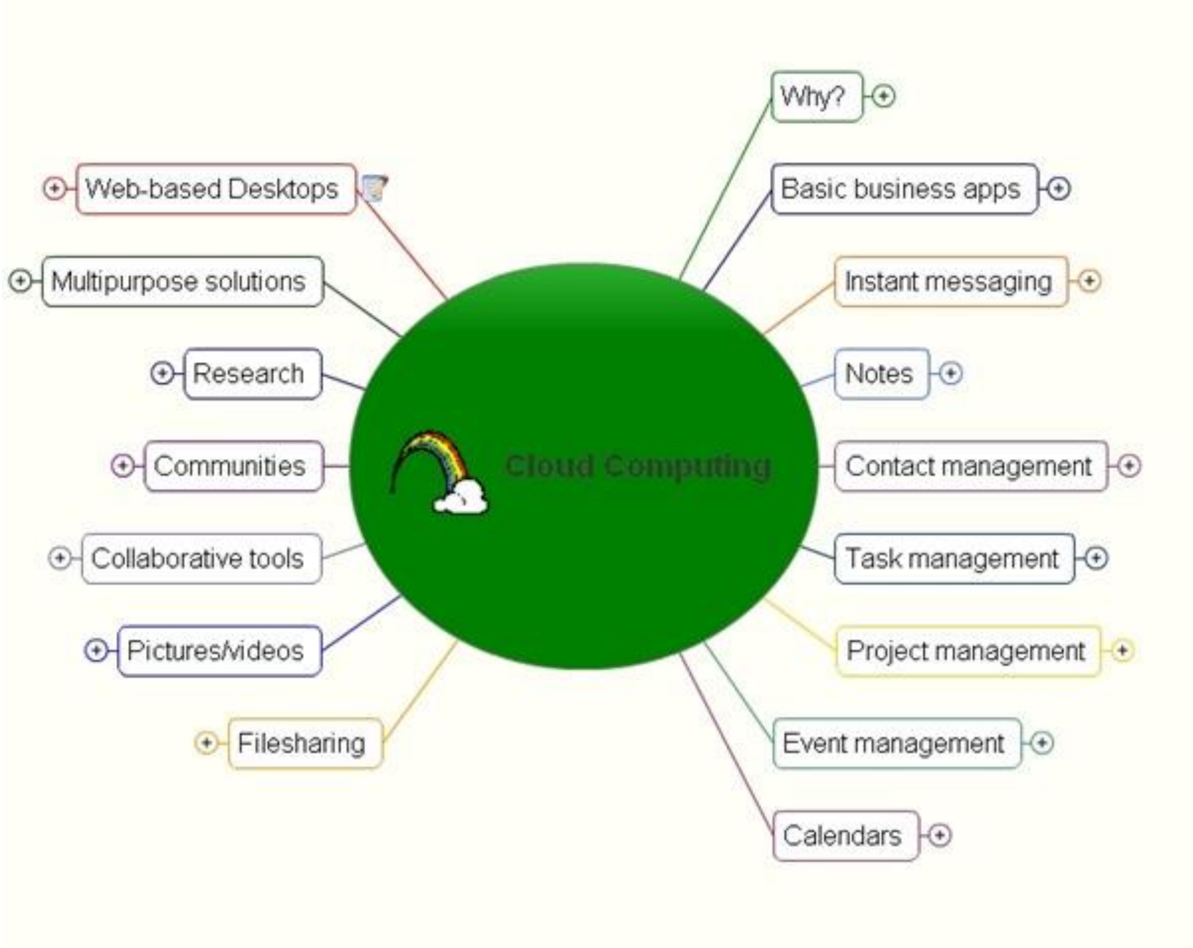
Objective of study

- To establish the type of cloud storage in use at UNISA; and
- To determine the security challenges with the type of cloud storage in use.

Defining cloud computing

Mell and Grance (2011) define cloud computing as 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. This cloud model is composed of five essential characteristics, three service models and four deployment models.

Cloud computing



Types of cloud storage

Cloud storage means "*the storage of data online in the cloud"* wherein company's data is stored in and accessible from multiple distributed an connected resources that comprise a Cloud.

1. Personal Cloud Storage

- Commonly known as mobile cloud storage or personal cloud storage;
- Individuals store personal data in the cloud and providing the individual with access to the data from anywhere; and
- Apple's iCloud is an example of personal cloud storage.

2. Public Cloud Storage

- Is where the enterprise and storage service provider are separate;
- There are no cloud resources stored in the enterprise's data center; and
- The cloud storage provider fully manages the enterprise's public cloud storage.

Types of cloud storage cont'd

3. **Private Cloud Storage**

- The enterprise and cloud storage provider are integrated in the enterprise's data center;
- The storage provider has infrastructure in the enterprise's data center that is typically managed by the storage provider; and
- Helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

4. Hybrid Cloud Storage

- Is a combination of public and private cloud storage;
- Critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

Examples of cloud storage

- Google drive
- Code 42 cash plan
- Microsoft one drive
- Certain safe
- Idrive
- Box
- Drop Box
- Sugar sync
- Apple iCloud
- High tail

Security challenges in cloud storage

Security threats must be overcome in order to benefit fully from this new computing paradigm. Babcock (2013) identified the following:

- Loss of control over physical security-resulting in leakages;
- Loss of data integrity/credentials;
- Account/service trafficking;
- Hijacking;
- Insecure Application Programming Interfaces (APIs);
- Performance/denial of service;
- Malicious insiders
- Abuse of cloud services;
- Insufficient due diligence;
- Shared technology

Methodology

- A qualitative research methodology will be used in this study;
- A pre-set of open-ended questions will be used;
- An interview protocol will be used during the interviews;
- 7 Face-to-face interviews will be conducted
- One focus group interview (8 participants) will be carried out;
- Convenience sampling strategy will be used

Preliminary findings

- UNISA is piloting the Enterprise Content Management system with a few selected departments;
- The ECM is independent of the main ERP system to avoid the use of shared technologies;
- Records will be stored on Google Drive, Box, Drop Box;
- The ECM consultants have not disclosed any weaknesses with cloud storage;
- There is lack of cooperation from other managers to commit resources on the project;

Preliminary findings

Interviewee A: *The pilot project has not yielded the desired results. The ECM project is still being piloted with departments/units that deal with a few records and it will be difficult to determine any security challenges at this stage.*

Interviewee B: *The ECM is being implemented and this stage involves digitising and storage of records. Different systems and technologies will be used to avoid compromising the main Oracle system.*

Interviewee C:*There is a low uptake of the project from some units and managers are reluctant to commit resources. The records will be stored on Google drive, Box and Drop Box. Perhaps with an option of using iCloud.*

Recommendations

- Pre-test cloud storage with dummy data;
- Proceed with the data collection process;
- Further interrogations with other organisations using cloud storage to establish security challenges with cloud storage;
- To implement parallel and complementary storage systems

Conclusion

A preliminary study was done to determine if the research questions were properly formulated and that relevant feedback was provided. Actual data for this study will be collected in June, 2015 as this is an on-going exercise.

References

Babcock, C. (2013) Management strategies for the Cloud Revolution, 4th Ed. McGraw-Hill. New York.

Carpenter, C and Steiner, S. 2005. Using Web 2.0 technologies to push e-resources. Available: http://smartech.gatech.edu/bitstream/1853/13640/2/236-fri-11_05.pdf (Accessed: 01 February 2015).

Creswell, J.W. 2007. *Qualitative inquiry and research design: choosing among five approaches*, 3rd Edition, Thousand Oaks, CA: Sage.

Creswell, J.W. 2009. *Research design: qualitative, quantitative and mixed methods approach*. Thousand Oaks, CA: Sage.

Grant, K.A. and Grant, C.T. 2008. *Developing a model of next generation knowledge management*. Toronto: Information Science Institute, Ryerson University.

Hedberg, J.G. (1995) Thoughts on: exploration of information landscapes through networks. Australian Telecommunications Networks and Applications Conference. Sydney. Australia:141-149.

References continued

Hurd, M. (2014) Operating in the cloud computing revolution. Digital Business Movement, Oracle. USA.

Laudon, K.C. and Laudon, J.P. 2012. *Management information systems: managing the digital firm*, 11th Edition. New Jersey: Prentice Hall, Pearson Education.

Laudon, K.C. and Laudon, J.P. 2013. *Management information systems: managing the digital firm,* 14th Edition, New Jersey: Prentice Hall, Pearson Education.

Leedy, P.D. and Omrod, J.E. 2010. *Practical research: planning and design*. Upper Saddle River, N.J.: Pearson.

Mell, P. & Grance, T. (2011) Computer security. National Institute of Standards and Technology, USA department of commerce, Gaithersburg. USA.

Thornton, C. (2012). Online Cloud backup. Dial a Nerd. Johannesburg. South Africa.

THANK YOU!