Cloud Security: challenges and perspectives

João J. C. Gondim, Priscila A. Solis Barreto, Luis Alberto B. Pacheco
Computer Science Dept.
Universidade de Brasília

Workshop on Cloud Networks
CSBC 2016

Agenda

- Introduction
- Cloud Computing
- Security Issues
- Government Use
- Conclusion

Introduction

- Emerging technology
- IT services as commodity
- Elasticity
- Possibility of entirely transfering the burden of IT operations
  - Infrastructure and services at affordable cost
  - Small, medium businesses
- Inherent risk in transfer
- Some security issues
- How governments are addressing

Cloud Computing

- Main characteristics:
  - On demand self service
  - Wide network access
  - Resourses pooling
  - Rapid elasticity
  - Measured servisse:
    - Per per use

Cloud Computing

- Models:
  - Private
  - Public
  - Community
  - Hybrid

Cloud Computing

- Supporting technologies:
  - Virtualization
  - SOA
  - Provisioning model
    - Minimum roll out

Security Issues

- Trust
- Multi Tenancy
- Privacy and Identity
- Use of Cryptography
- Compliance

Security Issues: Trust

- As a basis for controlling interactions in the cloud
  - Still a research issue
- Risk transfer :
  - User -> provider
  - SLAs

Security Issues: Multi Tenancy

- Contention
  - Failure
  - Incidents
- Forensics
  - Storage may give clues on how to treat properly
- Resource management and allocation

Security Issues: Privacy and Identity

- Complementary issues
- Legal issues
  - Transnationality
- Identity systems should be able to cope with:
  - Easy id management
  - On line collaborative work
  - Device independent/agnostic
  - Federation
  - Transparent
  - Auditable

Security Issues: Use of Cryptography

- Overhead
  - Processing
  - Space
- Fully Homomorphic Encryption
- Privacy Preserving Operations

Security Issues: Compliance

- Current standards have been adapted and applied to cloud environments
  - Not fully satisfatory
- Solutions that work outside the cloud may not be applied straightforward

Government use: Brazil

- Early stage of regulation
- Follows the Law of Information
- Cloud first policy
- Data sensitivity and cloud usage:
  - Public data: hybrid clouds (private sector)
  - Sensitive data: federal clouds
- Information location: only in national territory

Government use: United Kingdom (G-Cloud)

- Mature: since 2012
- Allows storage of sensitive information (only first level)
- Companies pre-register (sign a SLA)
  - Ease hiring by government agencies
- Government agencies responsible for data security
  - Guindance provided by federal government

Government use: United States (FedRAMP)

- Mature: since 2012
- Companies pre-register
  - Includes accreditation by third party organizations
- Military data can also be stored in the cloud
  - Extra accreditation process
- Examples:
  - Amazon GovCloud (entire datacenter accredited)
  - Azure (entire datacenter accredited)

Thank you!