SCIENCESPRINGDAY

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

DEPARTAMENTO DE INFORMÁTICA

Cloud Dependability and Data Privacy

Outsourcing Data Without Outsourcing Control

Computer Systems Research Group

CENTER FOR INFORMATICS AND INFORMATION TECHNOLOGIES

Bernardo Ferreira

PhD Student

Bernardo Ferreira is a PhD Student at CITI / DI-FCT Doctoral Program

Advisor: Henrique Domingos Assistant Professor at DI-FCT and a Researcher at CITI Computer Systems Group

Objectives

Cloud Security and Dependability Solutions

- Prevention of Malicious Actions: insider and outsider attacks against Clouds
- Cloud Vendor Lock-In Practices
- Reliability and Availability with Privacy Concerns
- User Control & Auditing
- Optimization of Trade-offs: Security vs. Dependability vs. Performance

New Foundations and Mechanisms:

- Trusted Computer Base Minimization Under the User Control
- Cloud-Vendor Independence: "Cloud-of-Clouds" Architecture
- Encrypted Operations on Encrypted Cloud Data Repositories
- Intrusion Tolerance
- Efficient Solution: Latency Aware

Methodology

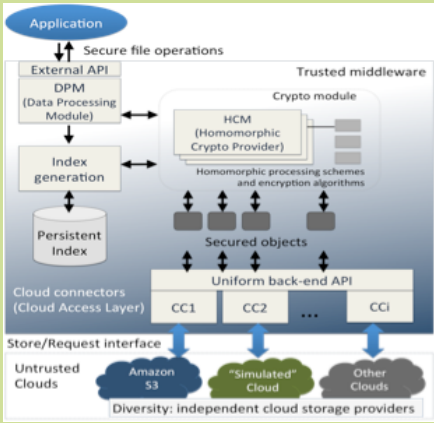
A Middleware Approach to Security and Dependability Services:

- **Homomorphic Encryption Schemes**: implementation and assessment
- **A "Cloud-of-Clouds" Software Architecture**
- **Ranked and Proximity Searching of Encrypted Heterogeneous Data** (Secure Media Searching over Cloud Private Encrypted Data)
- **Flexibility of Deployment (TCB/TPM in local devices vs. Trusted Computational Cloud offering "Dependability as a Service")** (meeting different trade-offs: security vs. latency vs. reliability vs. availability)
- **Dynamic Profiling:** user resources matching cloud operation metrics and costs

Expected Results

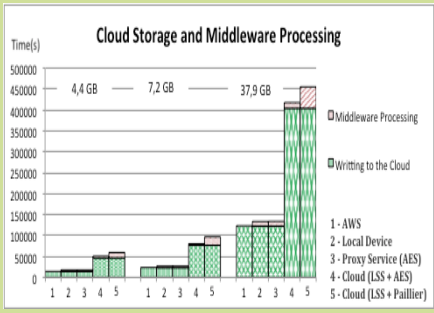
- **Enhanced Privacy with small overhead**
- **Lightweight Encrypted Queries over Encrypted Cloud Data Domains**
- **Appropriate Response Times for Real-Time use** (overhead < 1 sec)
- **Optimization of Cloud Operational Metrics and Costs**
- **Scalability for Real Scenarios of Cloud-Based Solutions**
- **Experimental Assessment with Real Clouds**

Architectural Model (Ref)

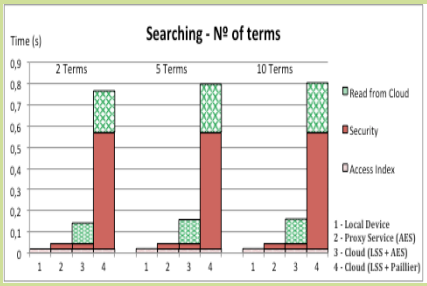


TSKY / CloudCryptoSearch Prototype Implementation

Some Achieved Results



Cloud Storage vs Middleware Processing



Ranked Encrypted Searching

Funding:

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

PEst-OE/EEI/UI0527/2011

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA