SecureCloud

Secure Big Data Processing in Untrusted Clouds

Andrey Brito (Federal University of Campina Grande, Brazil)

CloudScape Brazil, Rio de Janeiro, RJ

December 1-2, 2015

Secure Cloud

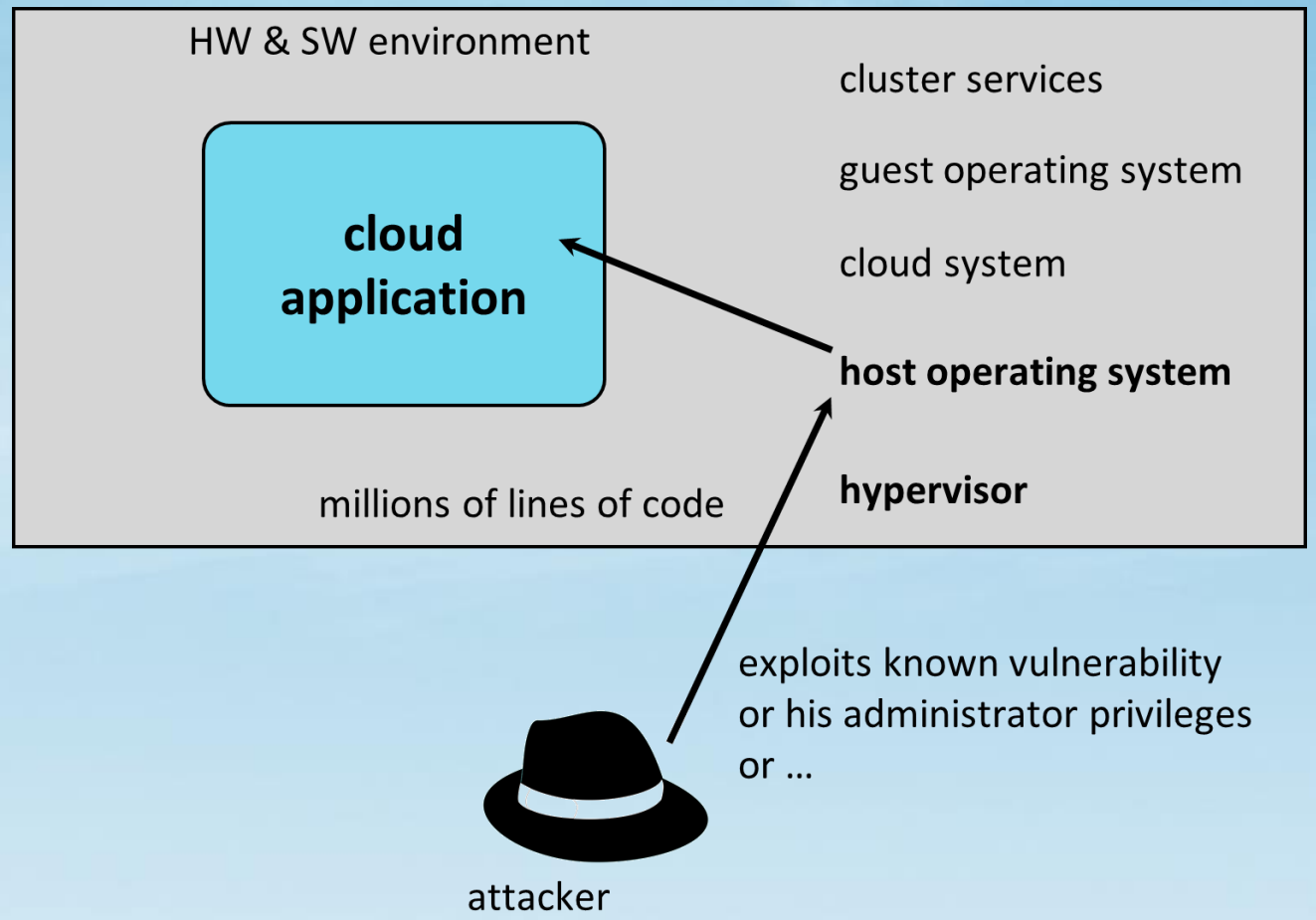
- Main objective
  Improve confidentiality of programs executed in clouds

- Approach
  Evaluate if/how hardware mechanisms in commodity CPUs (esp., Intel SGX) and can be used to protect the confidentiality of programs

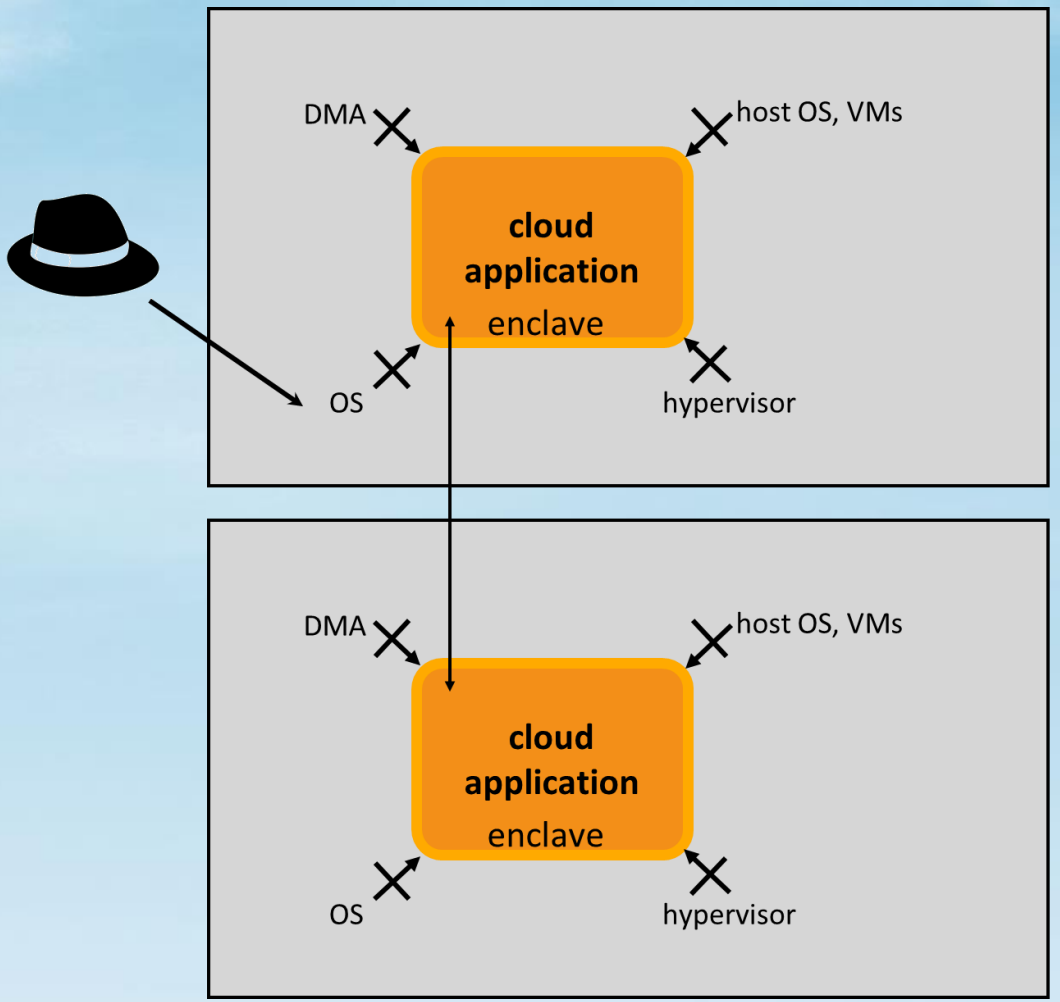
Confidentiality++

- Ensure confidentiality as well as integrity, consistency and availability of applications
- Protect cloud applications against attacks by
  - employees of the cloud provider
  - other tenants / hackers
  - hackers with physical access
- Enable novel applications by removing trust dependency between data providers, application providers and cloud providers

Challenge: lots of software



Protection with enclaves



Objective: All critical application components are protected

Core challenges

- How to protect an application?
- How to minimize the security-induced overhead in big data processing?
- How to ensure application availability?
- How to reconfigure applications if components are unavailable?
- How to ensure the integrity of applications and data?
- How to implement efficient remote attestation to detect unauthorized changes on the application code?
- How to protect cryptographic keys to ensure the confidentiality?

Objectives

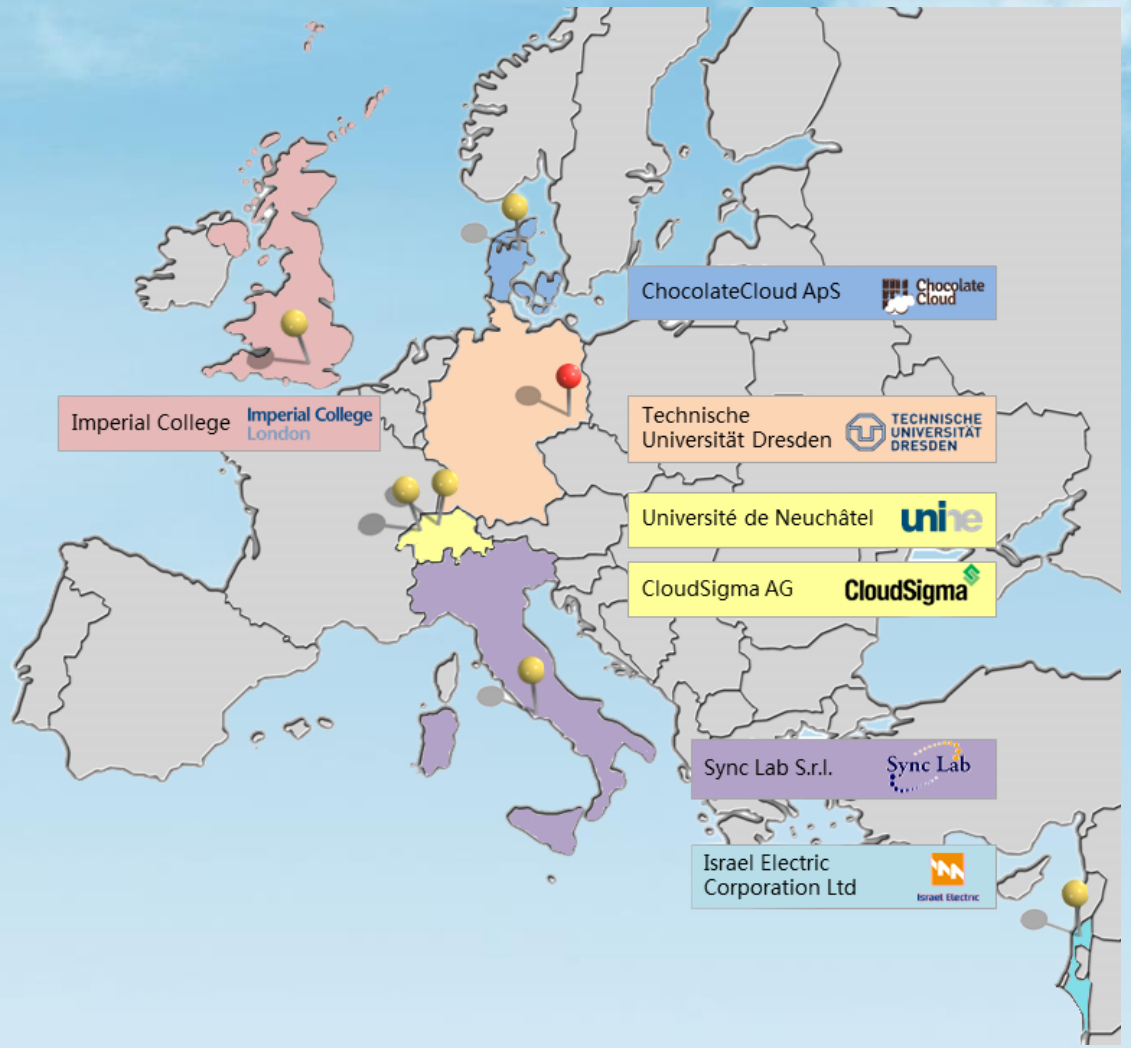
- Substantially improve the state-of-the-art in cloud dependability
- Seamlessly integrate new features into standard cloud infrastructure (e.g., OpenStack)
- Validate and demonstrate in applications for critical infrastructures (e.g., Smart Grids)
- Widely promote and disseminate the outcomes

SecureCloud contributions

- Security and Safety
  - Identify and propose patterns for cloud-based big data applications that are aware of quality-of-service, privacy, and security
  - Address the problem of data privacy by using cutting-edge technology to store data with different levels of protection and in multiple locations
- Accessibility
  - Design and implement services that manage secure containers in an open-source middleware
- Latency
  - Develop a validation system for demonstration and evaluation of cloud-based services applied to the smart grid

Consortium


Federal University of Campina Grande
Universidade Federal de Campina Grande
Universidade Federal de Itajuba
Copel Distribuição SA
COPEL
Intituto Nacional de Metrologia, Qualidade e Tecnologia
INMETRO
Universidade Tecnológica Federal do Paraná
UTFPR
CAS TECNOLOGIA
CAS
Instituto de Tecnologia para o Desenvolvimento
institutos lactec


ChocolateCloud ApS
Chocolate Cloud
Imperial College
Imperial College London
Technische Universität Dresden
TECHNISCHE UNIVERSITÄT DRESDEN
Université de Neuchâtel
unine
CloudSigma AG
CloudSigma
Sync Lab S.r.l.
Sync Lab
Israel Electric Corporation Ltd
Israel Electric

SecureCloud project is funded by the 3rd EU-Brazil coordinated call within the Horizon 2020 program.

European Commission
Horizon 2020

Brazil
Federal Government
MCTI – RNP – CTIC

Swiss Confederation
State Secretariat for Education,
Research and Innovation