SecureCloud
Secure Big Data Processing in Untrusted Clouds

EQUIPE

Coordenador no Brasil
Andrey Elísio Monteiro Brito
Universidade Federal de Campina Grande (UFCG)

Coordenador na União Europeia
Christof Fetzer
Technische Universität Dresden (TUD)

Parceiros brasileiros
Instituto de Tecnologia para o Desenvolvimento (Lactec)
Universidade Federal de Campina Grande (UFCG)
Universidade Federal Técnica do Paraná (UTFPR)
Universidade Federal de Itajubá (Unifei)
Copel Distribuição SA (Copel)
CAS TECNOLOGIA S/A (CAS)
Instituto Nacional de Metrologia, Qualidade e Tecnologia (INM)

Parceiros europeus
Technische Universität Dresden (TUD)
Imperial College (IMP)
University of Neuchâtel (UniNE)
Chocolate Cloud ApS (CC)
Synclab S.r.l. (SYNC)
Israel Electric Corporation Ltd (IEC)
CloudSigma AG (CS)

SITE
http://securecloud.works

CONTATO
securecloud@lsd.ufcg.edu.br

INÍCIO DO PROJETO
Janeiro de 2016

DESCRIÇÃO

Confidencialidade, integridade e disponibilidade de aplicações e dados são uma preocupação imediata para quase todas as organizações que utilizam a computação em nuvem. Isso é particularmente verdadeiro para as organizações que devem cumprir rigorosas políticas de confidencialidade, disponibilidade e integridade, incluindo as **infraestruturas mais críticas** da sociedade, tais como finanças, saúde e redes inteligentes.

Dependabilidade (o que implica confidencialidade, integridade e disponibilidade) surgiu como uma necessidade comercial para que os provedores de nuvem sejam capazes de apoiar os mercados emergentes, incluindo infraestruturas críticas ou robótica na nuvem. A nuvem não só se tornou uma infraestrutura crítica por si só, como também precisa apoiar outras infraestruturas também críticas. Essas incluem redes e sistemas inteligentes nos domínios de saúde e transporte, e se estendem para o futuro de computação de grande escala, tais como a Internet das Coisas (*Internet of Things* - IoT) e Sistemas Cyber-Físicos (Cyber-Physical Systems - CPS).

O projeto **SecureCloud** visa eliminar os obstáculos técnicos para a computação em nuvem confiável, isto é, irá garantir a confidencialidade, integridade, disponibilidade e segurança de aplicações e seus dados. Dessa forma, irá incentivar e permitir uma maior incorporação de soluções de baixo custo, sustentável e inovadora, no contexto de computação em nuvem e, em particular, para aplicações de infraestruturas críticas na Europa e no Brasil.

O objetivo principal do SecureCloud é garantir a dependabilidade de aplicações críticas que são executados em infraestruturas de nuvem potencialmente não confiáveis.

A abordagem inovadora para a dependabilidade na nuvem que desejamos no projeto SecureCloud toma proveito do surgimento de uma nova tecnologia de segurança que promete permitir uma nova geração de aplicações seguras, baseando-as nos mecanismos de *hardware* oferecidos, em particular, no **Intel's Secure Guard eXtensions (SGX)**. Isso permite que as aplicações sejam isoladas, não só de outras aplicações na nuvem, mas também do

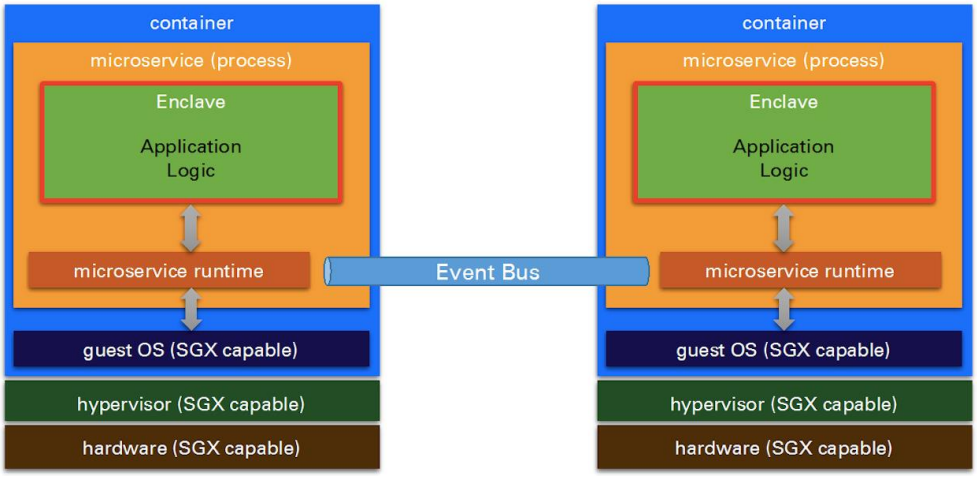
SecureCloud - Secure Big Data Processing in Untrusted Clouds

sistema operacional subjacente e do *hypervisor*. Isso permite aos usuários executar suas aplicações sensíveis em uma nuvem pública, sem a necessidade de confiar incondicionalmente no provedor de nuvem.

O projeto SecureCloud irá facilitar o uso de aplicações com requisitos de alta ou muito alta segurança. Os **desafios técnicos fundamentais** do projeto são integrar e ampliar as tecnologias mais populares dos últimos anos para garantir a confiabilidade de aplicações em nuvem.

SecureCloud irá:

- Alavancar a tecnologia **Intel SGX** como raiz de confiança (*root of trust*) para fornecer confidencialidade e integridade de dados sigilosos. SGX cifra o conteúdo em memória das aplicações para evitar que o sistema operacional ou o *hypervisor* seja capaz de ler e/ou modificar dados dessas aplicações;
- Usar **OpenStack** como infraestrutura de nuvem;
- Estender a tecnologia de ***Container*** para permitir a execução em máquinas com Intel SGX;
- Usar um **serviço de coordenação** para detectar uma falha em uma máquina ou em um serviço de uma aplicação e reiniciar o serviço em uma máquina diferente (física ou virtual) ou em um contêiner, de acordo com as exigências do serviço;
- Usar **Redes Definidas por Software (SDN, em inglês)** para conectar os componentes das aplicações dentro ou entre *datacenters*.



Consórcio