

SecureCloud - Secure Big Data Processing in Untrusted Clouds



EQUIPE

Coordenador no Brasil:

Prof. Andrey Brito

Universidade Federal de Campina Grande (UFCG)

Coordenador na União Europeia

Prof. Christof Fetzer

Technische Universität Dresden (TUD)

PARCEIROS

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)

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

www.securecloud.works

CONTATO

securecloud@lsd.ufcg.edu.br



DESCRIÇÃO

Confidencialidade, integridade e disponibilidade de aplicações e dados são uma preocupação imediata para quase todas as organizações que utilizam computação na nuvem. Isso é particularmente verdadeiro para as organizações que desenvolvem aplicações para suportar as infraestruturas mais críticas da sociedade, como energia, saúde e transporte.

A solução proposta pelo SecureCloud é um ecossistema de serviços e ferramentas para ambientes de nuvem. Este ecossistema é caracterizado por prover garantias superiores de confidencialidade e integridade, fornecendo proteção contra ataques de usuários privilegiados (por exemplo, o provedor da nuvem ou o administrador do sistema) e software (por exemplo, o hypervisor). Essa proteção depende de novas extensões de segurança recentemente introduzidas em CPUs disponíveis comercialmente. A implementação atual é baseada em Intel® SGX, que permite que as aplicações sejam isoladas não só de outras aplicações na nuvem, mas também do sistema operacional subjacente e do hipervisor. Desta forma, os usuários tornam-se capazes de executar suas aplicações sensíveis em nuvens públicas, sem a necessidade de confiar incondicionalmente nos provedores. A solução é de aplicação ampla e possui as seguintes características: i) é personalizável e modular, permitindo aos desenvolvedores usar apenas os recursos que precisam; ii) é flexível, pois pode satisfazer uma ampla gama de requisitos específicos de clientes, incluindo processamento de big data, computação confidencial, comunicação segura entre nuvens, e armazenamento de dados confiável; e iii) é interoperável, pois suas instalações podem ser perfeitamente integradas com as melhores ofertas da comunidade Open Source.

Resultados

Infraestrutura

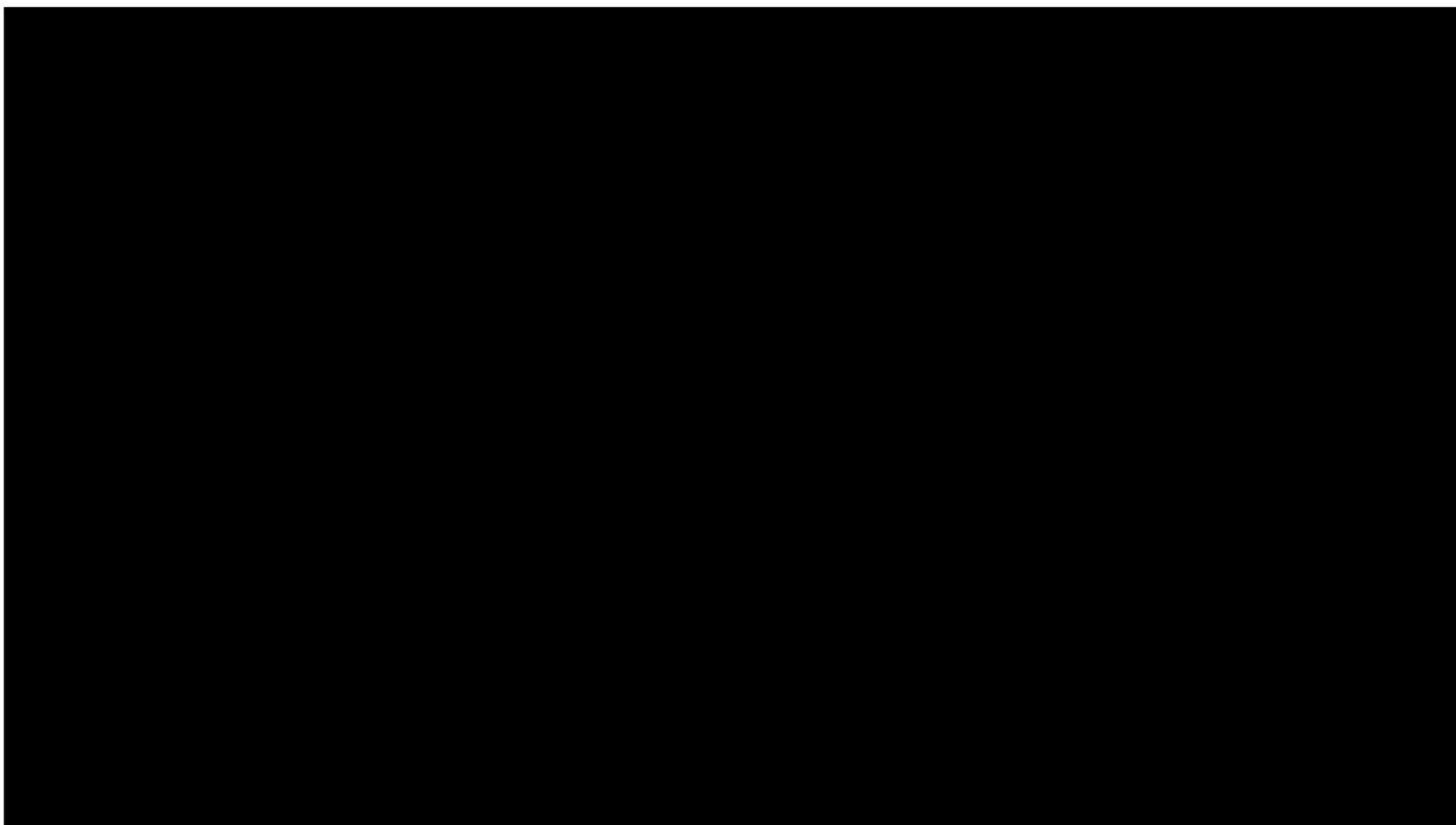
Provisionamos contêineres e máquinas virtuais preparados para uso de Intel® SGX, ao ponto de possibilitar a instanciação de recursos de maneira transparente ao usuário via OpenStack ou Kubernetes, oferecendo mecanismos para detecção de violações de integridade em aplicações através do uso de **SCONE** ou **LibSeal**.

Plataforma

Neste nível podemos destacar os seguintes serviços: i) **SCBR**, um barramento de mensagem (**Pub/Sub**) capaz de prover roteamento confidencial; ii) **TaLoS**, uma biblioteca para criação de terminadores TLS dentro de enclaves, protegendo certificados e conexões; e iii) plugins para o **Asperathos**, permitindo execução de aplicações seguras que processam grandes quantidades de dados com garantias de tempo e capacidade de autoajuste dos recursos usados.

Aplicação

Criação de um runtime para facilitar o porte de aplicações e de uma coleção de modelos de aplicações que realizam processamento de dados de forma segura e confidencial na plataforma **Asperathos**, bem como exemplos de validação de aplicações considerando casos de uso em **IoT** e **SmartGrids**.



Consórcio



Universidade Federal
de Campina Grande

Université
de Neuchâtel

unine



TECHNISCHE
UNIVERSITÄT
DRESDEN

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ



Imperial College
London



Israel Electric



COPEL
Telecom



INMETRO

CloudSigma



institutos lactec
INOVADORES POR NATUREZA



Chocolate
Cloud