18º WRNP Workshop RNP

15 | 16 MAIO
Belém | PA

3ª CHAMADA COORDENADA BR-UE

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
Prof. 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
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
securecloudproject.eu

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 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, garantirá a confidencialidade, integridade, disponibilidade e segurança de aplicações e seus dados. Dessa forma, incentivará e permitirá 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 nova tecnologia de segurança, que promete permitir uma nova geração de aplicações seguras, baseando-as nos mecanismos de *hardware* oferecidos, tais como, Intel's Secure Guard eXtensions (SGX), Amd's Secure Memory Encryption (SEM). Isso permite que as aplicações sejam isoladas, não só de outras aplicações na nuvem, mas também do 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.

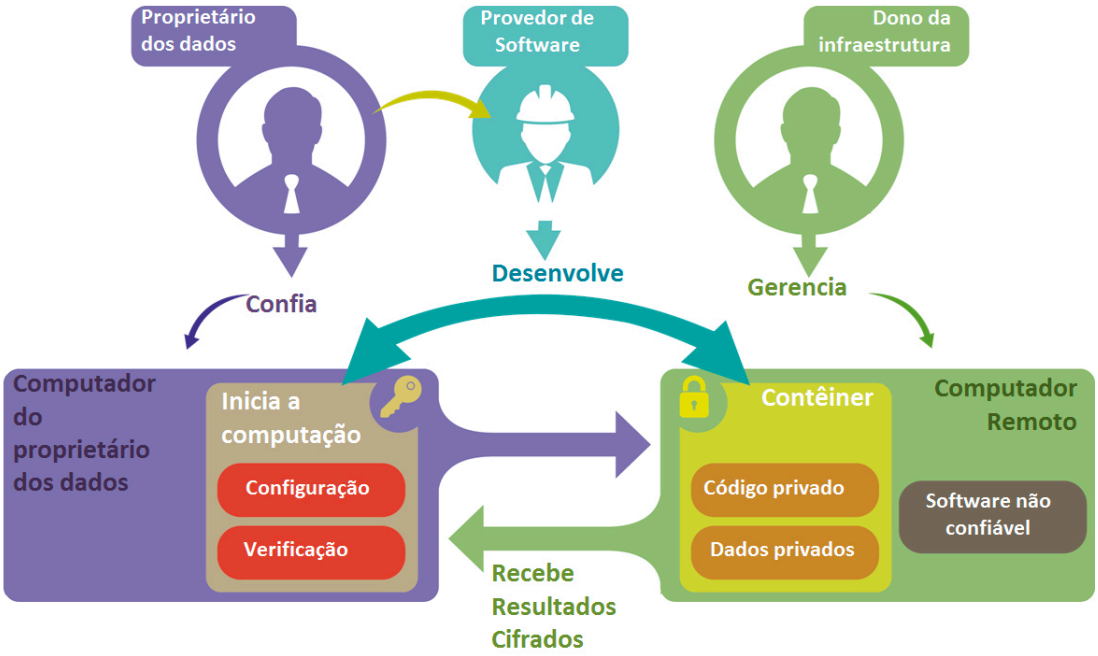
3ª CHAMADA COORDENADA BR-UE

SecureCloud - Secure Big Data Processing in Untrusted Clouds

O projeto **SecureCloud** facilitará 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.

Atualmente, o projeto SecureCloud provê:

- **SCONE** : Secure Linux containers with SGX;
- Ferramentas para compilação e orquestração de contêineres seguros;
- **LibSeal** : Detecting Service Integrity Violations Using Trusted Execution;
- Ferramentas para auditoria de serviços que não serão completamente executados dentro de enclaves;
- Aplicações seguras com *smartmeters*;
- Modelos de aplicações para IoT e *smart grids* que garantem privacidades dos dados mesmo com armazenamento e processamento na nuvem;
- Uso de OpenStack como infraestrutura de nuvem.



Consórcio:

Imperial College London · Universidade Federal de Rio Grande do Norte · Universidade Federal de Campina Grande · Technische Universität Dresden · UTFPR · Université de Neuchâtel · CAS Tecnologia · Instituto Lactec · Israel Electric · Chocolate Cloud · CloudSigma · COPEL · Sync Lab · INMETRO

RNP · Ministério da Defesa · Ministério da Cultura · Ministério da Saúde · Ministério da Educação · Ministério da Ciência, Tecnologia, Inovações e Comunicações · Brasil Governo Federal