

# ATMOSPHERE: Uma Plataforma para Serviços Confiáveis em Nuvens Híbridas Federadas

## EQUIPE

### Coordenador no Brasil:

Prof. Francisco Brasileiro

Universidade Federal de Campina Grande (UFCG)

### Coordenador Europeu

Prof. Ignacio Blanquer

Universitat Politècnica de València

## PARCEIROS

Universidade Federal de Campina Grande (UFCG)

Universidade Federal de Minas Gerais (UFMG)

Universidade Federal do Amazonas (UFAM)

Universidade Estadual de Campinas (Unicamp)

Universidade de Brasília (UNB)

Kunumi

Universitat Politècnica de València (UPV)

Technische Universität Dresden (TUD)

University of Piraeus (UNIP)

Politecnico di Milano (POLIMI)

Trust-IT Services (Trust-IT)

Universidade de Coimbra (UC)

Quibim

## SITE

www.atmosphere-eubrazil.eu

## CONTATO

fubica@computacao.ufcg.edu.br



## DESCRIÇÃO

A falta de meios apropriados para avaliar a confiabilidade que pode ser aplicada nos serviços oferecidos pelos provedores de nuvem tem sido tratada como um fator limitante para a adoção do paradigma de computação em nuvem para o fornecimento de serviços de TI em diversos segmentos. Embora, sem dúvida, alguns aspectos relacionados à confiabilidade, como a tolerância a falhas, possam ser melhor administrados em um ambiente de nuvem, outros, como segurança e privacidade, ainda causam grande preocupação. Além disso, dimensões de confiança novas e menos exploradas aparecem quando consideramos, por exemplo, aplicações de big data, uma classe importante de aplicações que normalmente executam infraestruturas de computação na nuvem devido aos seus requisitos.

O projeto ATMOSPHERE está realizando o projeto e desenvolvimento de uma plataforma capaz de realizar o design, implementação, implantação e gerenciamento de aplicações confiáveis fazendo uso de um pool intercontinental de recursos híbridos e federados.

A plataforma fornece serviços de monitoramento e adaptação de confiabilidade que podem ser usados para avaliar a confiabilidade das aplicações, tanto em tempo de projeto quanto de execução, e para adaptar aplicações em execução que se desviam dos níveis de confiabilidade visados.

Além disso, a plataforma fornece um toolbox de serviços de armazenamento e processamento de dados confiáveis que podem ser usados para aumentar a confiabilidade das aplicações, bem como serviços que facilitam a implantação de aplicativos em vários provedores de nuvem.

### Visão Conceitual da plataforma ATMOSPHERE

A plataforma ATMOSPHERE oferece serviços que podem ser usados para melhorar a confiabilidade de aplicações distribuídas, assim como facilitar sua implantação e execução em infraestruturas de nuvens privadas federadas que cooperam através de um conjunto de políticas compartilhadas.

Esses serviços são organizados em três camadas:

- Os Serviços de Gerenciamento de Infraestrutura (IMS - Infrastructure Management Services) são fornecidos na

camada mais baixa e permitem o gerenciamento abstrato de recursos em diferentes provedores de nuvem, bem como a instalação automatizada e personalizada de software nesses recursos;

- Os Serviços de Gerenciamento de Dados Confiáveis (TDMS - Trustworthy Data Management Services) usam os serviços do IMS para lidar com o gerenciamento de serviços de armazenamento confiáveis, seguros, com garantia de privacidade e eficientes;
- Serviços de Processamento de Dados Confiáveis (TDPS - Trustworthy Data Processing Services) confiam no TDMS e no IMS para oferecer mecanismos baseados em ML que fornecem funcionalidades confiáveis de análise de dados para as aplicações.

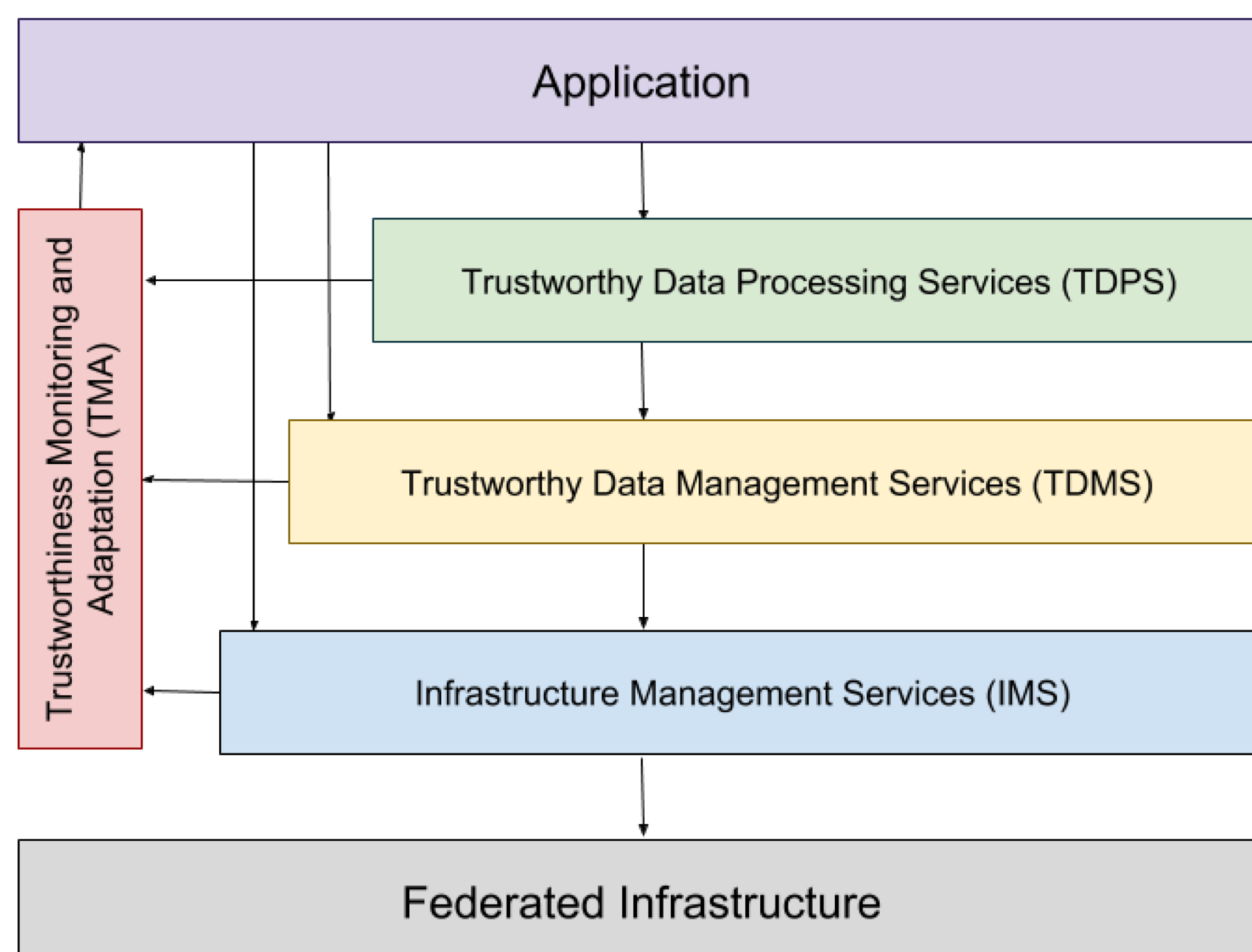


Figura 1 - Camadas da plataforma ATMOSPHERE.

Cada uma dessas camadas possui propriedades de confiabilidade relevantes e trabalha em conjunto para fornecer um serviço que seja confiável. Além disso, existe uma camada transversal que oferece serviços para gerenciar a confiabilidade em todos os níveis da plataforma. A Figura 1 fornece uma representação gráfica dessa estrutura.

Os serviços fornecidos por cada uma das camadas que compõem a plataforma ATMOSPHERE podem ser serviços de toda a federação disponíveis para todos os usuários e aplicações ou serviços reutilizáveis que podem ser personalizados e incorporados às próprias aplicações.



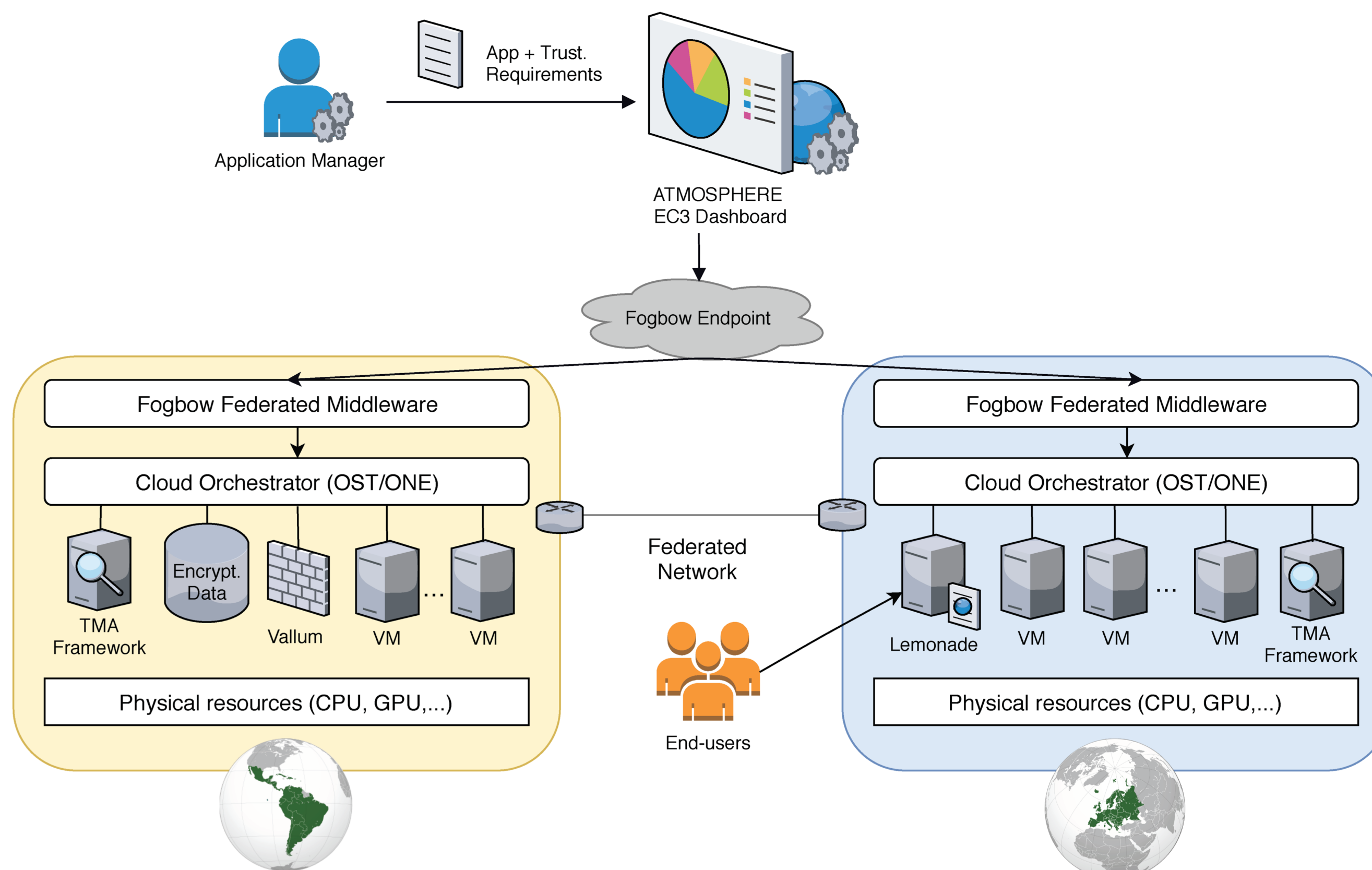


Figura 2 – Arquitetura simplificada da plataforma ATMOSPHERE

Além dos usuários finais das aplicações, há pelo menos três classes de usuários que interagem com a plataforma ATMOSPHERE e os serviços e aplicações que a utilizam: desenvolvedores de aplicações, gerenciadores de aplicações e gerenciadores de recursos. Além disso, as interações desses usuários com a plataforma podem ocorrer tanto em tempo de projeto quanto de execução.

#### Experimentos com implementações de provas de conceito

Para realizar a avaliação da plataforma ATMOSPHERE, a mesma foi implementada e implantada com os componentes apresentados na Figura 2. Dois aspectos principais já foram avaliados na plataforma ATMOSPHERE: privacidade e segurança.

Para as avaliações referentes a privacidade foram implementados sensores e atuadores que oferecem a funcionalidade de privacidade como serviço (PRIVAAaaS). Os sensores se comunicam com a plataforma através do componente de monitoramento através de TCP usando criptografia baseada em certificados para a transmissão dos dados. A operação dos sensores consistem em: após executar a anonimização dos dados recebidos dos clientes, os dados obtidos da operação. Ao receber os dados o monitor verifica se o nível de anonimização alcançou os critérios definidos e caso não o tenha o sensor será notificado para melhorar o processo realizado. De toda forma a notificação será enviada para o sensor através de um atuador que irá indicar se o resultado obtido já foi bom o suficiente ou se ainda é necessário continuar o processo.

Steps	ID Supress	QuasiID Supress	Medicines Dataset					
			Risk Threshold					
			100%	50%	10%	1%	0.5%	0.1%
Possibilities	1	1	2	2	5	62	62	62
# Attacks	153	153	247	247	520	5730	5730	5730
Re-identification Risk	1	1	0.33333	0.33333	0.025	0.00063131	0.00063131	0.0000307
Data Loss	0	0	0.3355	0.3355	0.509	0.8587	0.8587	0.8587
Privacy Score	0.1	0.1	0.666453	0.666453	0.9266	0.91356182	0.91356182	0.91410237
k-value	-	-	2	2	5	62	62	62

Figura 3 - Resultados referentes a privacidade

Para realizar a avaliação, oito datasets foram usados, mas os resultados apresentados se referem a apenas um deles uma vez que os resultados foram bastante similares. Em todos os

conjuntos de dados, foi realizada a anonimização dos atributos de identificação, depois dos atributos de semi-identificação e os atributos sensíveis. Além disso, o modelo k-anonymity foi aplicado aumentando k até que o risco de reidentificação chegasse a um determinado limiar, que teve os seguintes valores: 100%, 50%, 10%, 1%, 0,5% e 0,1%. A Figura 3 apresenta os resultados obtidos.

No que se refere a segurança, foram executados experimentos para demonstrar o impacto no desempenho quando é realizada uma execução remota segura de uma aplicação fazendo uso do Vallum, que é um componente que permite a execução em enclaves diretamente protegidas no processador, que foi implementado na plataforma ATMOSPHERE.

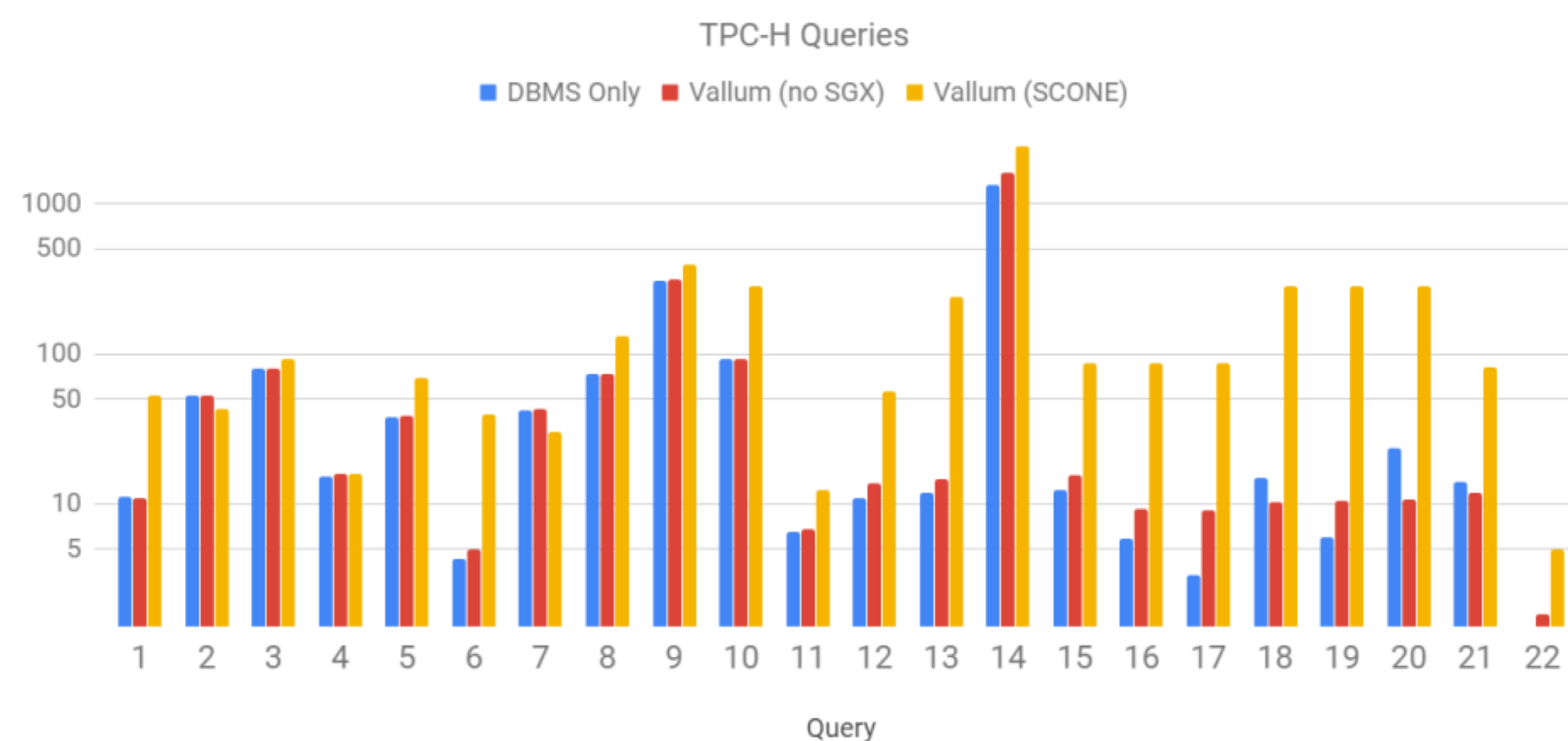


Figura 4 - Resultados referentes às consultas do TPC-H

Para tanto, foram realizadas consultas TPC-H (um benchmark de 22 consultas SQL). Os resultados obtidos podem ser vistos nas figuras 4 e 5.



Figura 5 - Resultados referentes ao tempo de execução dos experimentos com o Vallum