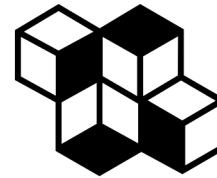


Privacy-preserving recommendations for Online Social Networks using Trusted Execution Environments

Recomendações com privacidade preservada para redes sociais *online* usando ambientes de execução confiável

Guilmour Rossi, Luiz Gomes-Jr, Marcelo Rosa e Keiko Fonseca



SBSeg2018
NATAL - RN

Guilmour Rossi
me@guilmour.org





Guilmour Rossi
me@guilmour.org

- *Engenharia de Computação* – Universidade Tecnológica Federal do Paraná (UTFPR)
- **Hacktivismo:** Projetos em software livre e de ativismo estudantil, político, social...
- Iniciação científica no Projeto *SecureCloud*.



Sumário

- Redes Sociais Online e Problemas
- Arquitetura Proposta (SSP)
- Sistemas de Recomendações
- Testes e resultados



Redes Sociais Online

- Revolucionaram como as pessoas interagem
 - Comunicação
 - Fonte de informação
 - Expressão de opiniões
- Maior base de usuários (FB+Twitter = >2bi)
- Impacto em várias áreas
 - Educação, Mídia, Política, Protestos, Filantropia...



2018 *This Is What Happens In An Internet Minute*



Created By:
@LoriLewis
@OfficiallyChadd



Facebook confirma que rastreia até os movimentos do seu mouse

tecnoblog

TECNOCAST

REVIEWS

CUPONS

CURSOS

ASSISTENTE DE COMPRAS

ANUNCIE



A controvérsia dos 50 milhões de perfis do Facebook manipulados pela Cambridge Analytica



Após vazamento de dados, Google enfim decide dar adeus ao Google+



SHARE



TWEET



WHAT

Após vazamento de dados, Google enfim decide dar adeus ao Google+



Advertising Business Model

Revenue

In Millions

- Payments and Other Fees
- Advertising



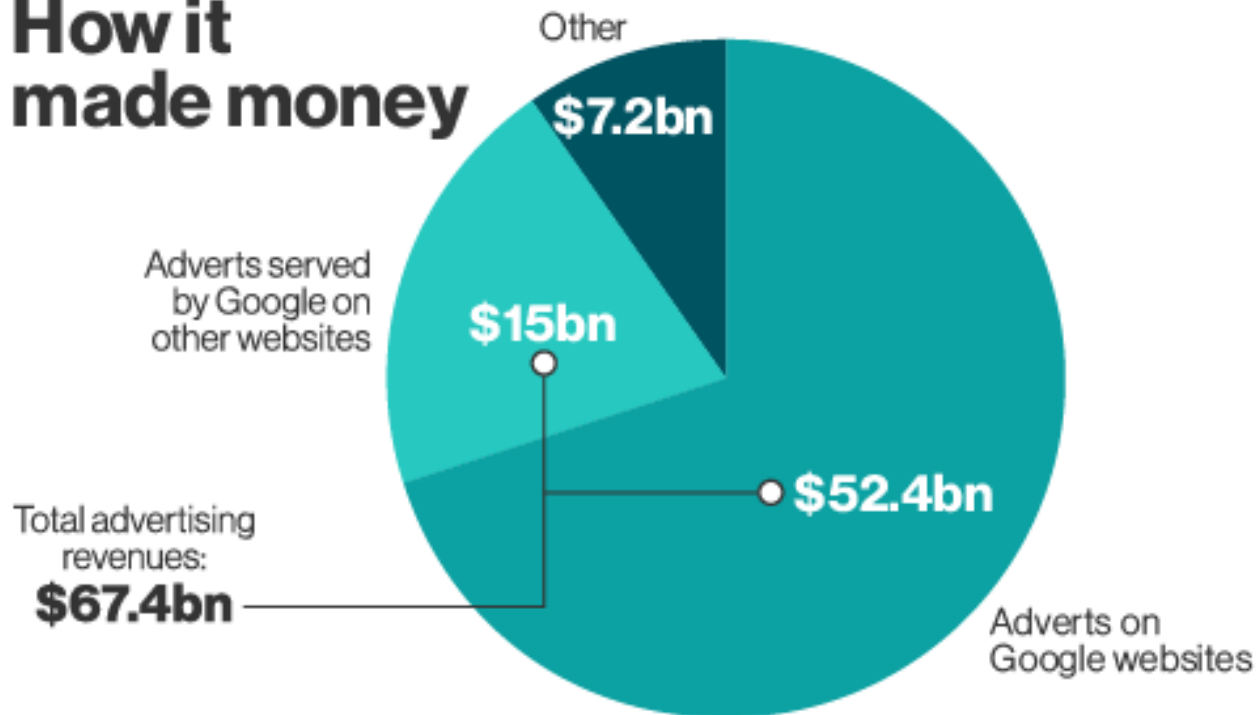
2018
> 98%



Advertising Business Model

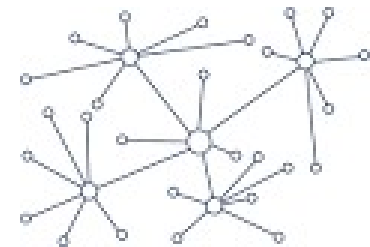
Google → 2015
> 90%

How it made money



Esforços Relacionados

- Regulamento Geral sobre a Proteção de Dados (GDPR)
- Projetos focados na anonimização de dados.
- Protocolos que se baseiam em blockchain



Ambiente de execução confiável

Trusted Execution Environment (TEE)

“Um ambiente de execução confiável é uma área segura de um processador principal. Garante que o código e os dados carregados no interior sejam protegidos em relação à confidencialidade e integridade.”

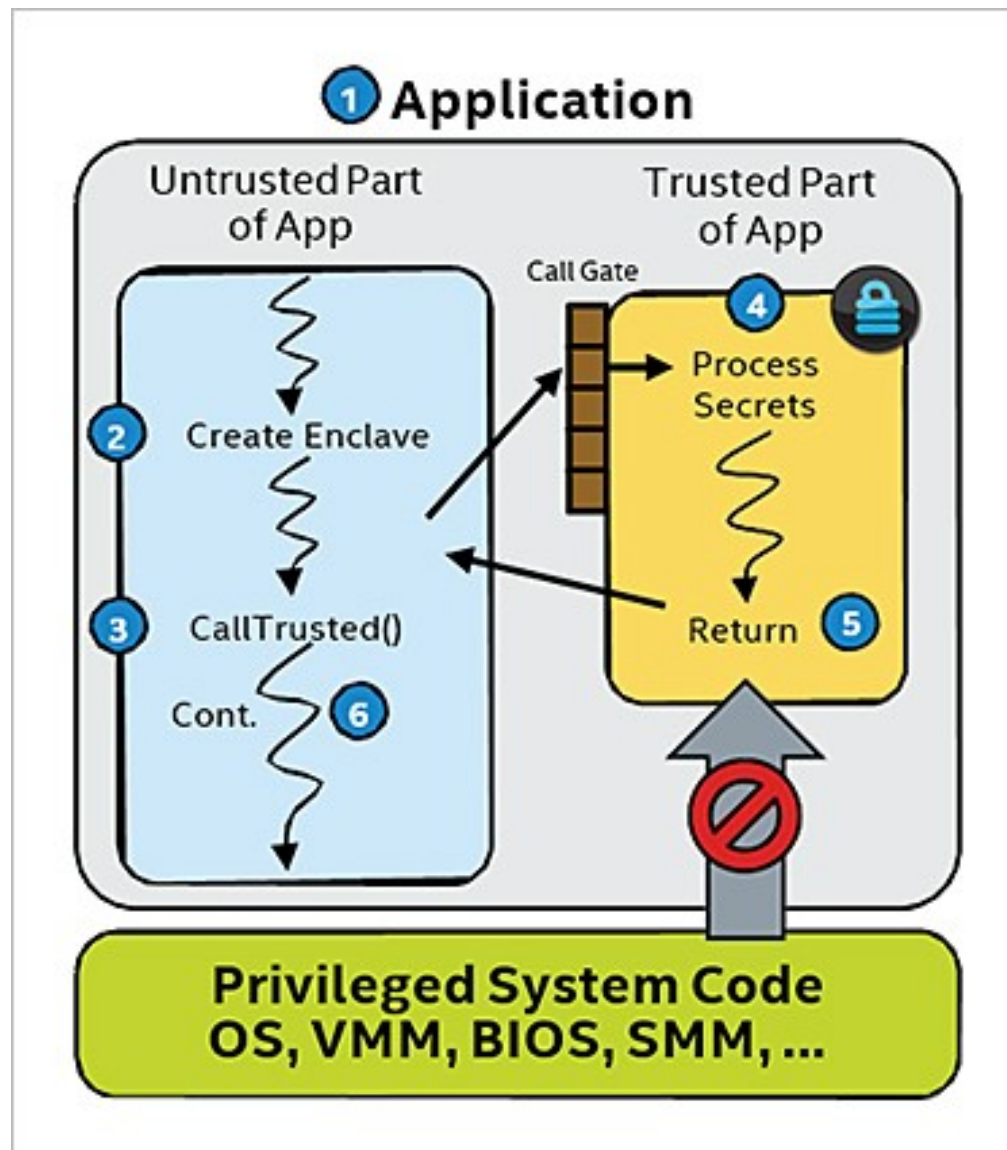


Intel SGX

(Ambiente de Execução Confiável)

- Instruções de CPU lançadas em 2015 com a 6ª geração de processadores Intel
- Processamento é feito em áreas criptografadas na memória (**enclaves**)
- Limite de memória atual: 128 Mb





Arquitetura Proposta

- É necessário projetar uma framework mais restritiva.
- Na nossa proposta, nem os provedores de serviços tem acesso aos dados de sua rede social.
- Em contrapartida, a framework é responsável por fornecer uma API para os provedores and anunciantes para inserir conteúdos em suas redes.

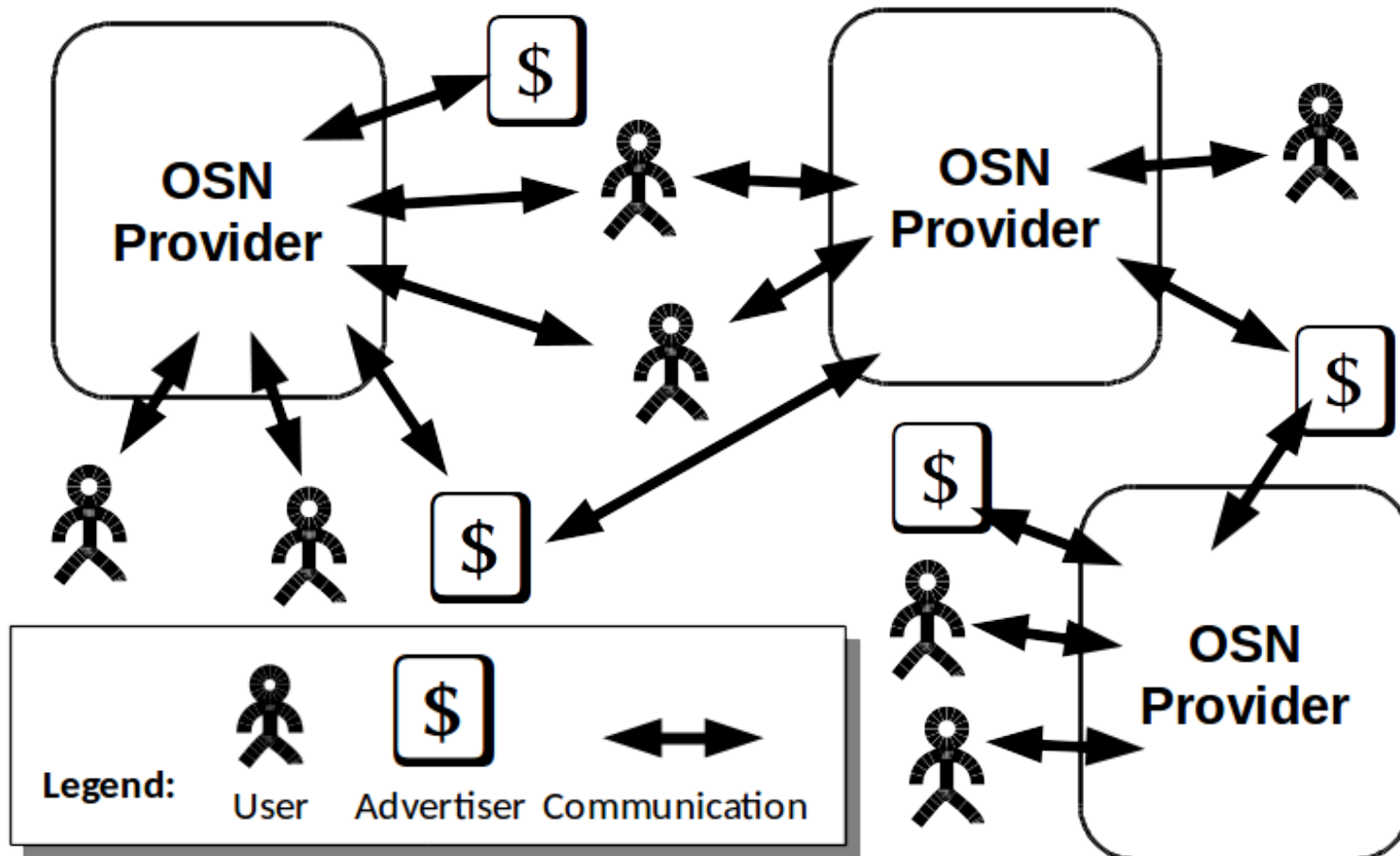


Arquitetura Proposta

- **Provedores:** Oferecem o serviço online (Redes sociais, ecommerce, governos)
- **Usuários:** Pessoas que acessam os serviços
- **Anunciantes:** Pagam os provedores para combinar seus anúncios baseados nas preferências dos usuários.



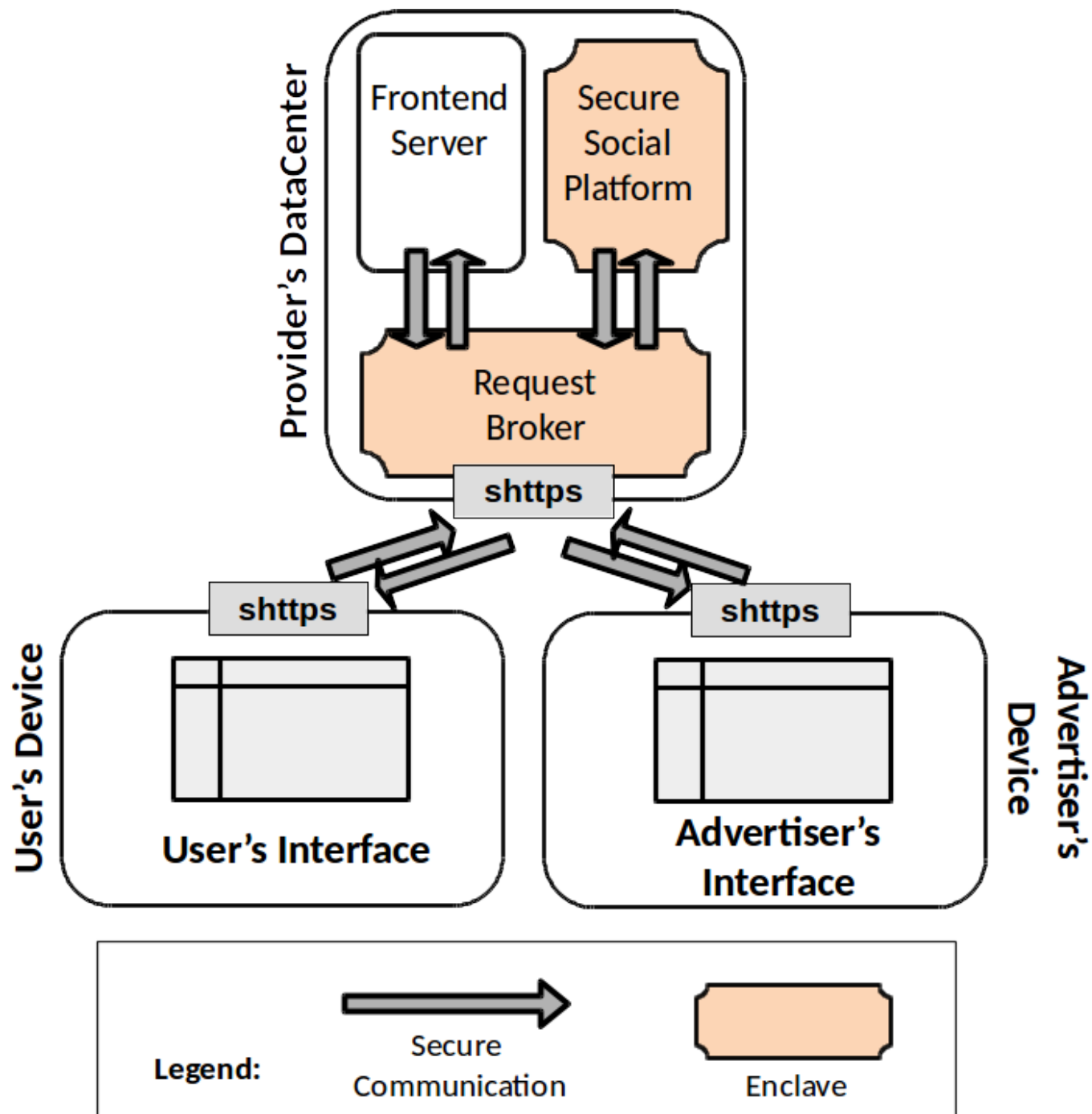
Arquitetura Proposta



Plataforma Social Segura (SSP)

- É efetivamente uma caixa preta para os provedores.
- Podem configurar a plataforma e adequar aos seus modelos de serviços.
- Terão acesso a estatísticas anônimas de visualização de conteúdo e anúncios.





Recomendações na SSP

Cientes que compraram este item também compraram



Hereges



Paisagem de Outono

Leonardo Padura

★★★★★ 3

Capa comum

R\$ 35,60



Ventos de Quaresma

Leonardo Padura

★★★★★ 3

Capa comum

R\$ 38,80



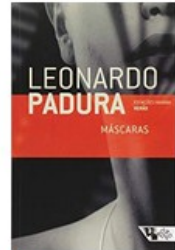
Passado Perfeito

Leonardo Padura

★★★★★ 4

Capa comum

R\$ 35,60



Máscaras

Leonardo Padura

★★★★★ 1

Capa comum

R\$ 35,60



BBC News Brasil @bbcbrasil

Twitter oficial da BBC Brasil. Aqui você encontra o melhor do nosso conteúdo e participa de um diálogo global. Junte-se a nós!

Seguir



EL PAÍS Brasil @elpais_brasil

As notícias globais mais relevantes e os últimos acontecimentos em português, pelos jornalistas do EL PAÍS. Instagram e Snapchat: elpaisbrasil

Seguir



Nexo @NexoJornal

Nexo é um jornal digital para quem busca explicações precisas e interpretações equilibradas sobre os principais fatos do Brasil e do mundo.

Seguir



CartaCapital @cartacapital

Mais do que a notícia, informação inteligente, relevante e necessária sobre política, economia e

Recomendados para você



Recomendações na SSP

- Parte fundamental de redes sociais para o usuário e para a receita com anúncios.

(Personalização, sugestão de amigos, filmes, produtos, anúncios...)

- Alto custo computacional



Experimentos - API Básica

- GetRecommendations(user_id)
- AddUser
- AddItem
- AddLike
- AddLikes



```
curl localhost:8080/api/recommendations/345
```

```
{  
  "uid" : "345",  
  "recommendations" : [  
    "Taxi Driver (1976) ",  
    "Vertigo (1958) ",  
    "Sabrina (1954) ",  
    "Fantasia (1940) ",  
    "Conan the Barbarian (1981) "  
  ]  
}
```



Experimentos - API Básica

- API feita em Python usando a biblioteca Scikit-Surprise.
- Vários algoritmos de sistemas de recomendação com abordagens de Decomposição em Valores Singulares de K-ésimo Vizinho mais Próximo, entre outros.
- SVD, kNN, CoClustering, SlopeOne, and more.



Experimentos - API Básica

- Treinadas com dataset do projeto MovieLens
- 100 mil avaliações (1-5) de 943 usuários em 1682 filmes.
- 1 milhão de avaliações (1-5) de 6040 usuários em 3706 filmes.



Experimentos - API Básica

- Executadas em containers SCONE.

SCONE: Secure Linux Containers with Intel SGX

Sergei Arnautov¹, Bohdan Trach¹, Franz Gregor¹, Thomas Knauth¹, Andre Martin¹,
Christian Priebe², Joshua Lind², Divya Muthukumaran², Dan O’Keeffe², Mark L Stillwell²,
David Goltzsche³, David Eyers⁴, Rüdiger Kapitza³, Peter Pietzuch², and Christof Fetzer¹

¹*Fakultät Informatik, TU Dresden, christof.fetzer@tu-dresden.de*

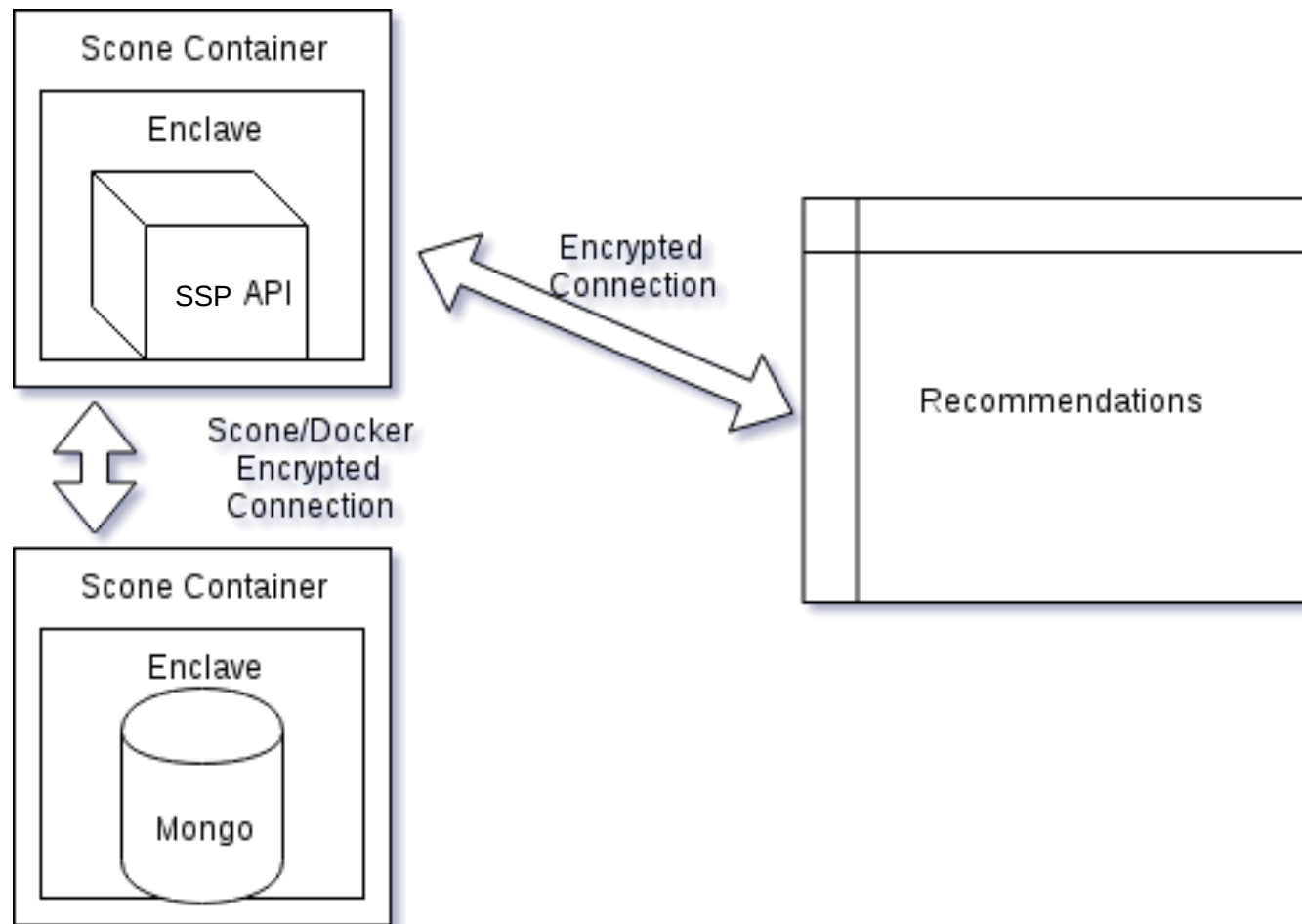
²*Dept. of Computing, Imperial College London, prp@imperial.ac.uk*

³*Informatik, TU Braunschweig, rrkapitz@ibr.cs.tu-bs.de*

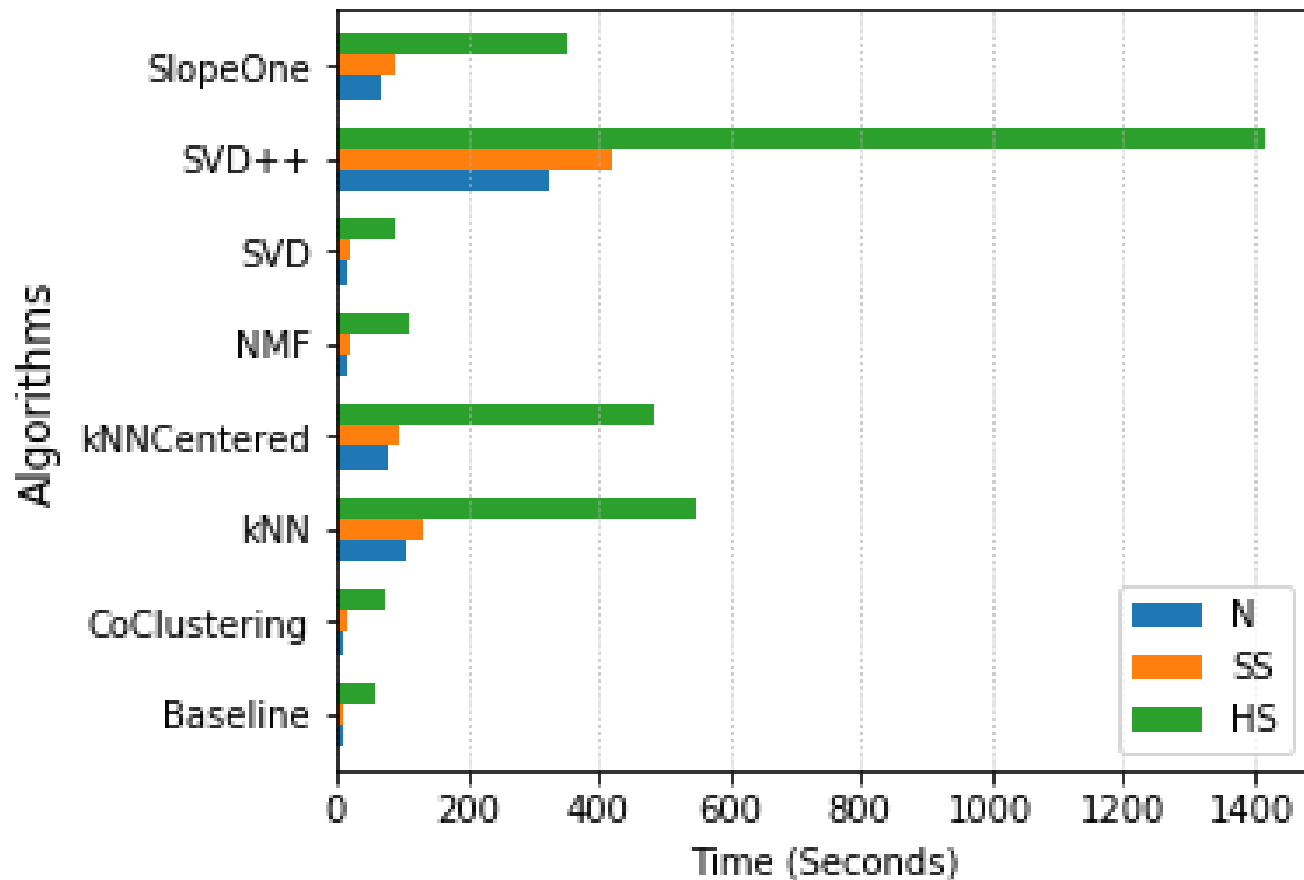
⁴*Dept. of Computer Science, University of Otago, dme@cs.otago.ac.nz*



Experimentos - API Básica



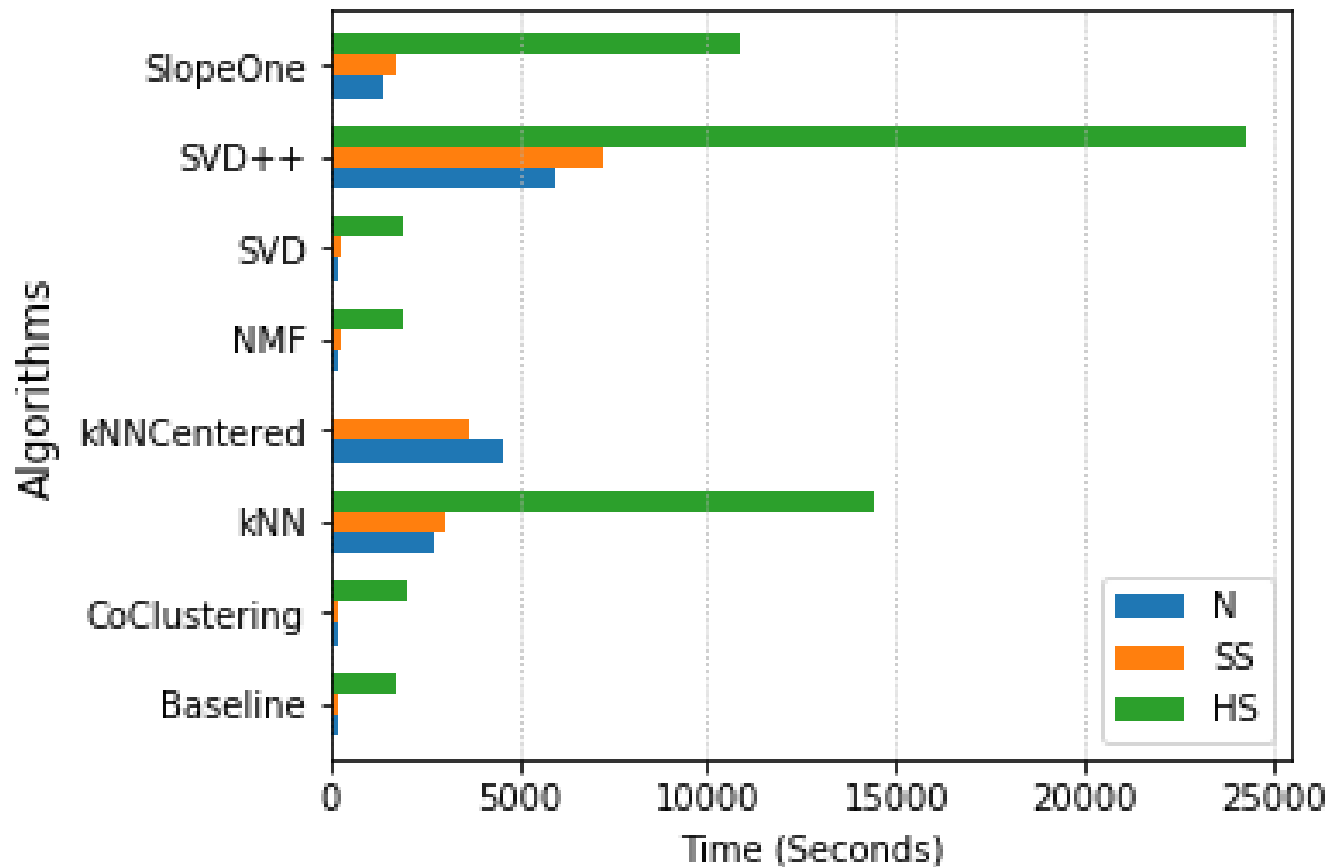
Experimentos – Resultados (100K)



Dataset de 100 mil avaliações



Experimentos – Resultados (1M)



Dataset de 1M de avaliações



Experimentos – Resultados

Table 1. Running times of the algorithms and proportional increase.

Algorithm	Time (s)					
	100K Dataset			1M Dataset		
	N	SS	HS	N	SS	HS
Baseline	8.3	12.8	59.6 (7.2*N; 4.7*SS)	142.2	180.4	1780 (12.6*N; 9.9*SS)
CoClustering	9.3	14.4	73.6 (7.9*N; 5.2*SS)	145.6	197.4	2000.7 (13.8*N; 10.2*SS)
kNN	107.8	135.1	548.9 (5.1*N; 4.1*SS)	2751.7	3025.8	14401.3 (5.3*N; 4.8*SS)
kNNCentered	81.1	98.5	484.3 (6*N; 5*SS)	4587.3	3619.0	82921,5 (18,1*N; 23*SS)
NMF	14.1	21.8	111.5 (7.9*N; 5.2*SS)	178.7	255.9	1925.3 (10.8*N; 7.6*SS)
SVD	14.7	22.3	92.5 (6.3*N; 4.2*SS)	194.6	263.2	1966.7 (10.2*N; 7.5*SS)
SVD++	324.0	422.6	1415.1 (4.4*N; 3.4*SS)	5966.8	7213.3	24277 (18*N; 3.4*SS)
SlopeOne	69.7	92.8	353.1 (5.1*N; 3.9*SS)	1354.1	1716.5	10877 (8.1*N; 6.4*SS)



SecureCloud Project

- Objetivo: fornecer serviços seguros na nuvem
- Colaboração internacional e interdisciplinar
- Oferece: containers de serviço, protocolos de comunicação, processamento de dados e **armazenamento**

Obrigado!

In an age of performative cruelty,
kindness is punk as f*ck.

Be punk as f*ck.



me@guilmour.org | [@guilmour](https://www.instagram.com/guilmour) | [guilmour.org](https://www.guilmour.org)

Créditos

- Images:
 - Watercolor leafs: [Projetado por Freepik](#)
 - Owl Drawing Art: [The Graphics Fairy](#)

