Cloud, Fog, Edge Security

PROF. DR. SÉRGIO TAKEO KOFUJI

PROF. MS. NORIS JUNIOR

TÓPICOS EM COMPUTAÇÃO EM NUVEM

Agenda

Cloud, Fog, Edge computing security

Vulnerabilidades

Riscos

Privacidade

Validação de dados de entrada

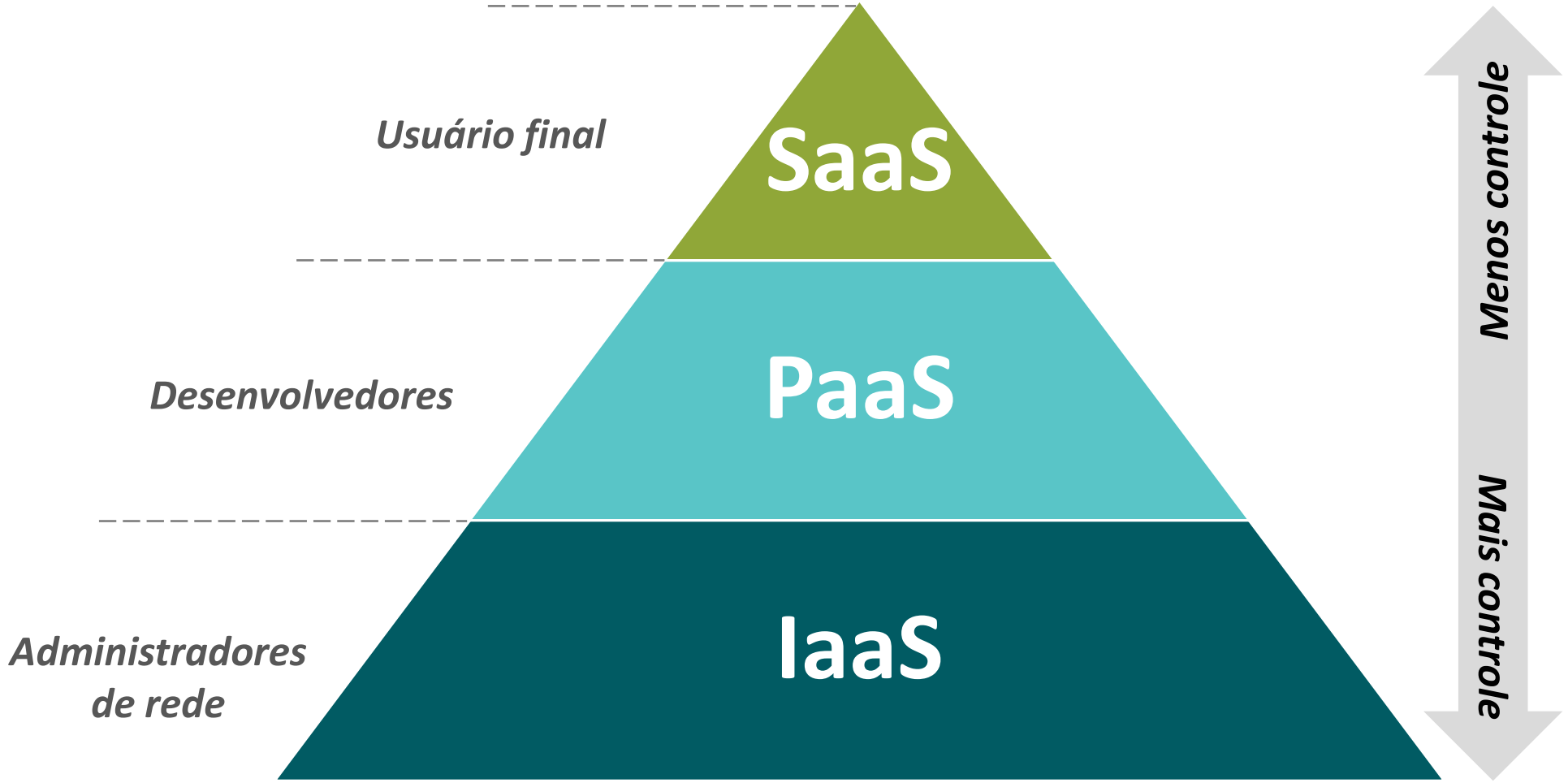
Sec-SLA

Transparência da segurança

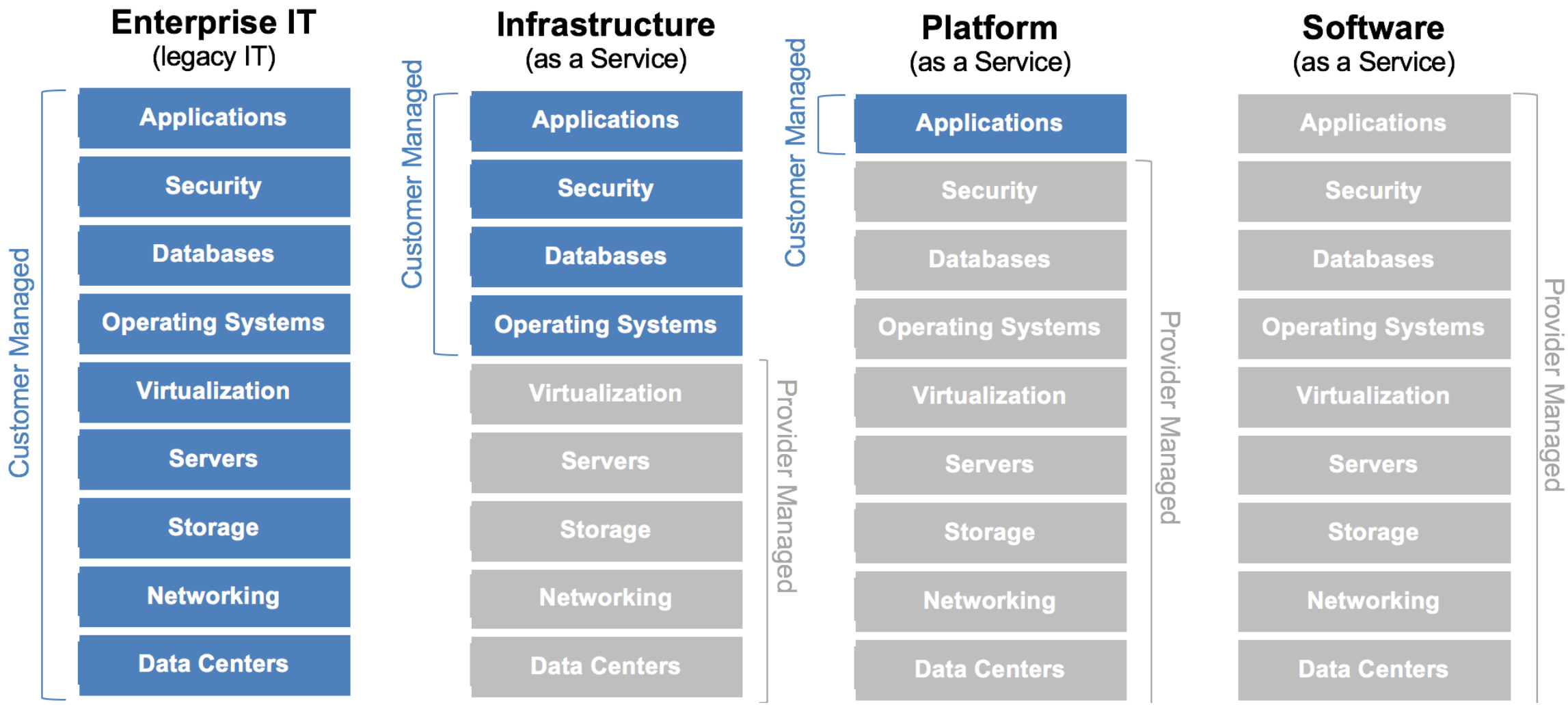
Proteção dos dados

Detecção de Intrusão

Panorama da nuvem



Panorama da nuvem



Múltiplos Stakeholders

Meus dados estão protegidos?

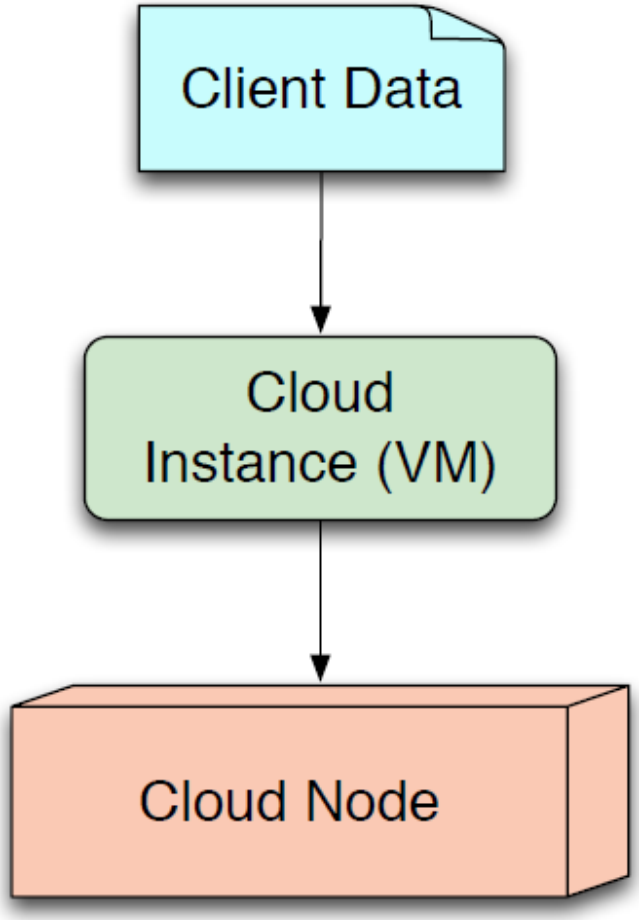
Meus serviços estão executando corretamente?

Minha plataforma é segura?

Clients

Service Providers

Cloud Administrators



Configurações de segurança

Muitas configurações relevantes para instâncias:

- O código do software é o mais atualizado?
- Firewalls
- Controle de acesso obrigatório:
  - SELinux, AppArmor, TrustedBSD, entre outros
- Políticas de aplicações (Banco de Dados, Web Sever)
- Arquivos de configuração das aplicações
- Armazenamento

Vulnerabilidades

Insiders:

- Provedor pode ter boa reputação: seus funcionários também devem

Co-Hosting

Uma instância armazenada na mesma plataforma física pode disparar ataques a outra instância

Instâncias “Co-hosted” compartilham recursos:

- CPU, Cache, Memória, Rede, entre outros

Recursos compartilhados podem ser usados como meio intermediário para aprender informações

Riscos

Conexão constante

- Dependência da conexão, disponibilidade de recursos

Perda da governança

- Alguns processos não são mais realizados pelo cliente (backup)

Aprisionamento na nuvem (a um provedor)

Riscos

Proteção dos dados

- Confidencialidade (roubo, vazamento)
- Integridade (perda, degradação)
- Garantia (os dados ainda funcionam?)

Vulnerabilidades da nuvem

- Dificuldade na integração de serviços e recursos
- Infraestrutura não preparada para compartilhamento
- Sequestro de conta (phishing, MITM)

Privacidade

Paravirtualização (modificação do kernel do SO para instruções de CPU e I/O)

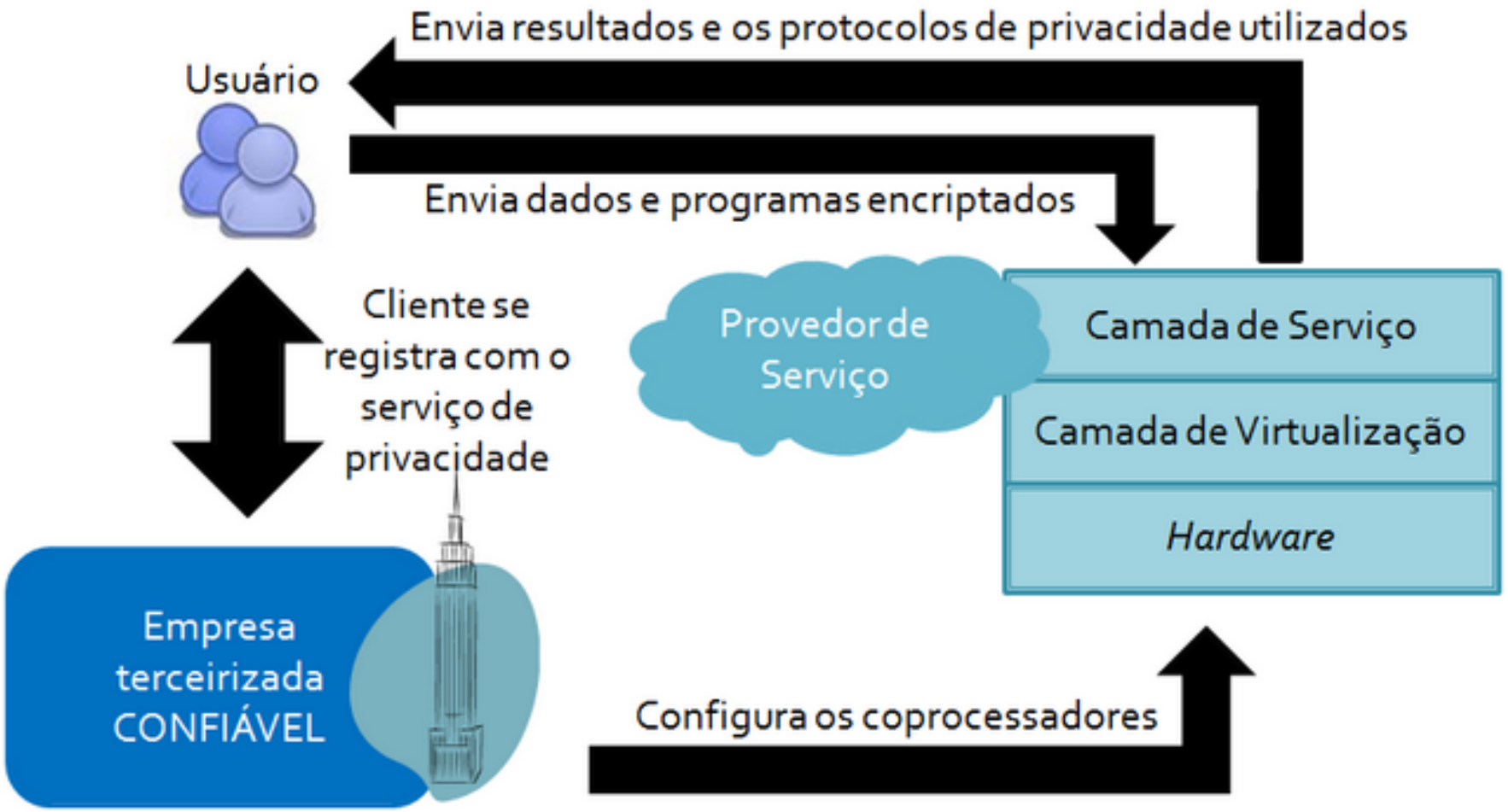
Cifração (lentidão)

Arquitetura para separar a execução dos aplicativos (segregação de processamento e memória)

Tamper -proof (evita violação física)

Privacy as a Service

Privacidade



Negação de Serviço

Lentidão

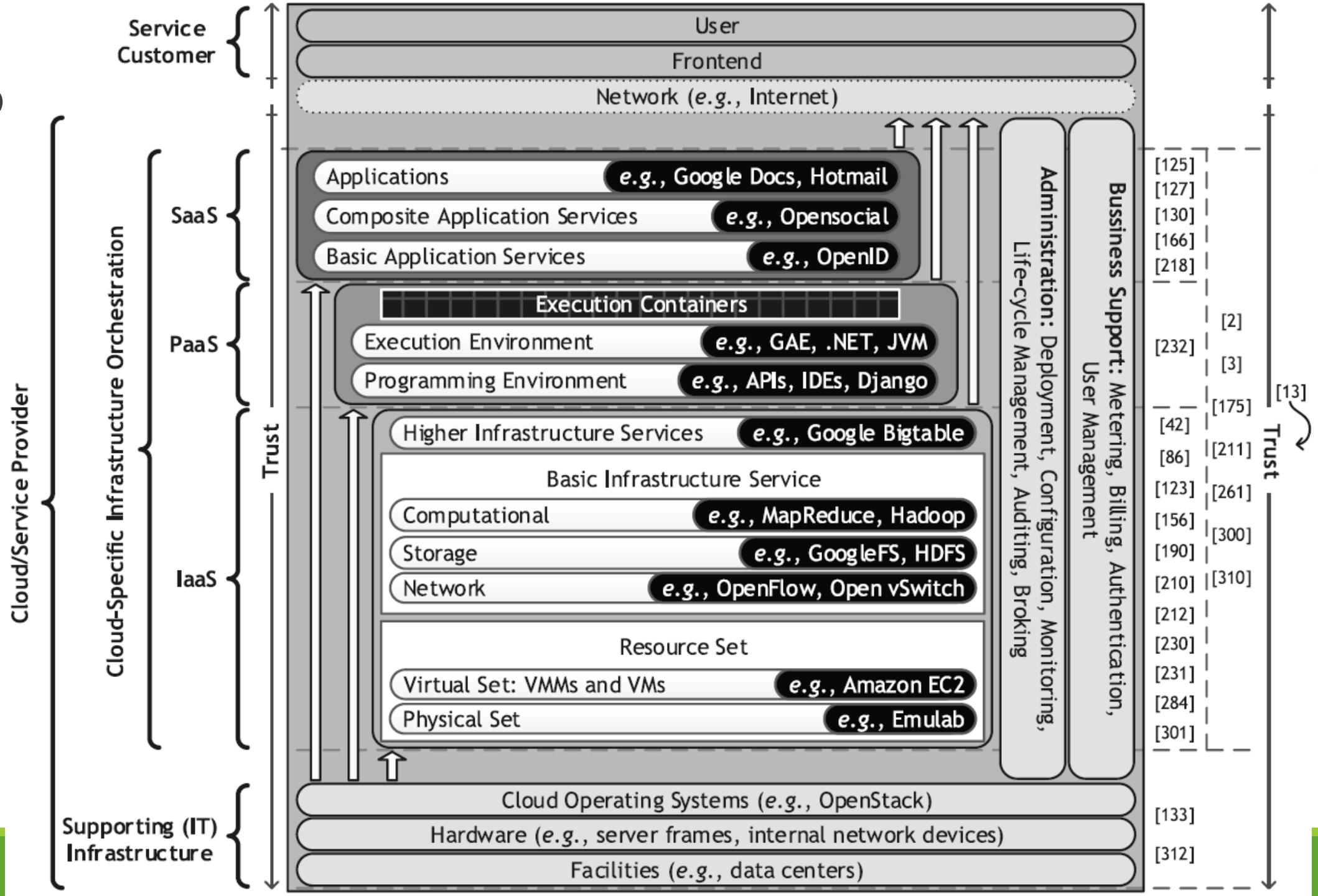
Indisponibilidade

DDoS (2016 - DynDNS)

Difícil solução:

- Técnicas de filtragem
- Redundância
- Monitoramento

P


Service Customer
User
Frontend
Network (e.g., Internet)
Cloud/Service Provider
Cloud-Specific Infrastructure Orchestration
SaaS
Applications
e.g., Google Docs, Hotmail
Composite Application Services
e.g., Opensocial
Basic Application Services
e.g., OpenID
PaaS
Execution Containers
Execution Environment
e.g., GAE, .NET, JVM
Programming Environment
e.g., APIs, IDEs, Django
IaaS
Higher Infrastructure Services
e.g., Google Bigtable
Basic Infrastructure Service
Computational
e.g., MapReduce, Hadoop
Storage
e.g., GoogleFS, HDFS
Network
e.g., OpenFlow, Open vSwitch
Resource Set
Virtual Set: VMMs and VMs
e.g., Amazon EC2
Physical Set
e.g., Emulab
Trust
Administration: Deployment, Configuration, Monitoring, Life-cycle Management, Auditing, Broking
Bussiness Support: Metering, Billing, Authentication, User Management
Supporting (IT) Infrastructure
Cloud Operating Systems (e.g., OpenStack)
Hardware (e.g., server frames, internal network devices)
Facilities (e.g., data centers)
[125]
[127]
[130]
[166]
[218]
[2]
[232]
[3]
[175]
[42]
[211]
[86]
[261]
[123]
[156]
[300]
[190]
[310]
[210]
[212]
[230]
[231]
[284]
[301]
[133]
[312]
[13]
Trust

Monitoramento e controle da segurança

Alto poder de processamento

Computação paralela multi-nível

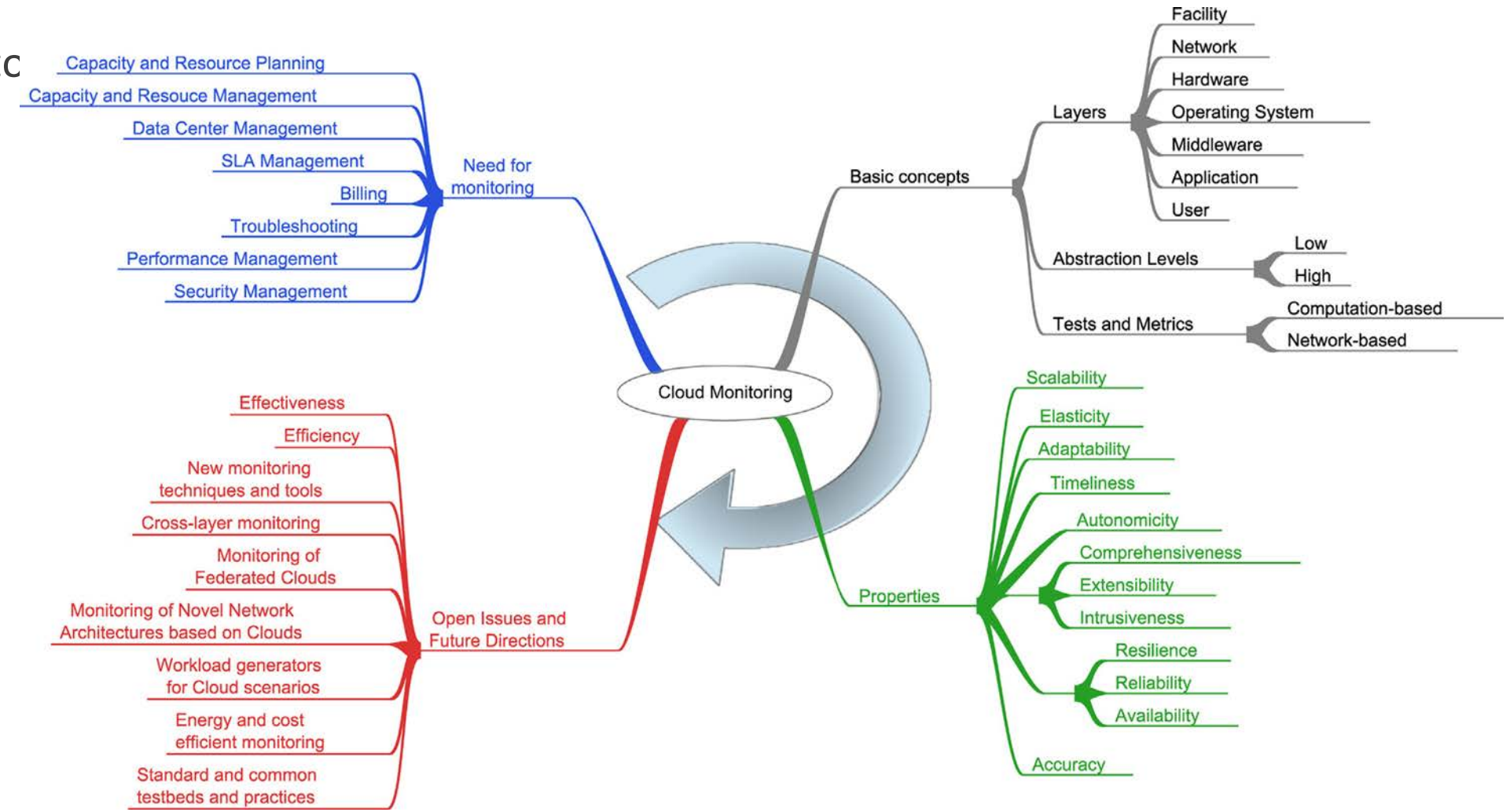
- Alternativa para aumentar o poder de processamento atual
  - Arquiteturas multicore
  - Multiprocessadores
  - Clusters de desempenho
  - Grids

Novos conceitos de serviços

Novas formas de controle e monitoramento de segurança

Monitoramento e controle da segurança

Monitc



Validação de dados na entrada

Aplicações WEB estão sujeitas a:

- Ataques que manipulam a entrada de dados:
  - Campos não validados na URL
  - Injeção de SQL
  - Manipulação por meio de campos ocultos

Proposta: **A Security Framework for Input Validation**

- Validação dos campos de entrada: documento XML
- XML define campos e entradas válidas
- Opera do lado servidor - todas as entradas são validadas

Validação de dados na entrada

Prós:

- Fácil reconfiguração
- Permite padronizar entradas
- Funciona para aplicações WEB e WEB Services

Contras:

- Ponto único de validação (e ponto único de falhas)
- Não impede ataques do lado do usuário

Security Service Level Agreements

Sec-SLA

Essencial no relacionamento Provedor x Cliente x Nuvem

Contratos definem a prestação de serviços provedor x cliente

Nível de segurança do serviço entregue é essencial:

- Melhor entendimento da função de segurança

Service Level Security Agreement

Proposta: SLA Perspective in Security Management for Cloud Computing

Sec-SLA depende de:

- Técnicas de prevenção de ataques

- Ferramentas computacionais:
  - Criptografia
  - Filtragem
  - Redundância
  - Monitoramento:
    - Métricas estão sendo cumpridas?
    - Arquitetura segurança-monitoramento é independente da tecnologia

Service Level Security Agreement

Desafios na definição das métricas usadas:

- Definir exatamente os pontos que requerem segurança
- A negociação do SLA precisa ser ágil para não atrasar a entrega de serviços

Segurança do cliente

Vulnerabilidades que usuários apontam no ambiente em nuvem

- Vulnerável à ataques
- Práticas de segurança padrão
- Garantia de confidencialidade quebrada por força de Lei

Segurança do cliente

Proposta: **Customer Security Concerns in Cloud Computing**

- Condições de segurança na escolha de um provedor de nuvem:
  - Acesso privilegiado a usuários
  - Regulamentação padronizada
  - Local de armazenamento dos dados
  - Esquema de segregação dos dados
  - Esquema de recuperação
  - Auditoria (forense investigativa)
  - Viabilidade de longo prazo

Transparência da segurança

Estado atual da segurança

- Transparência de segurança entre Provedor x Cliente
- SaaS: há dúvidas de clientes sobre a falta de informação de como os dos dados são armazenados e se há segurança (além da preocupação com insiders)
- IaaS: segurança com firewall e load balancing
- PaaS: Malware as a Service

1 Uso abusivo da nuvem

2 Interfaces e API's inseguras

3 Insider malicioso

4 Compartilhamento de tecnologia

5 Vazamento de dados

6 Sequestro de contas ou serviços

7 Perfil de segurança desconhecido

Transparência da segurança

1 Uso abusivo da nuvem

- Amazon Zeus botnet

2 Interfaces e API’s inseguras

- Provedores expõem aos clientes:
  - Recursos disponíveis dos seus componentes
  - Permitem aos clientes arquitetar em conjunto nova API

Transparência da segurança

3-5 Segurança de dados

- Relacionados à falta de Confidencialidade, Integridade, Disponibilidade

6 Sequestro de contas ou serviços

- Permitem fraudes
- Vulnerabilidade em um cliente pode liberar acesso a outro

7 Perfil de segurança desconhecido

- Múltiplos clientes aumentam complexidade

Transparência da segurança

Proposta: Security Transparency and Mutual Audit (STMA)

1 Ranking de provedores de serviços

- Fornecer uniformidade de checklists de segurança, benchmarks e outras configurações
- Ferramentas para definição de eventos atômicos

2 Prover arquitetura em nuvem baseada no STMA

- Detecção de eventos atômicos (por sistema multi-agente)
- Definir em contrato quais informações pode ser compartilhada entre provedor x cliente
- Padrões de eventos de segurança podem ser definidos por cliente e provedor

Transparência da segurança

Proposta: Security Transparency and Mutual Audit (STMA)

3 Projeto e método para forçar a transparência da segurança e auditoria mútua

- Continuamente obter evidências para apoiar a segurança
- Compartilhar os eventos de segurança com o cliente

Proteção dos dados em nuvem

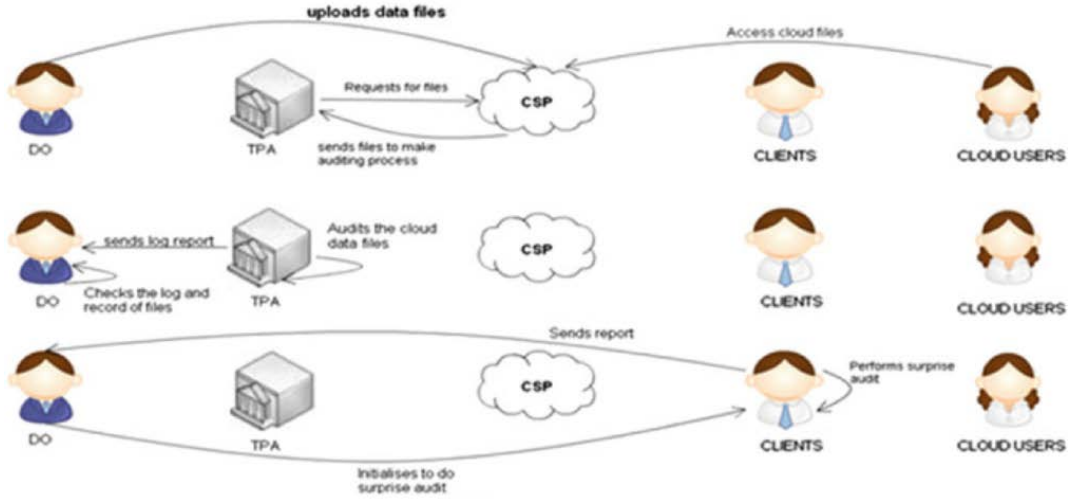
Além das vulnerabilidades anteriormente apresentadas:

- Ataque VM side-channel
- Ataque na VM modelo
- Escape de um atacante da VM para o hypervisor
- Exposição de dados na transição (migração/movimentação) de VM

Proteção dos dados em nuvem

Protegendo a integridade dos dados:

- Caso os dados sejam enviados cifrados para a nuvem: a segurança é suficiente?
  - Não há proteção contra dados corrompidos, erros de config, bug de sw
- Provar a integridade:
  - Auditoria externa confere a integridade



Proteção dos dados em nuvem

Prova da posse dos dados:

- Mensagem (tag usando RSA) enviada pela máquina verificada pelo cliente (prova estatística da presença dos dados) – prova que o servidor tem aquele trecho de dados

Prova de recuperabilidade:

- Cliente usa chave para gerar hash antes de enviar arquivos à nuvem
- Conferência: cliente envia chave, servidor gera hash, cliente confere hash

Proteção dos dados em nuvem

Confidencialidade:

- Dados criptografados antes de enviar: uma única chave compartilhada para administração (distribuída a um grupo de usuários)
- Sistema criptográfico de compartilhamento de chaves:
  - Proprietário tem uma chave mestra, que gera outras chaves
  - Usuário ou grupo com chave derivada somente enxerga a parte que lhe cabe

Proteção dos dados em nuvem

Confidencialidade:

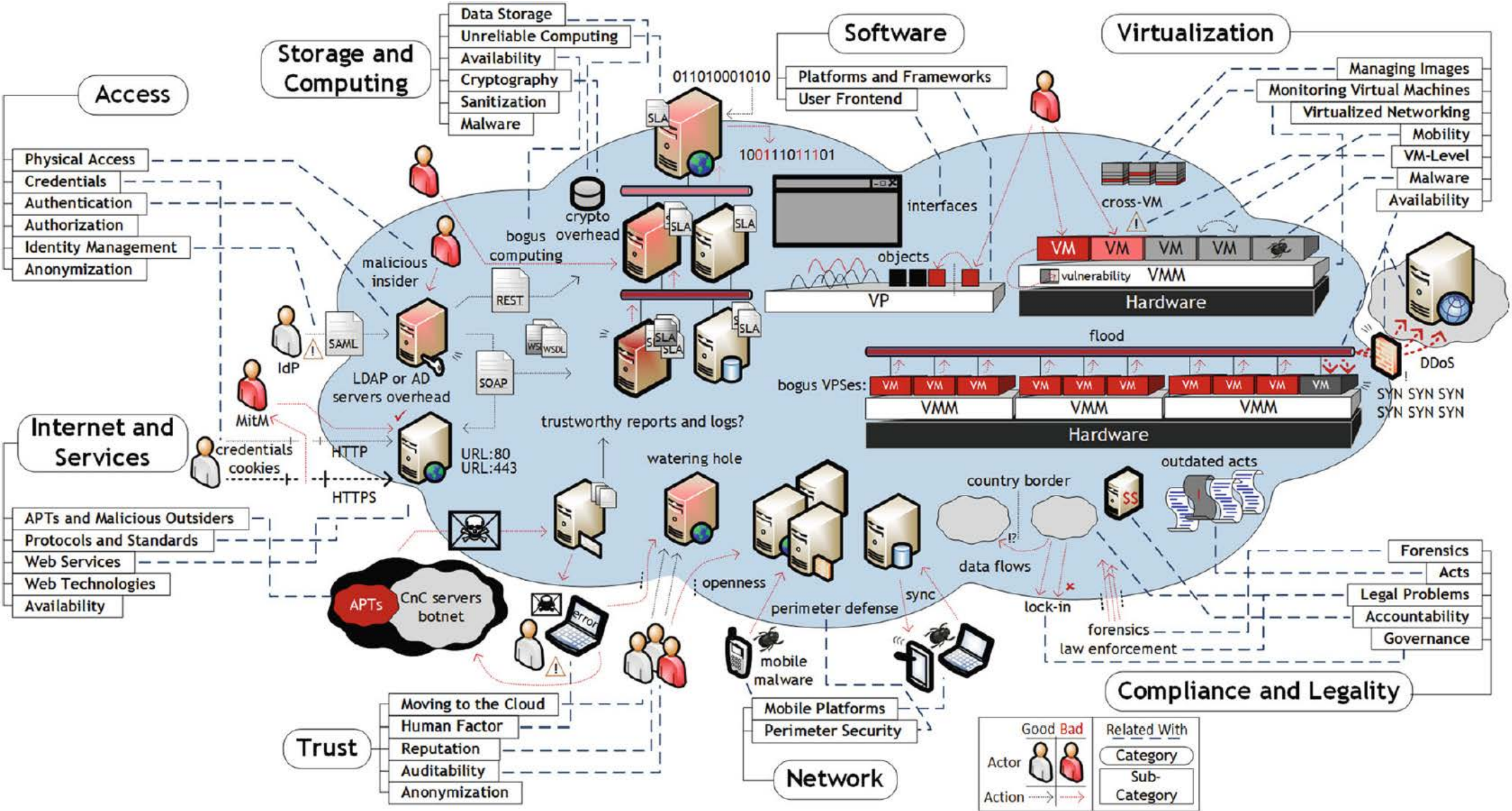
- Dados criptografados antes de enviar: uma única chave compartilhada para administração (distribuída a um grupo de usuários)

- Sistema criptográfico de compartilhamento de chaves:
  - Proprietário tem uma chave mestra, que gera outras chaves
  - Usuário ou grupo com chave derivada somente enxerga a parte que lhe cabe

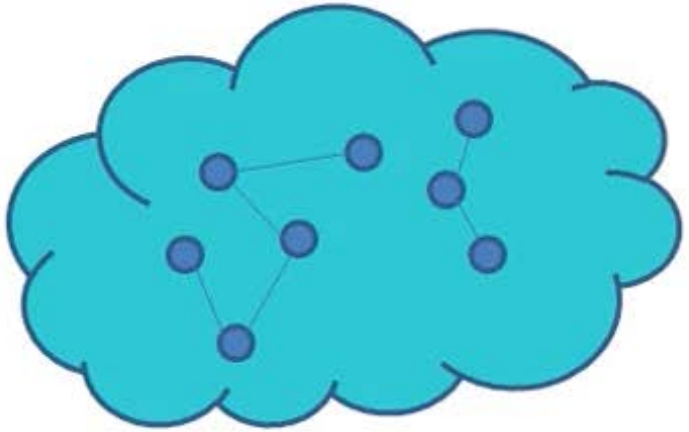
Proteção dos dados em nuvem

Multi-cloud

- Um provedor: ponto único de falha
- Múltiplos provedores: altíssima disponibilidade e tolerância à falhas
- Como alinhar confiança, confiabilidade e segurança entre múltiplos provedores?

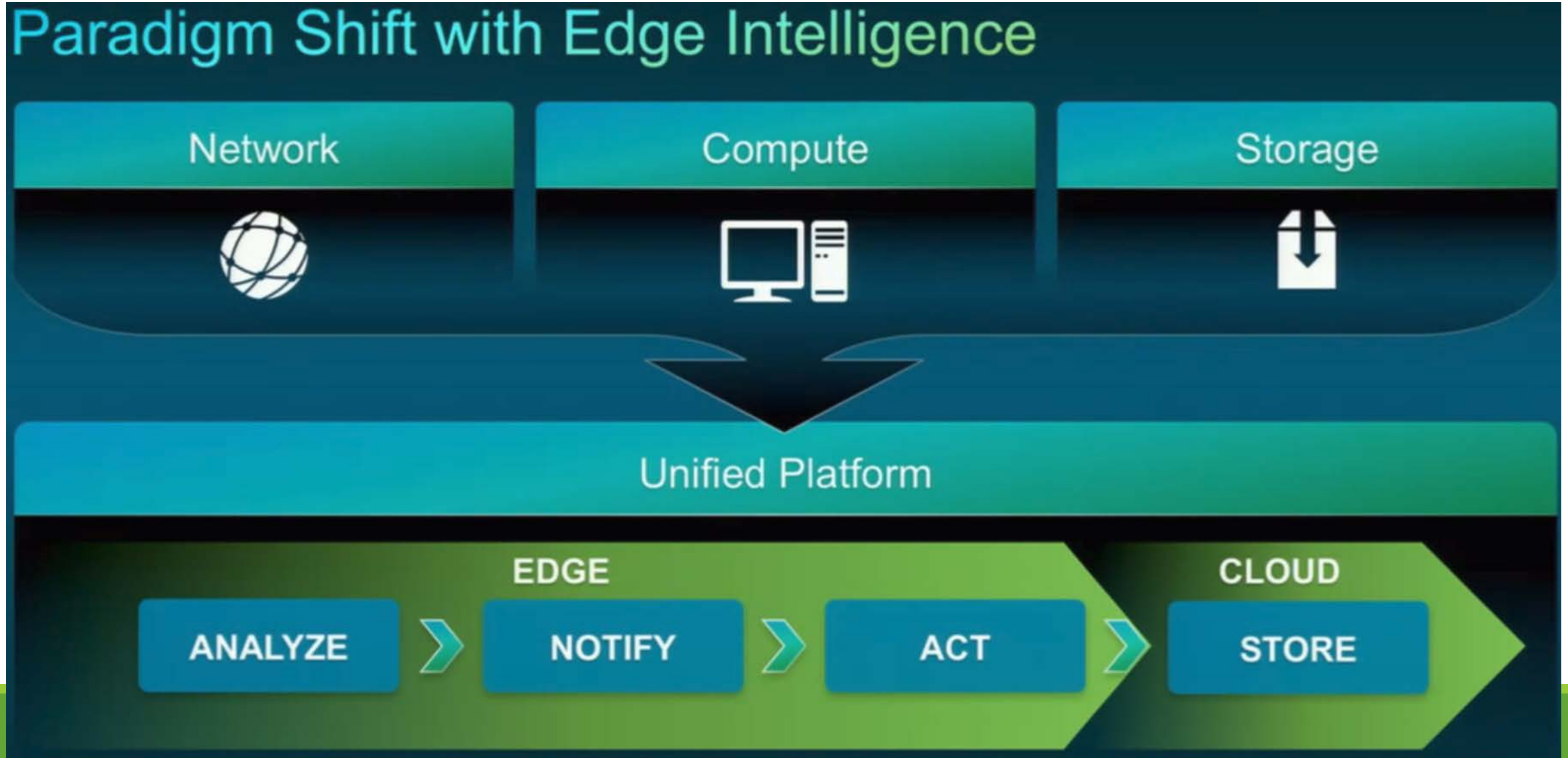

Access
Physical Access
Credentials
Authentication
Authorization
Identity Management
Anonymization
Storage and Computing
Data Storage
Unreliable Computing
Availability
Cryptography
Sanitization
Malware
Software
Platforms and Frameworks
User Frontend
Virtualization
Managing Images
Monitoring Virtual Machines
Virtualized Networking
Mobility
VM-Level
Malware
Availability
011010001010
100111011101
SLA
crypto overhead
bogus computing
malicious insider
REST
WSDL
SOAP
SAML
IdP
MitM
LDAP or AD servers overhead
interfaces
objects
VP
cross-VM
VM
vulnerability
VMM
Hardware
flood
bogus VPSes:
DDoS
SYN SYN SYN
SYN SYN SYN
Internet and Services
credentials
cookies
HTTP
HTTPS
URL:80
URL:443
trustworthy reports and logs?
watering hole
outdated acts
country border
SS
data flows
lock-in
forensics
law enforcement
APTs and Malicious Outsiders
Protocols and Standards
Web Services
Web Technologies
Availability
APTs
CnC servers
botnet
error
openness
perimeter defense
sync
mobile
malware
Forensics
Acts
Legal Problems
Accountability
Governance
Compliance and Legality
Trust
Moving to the Cloud
Human Factor
Reputation
Auditability
Anonymization
Mobile Platforms
Perimeter Security
Network
Good Bad
Related With
Actor
Action
Category
Sub-Category

Fog



Smart Homes

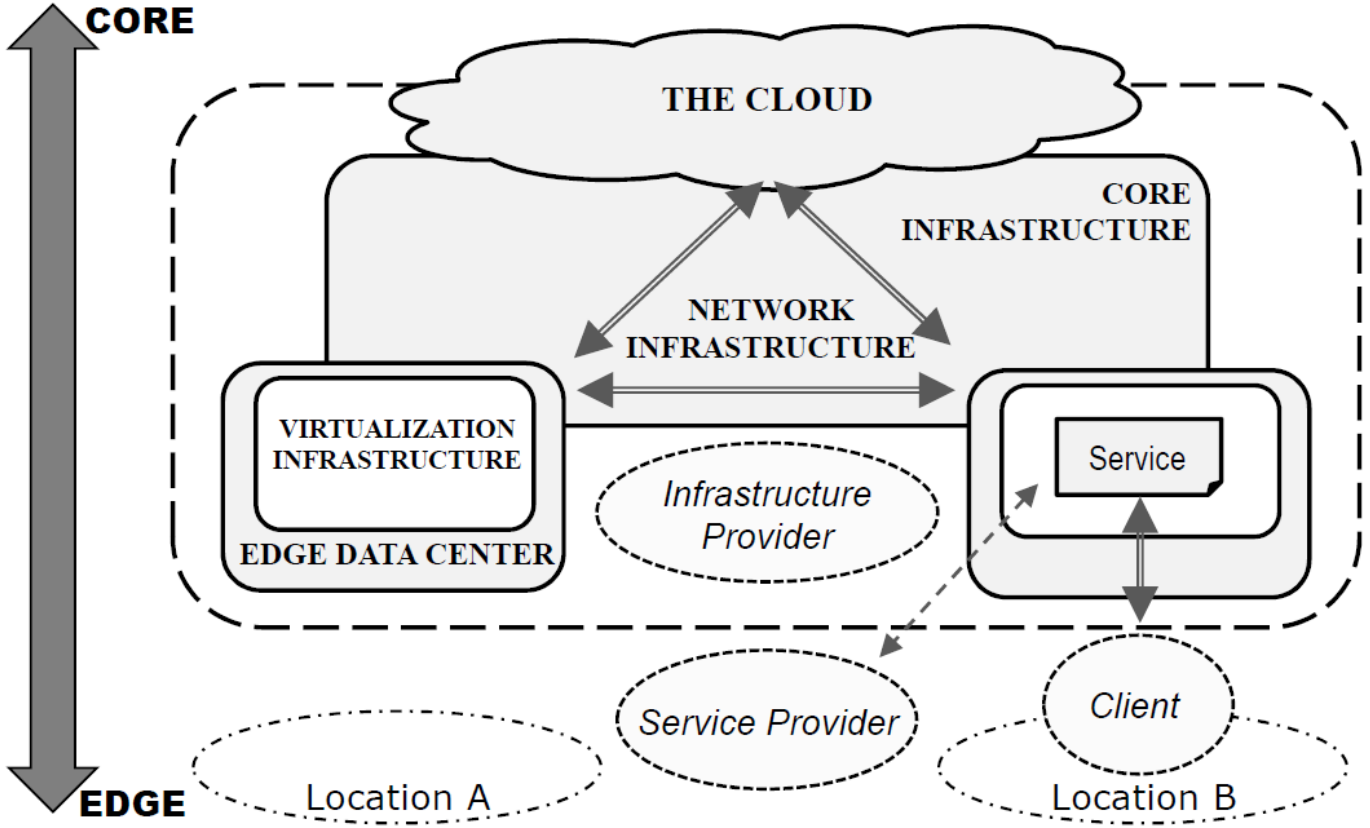
Fog e Edge


Paradigm Shift with Edge Intelligence
Network
Compute
Storage
Unified Platform
EDGE
CLOUD
ANALYZE
NOTIFY
ACT
STORE

Segurança em Mobile Edge, Cloud, Fog

Cloud na extremidade:

- Edge data centers comunicam-se entre si e com a nuvem



Segurança em Mobile Edge, Cloud, Fog

Fog: plataforma que habilita a criação de novas aplicações e serviços no contexto IoT

- Smart cities, processamento de dados de bilhões de dispositivos
- Tolerantes à alta latência (oposto da cloud)
- Fog servers colaboram entre si: drones, estações rádio-base, servidores, etc.
- API para diferentes máquinas (VMs também) acessarem estatísticas de rede, dados de dispositivos IoT, entre outros

Segurança em Mobile Edge, Cloud, Fog

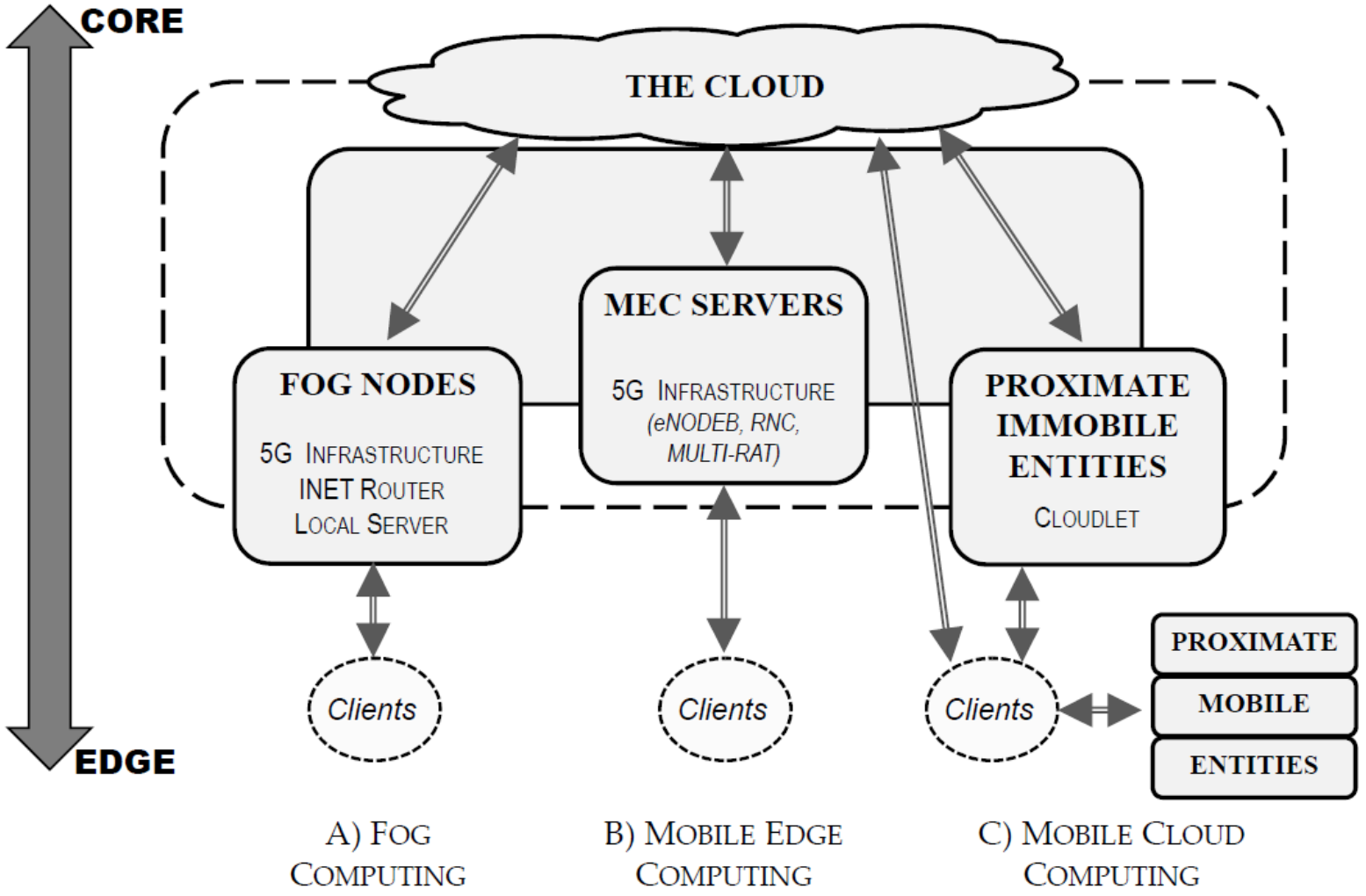
Mobile Edge: execução de aplicações em estação rádio-base móveis

- Capacidades da cloud para a extremidade das redes móveis (3G, LTE, 5G)

Mobile Cloud:

- Tarefas como armazenamento e processamento delegadas para serviços na borda da rede (servidor de pesquisa de voz comunicando-se com aplicativos – text-to-speech)
- Migração de parte do código da aplicação para a borda

Segurança em Mobile Edge, Cloud, Fog



Segurança em Mobile Edge, Cloud, Fog

Identidade e autenticação

Sistemas de controle de acesso

Segurança na rede e seus protocolos

Gerenciamento da confiança (trust)

Sistemas de Detecção de Intrusão

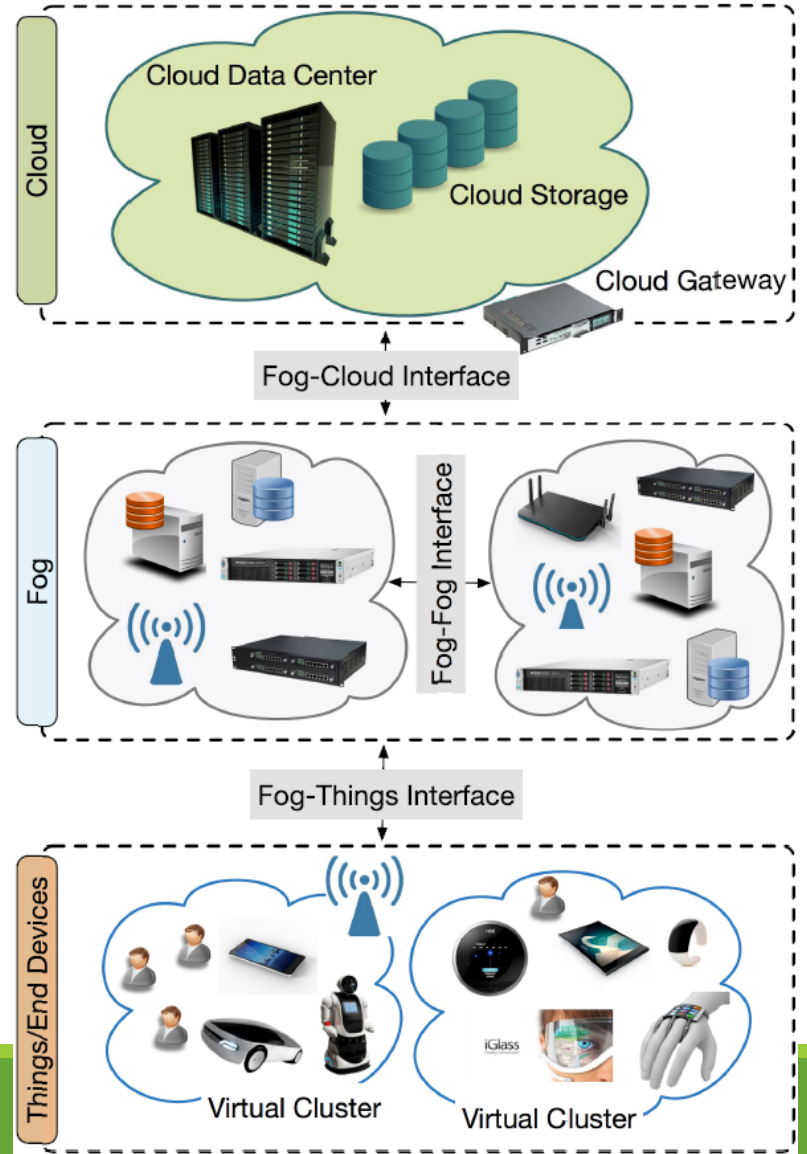
Privacidade

Virtualização

Segurança e privacidade em Fog

Edge: cada componente executa seu papel de processar dados localmente

Fog: nós da Fog decidem se processam com seus recursos ou se enviam à cloud



Segurança e privacidade em Fog

Desafios de pesquisa

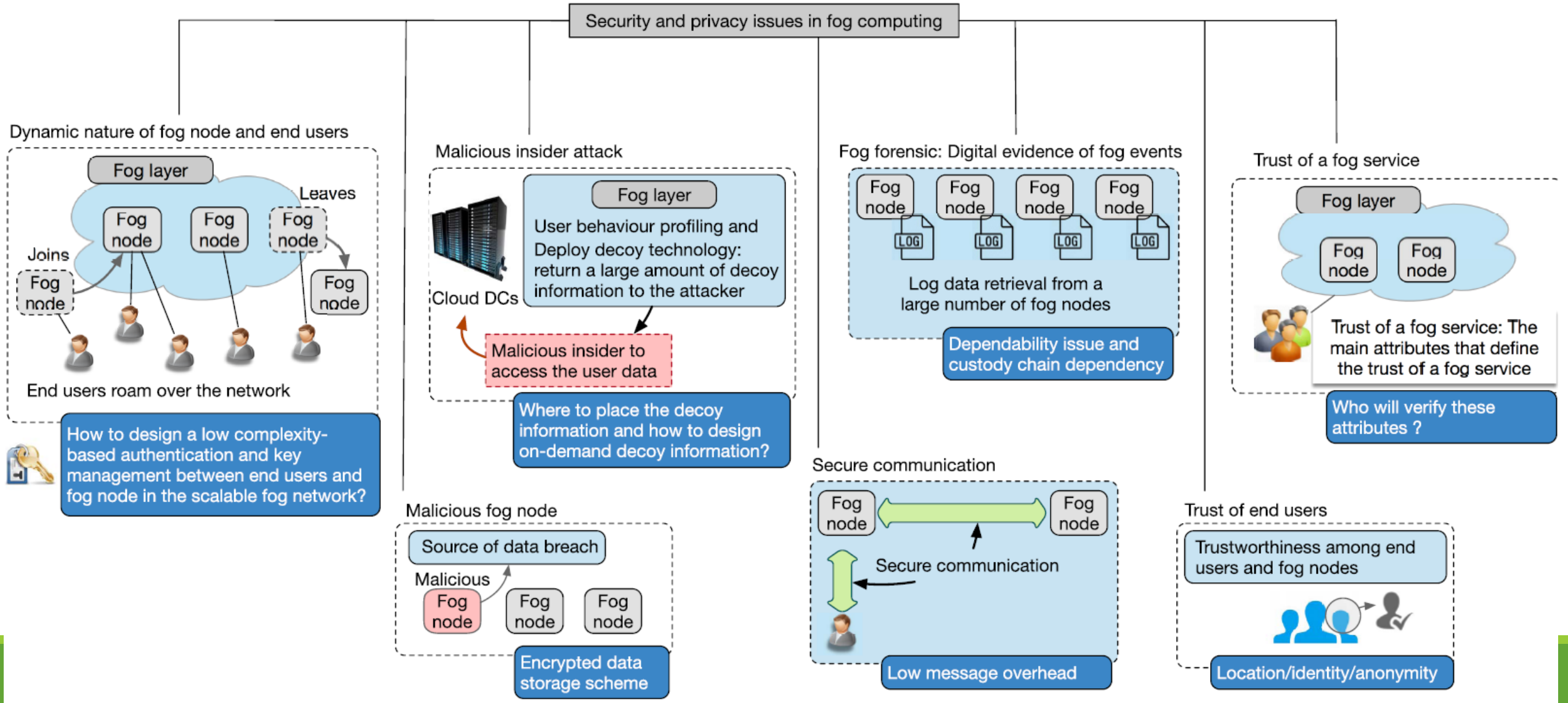
- Confiança (trust)
  - Em cloud, a comunicação é em uma direção (southbound). Em Fog há também northbound
  - Relacionamento de confiança com a cloud e com os dispositivos/clientes
- Privacidade
- Autenticação e troca de chaves
  - Lightweight (dispositivos não são potentes)
  - Fim-a-fim

Segurança e privacidade em Fog

Desafios de pesquisa

- SDI
  - Análise de comportamento dos nós Fog e de quem se conecta (dispositivos e servidores da nuvem)
- Ingresso e saída de nó Fog
  - Como: (a) nós Fog se autenticam; (b) usuários se autenticam em novo nó; (b) preservar a identidade do usuário em nó que saiu da Fog
- Computação forense em Fog
  - Necessidade de legislação nacional e internacional

Segurança e privacidade em Fog



Sistemas de Detecção de Intrusão (SDI)

Atualmente limitada para Grid computing

Essenciais, mas não infalíveis (falsos positivos e negativos)

Requisitos:

- Cobertura (alcance a todos os nós/rede)
- Escalabilidade
- Compatibilidade

Proposta: Intrusion Detection for Computational Grids

Sistemas de Detecção de Intrusão (SDI)

Proposta: Intrusion Detection for Computational Grids

- Sistema instalado em nós específicos ou domínios
- Trabalha integrado ao SDI
- Reutiliza as funcionalidades do SDI em baixo e alto nível
- Cada nó ou domínio deve ter um SDI de baixo nível instalado
- Auditores procuram e analisam por anomalias na rede para identificar evidência de ataques

Um administrador de rede é alertado quando há detecção de intrusão

Agentes compartilham informações para analisar comportamentos e atualizar perfis de máquinas

Sistemas de Detecção de Intrusão (SDI)

Requisitos de segurança em sistemas distribuídos de nuvens (ideal):

- Autenticação com senhas e certificado digital não é suficiente
- Confidencialidade nas transmissões
- Controle das tarefas executadas
- Prevenir acesso e uso não autorizado
- Detecção rápida de ataques conhecidos

Sistemas de Detecção de Intrusão (SDI)

Proposta: Intrusion Detection for Grid and Cloud Computing

- Detecção de intrusão aplicada na coleta de dados entre o cliente e a nuvem
- Análise por anomalia para verificar a ação de usuários
- Auditoria sobre a violação de políticas de segurança
- Auditoria sobre a quebra em padrões de ataques conhecidos

IDS precisa ser compartilhado pelos nós

- Cada nó monitorado avisa os outros nós em caso de ataque
- Porém, ataques podem ser silenciosos ou encriptados

Sistemas de Detecção de Intrusão (SDI)

Cloud Computing Intrusion Detection Systems (CCIDS)

- Arquitetura que realiza detecção na rede e nos hosts
- Age no middleware (entre o usuário e a nuvem)
- Rede neural correlaciona dados de múltiplas fontes (registro, serviços, nós)
- SDI baseado no comportamento do usuário + BD de ataques
- Análise do BD do SDI mantida em storages
- Baixo custo de processamento
- Tempo real

FIWARE

Generic Enablers (GE)

Security GE:

- Identity Management (IdM) – KeyRock (SSO)
  - Atributos
  - Usuários existentes, ativos, entre outros
  - Localização
  - Histórico
  - Autenticação de usuários e dispositivos IoT

FIWARE

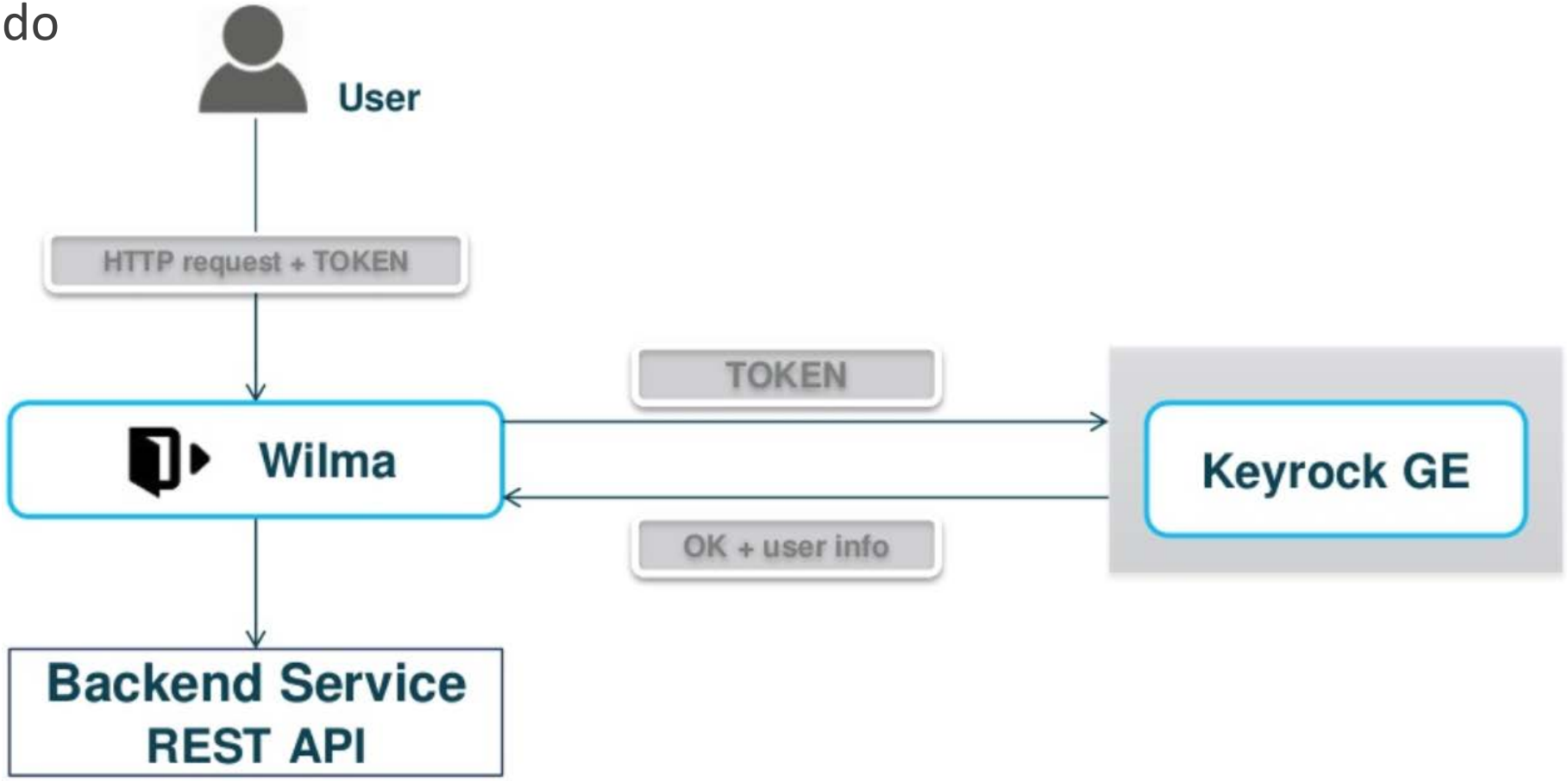
Generic Enablers (GE)

Security GE:

- Policy Enforcement Proxy (PEP) – Wilma:
  - Controla o acesso aos recursos
  - Requisitante deve usar token (temporalidade do acesso) – requisição feita ao IdM

FIWARE

Acesso identificado



FIWARE

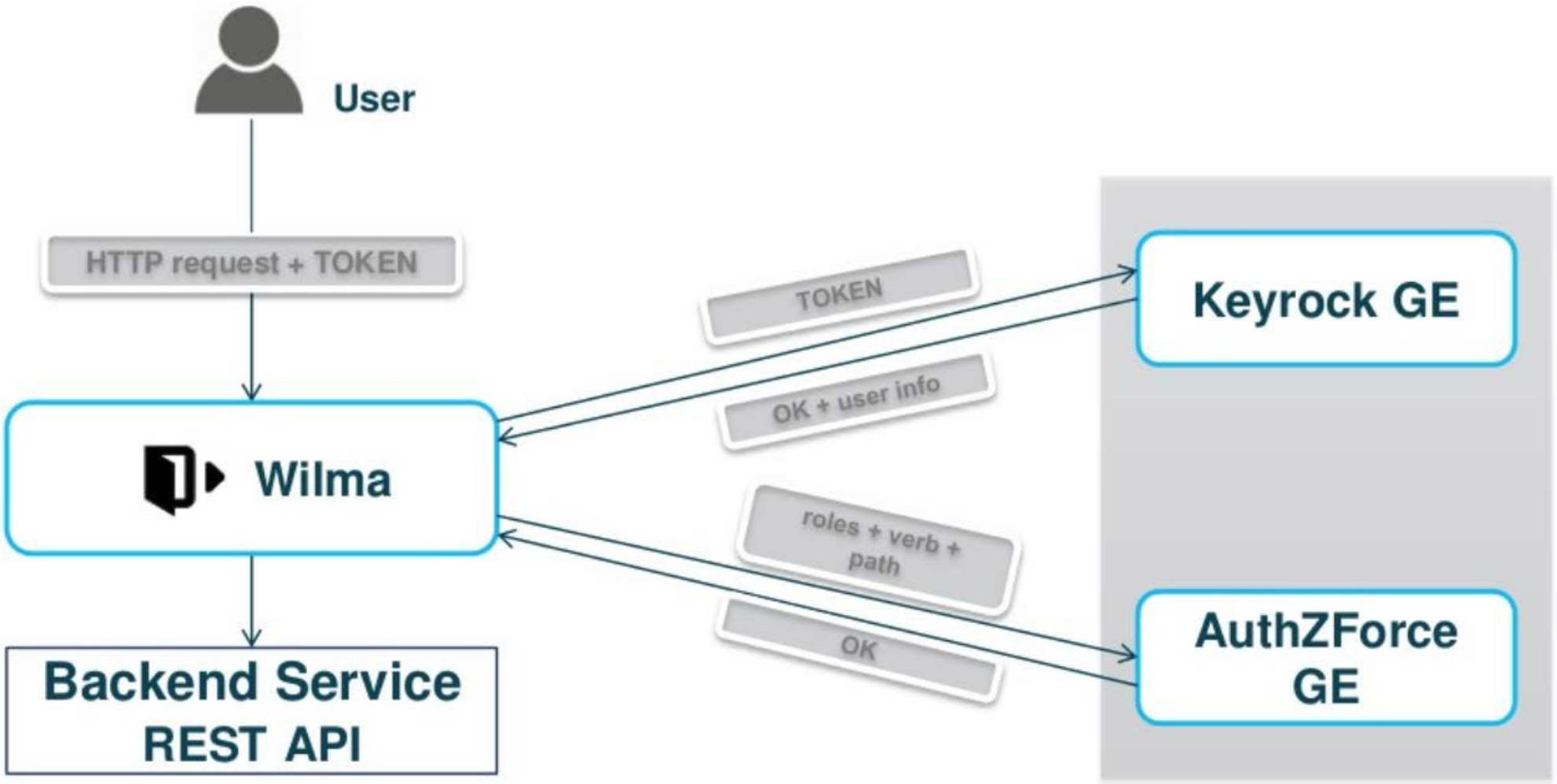
Generic Enablers (GE)

Security GE:

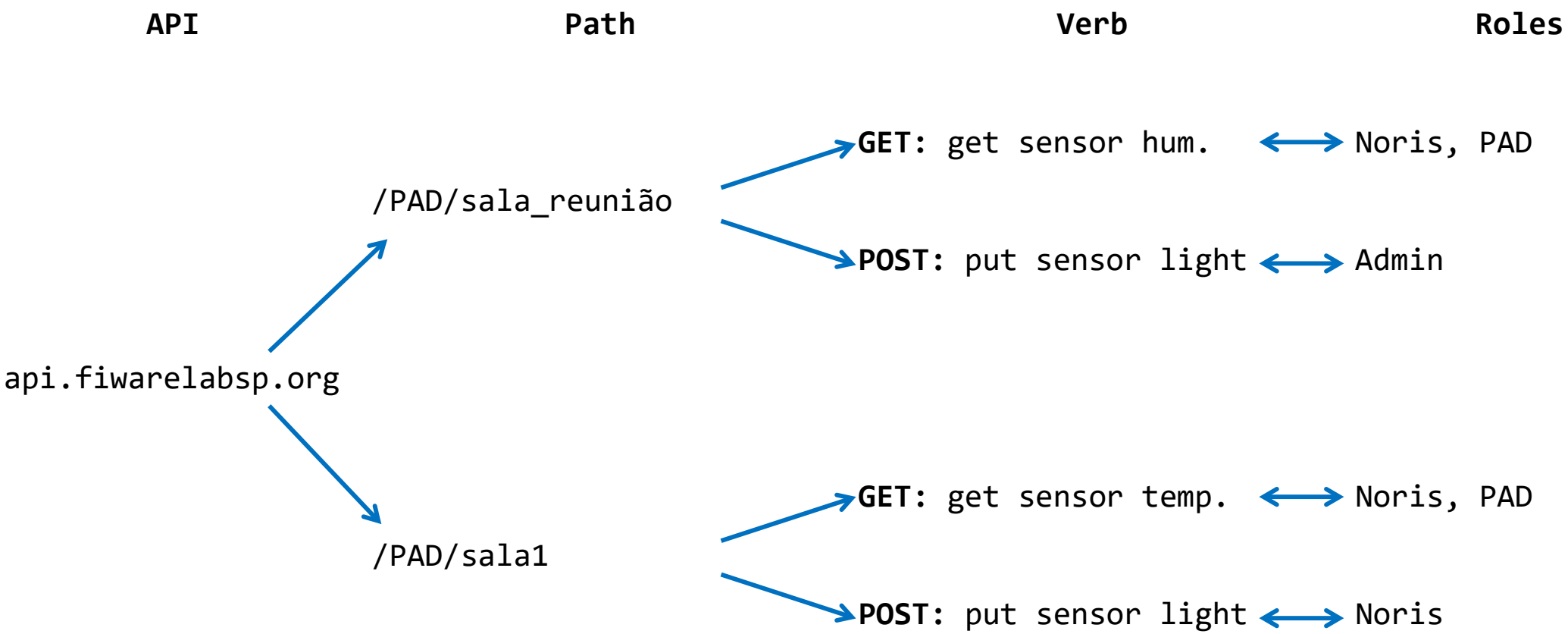
- Policy Administration Point (PAP) e Policy Decision Point (PDP) - AuthZForce

Autenticação usando 3 fatores: SSO + token + políticas de acesso

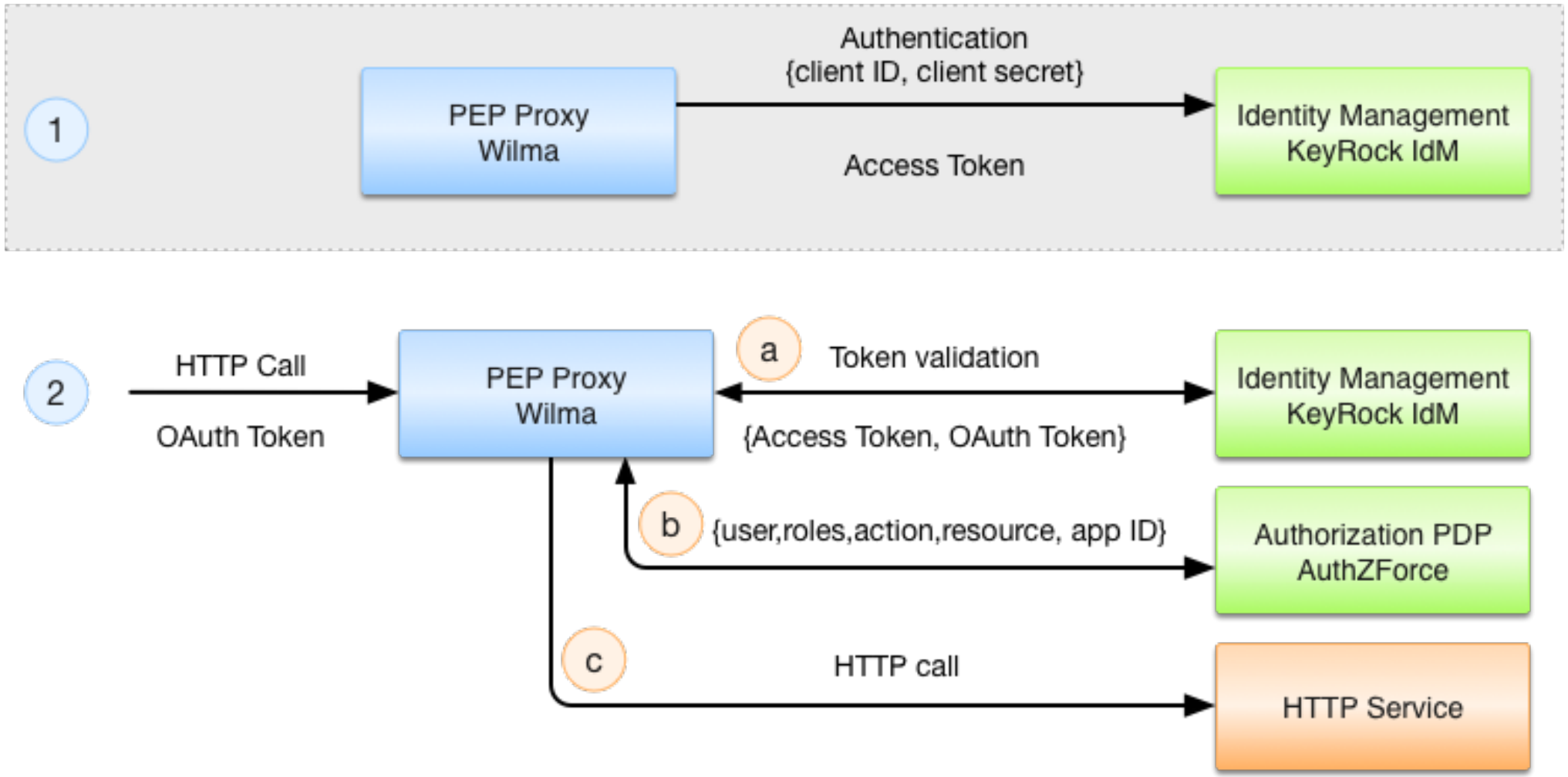
FIWARE


User
HTTP request + TOKEN
Wilma
Backend Service
REST API
TOKEN
OK + user info
roles + verb + path
OK
Keyrock GE
AuthZForce GE

FIWARE


API
Path
Verb
Roles
api.fiwarelabsp.org
/PAD/sala_reunião
/PAD/sala1
GET: get sensor hum.
POST: put sensor light
GET: get sensor temp.
POST: put sensor light
Noris, PAD
Admin
Noris, PAD
Noris

FIWARE


1
PEP Proxy
Wilma
Authentication
{client ID, client secret}
Access Token
Identity Management
KeyRock IdM
2
HTTP Call
OAuth Token
PEP Proxy
Wilma
a
Token validation
{Access Token, OAuth Token}
Identity Management
KeyRock IdM
b
{user,roles,action,resource, app ID}
Authorization PDP
AuthZForce
c
HTTP call
HTTP Service

FIWARE

Segurança com autenticação usando 3 fatores: SSO + token + políticas de acesso

Bibliografia

Fernandes, D. A. B. et al. **Security issues in cloud environments: a survey**. International Journal of Information Security, 2013.

Ouedraogo, M. et al. **Security transparency: the next frontier for security research in the cloud**, Journal of Cloud Computing: Advances, Systems and Applications, 2015

Aldossary, S., Allen, W. **Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions**, (IJACSA) International Journal of Advanced Computer Science and Applications, 2016

Roman, R., Lopez, J., Mambo, M. **Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges**, Future Generation Computer Systems, 2016

Mukherjee, M. et al. **Security and Privacy in Fog Computing: Challenges**, IEEE Access, 2017

Barreto, L. et al. **Identity Management in IoT Clouds: a FIWARE Case of Study**, 1st Workshop on Security and Privacy in the Cloud (SPC), 2015.

Alonso, A. et al. **IAACaaS: IoT Application-Scoped Access Control as a Service**, Future Internet, 2017.

G. Aceto, A. Botta, W. Donato, A. Pescapè. **Cloud monitoring: A survey**. Computer Networks Journal – Elsevier – 2013 – Italy – 23 p.

C. B. Westphall, C. O. Rolim. Slides of **Management and Security for Grid, Cloud and Cognitive Networks**. Universidade Federal de Santa Catarina – Brasil – 2012. 53 pp.

Notas de aula do Prof. Dr. Anderson A. A. Silva e Prof. Dr. Adilson E. Guelfi