

# No More Dark Clouds With PaaSword – An Innovative Security By Design Framework



# PaaSword

*Cloud Forward Conference  
Oct 18-20, 2016 – Madrid, Spain*

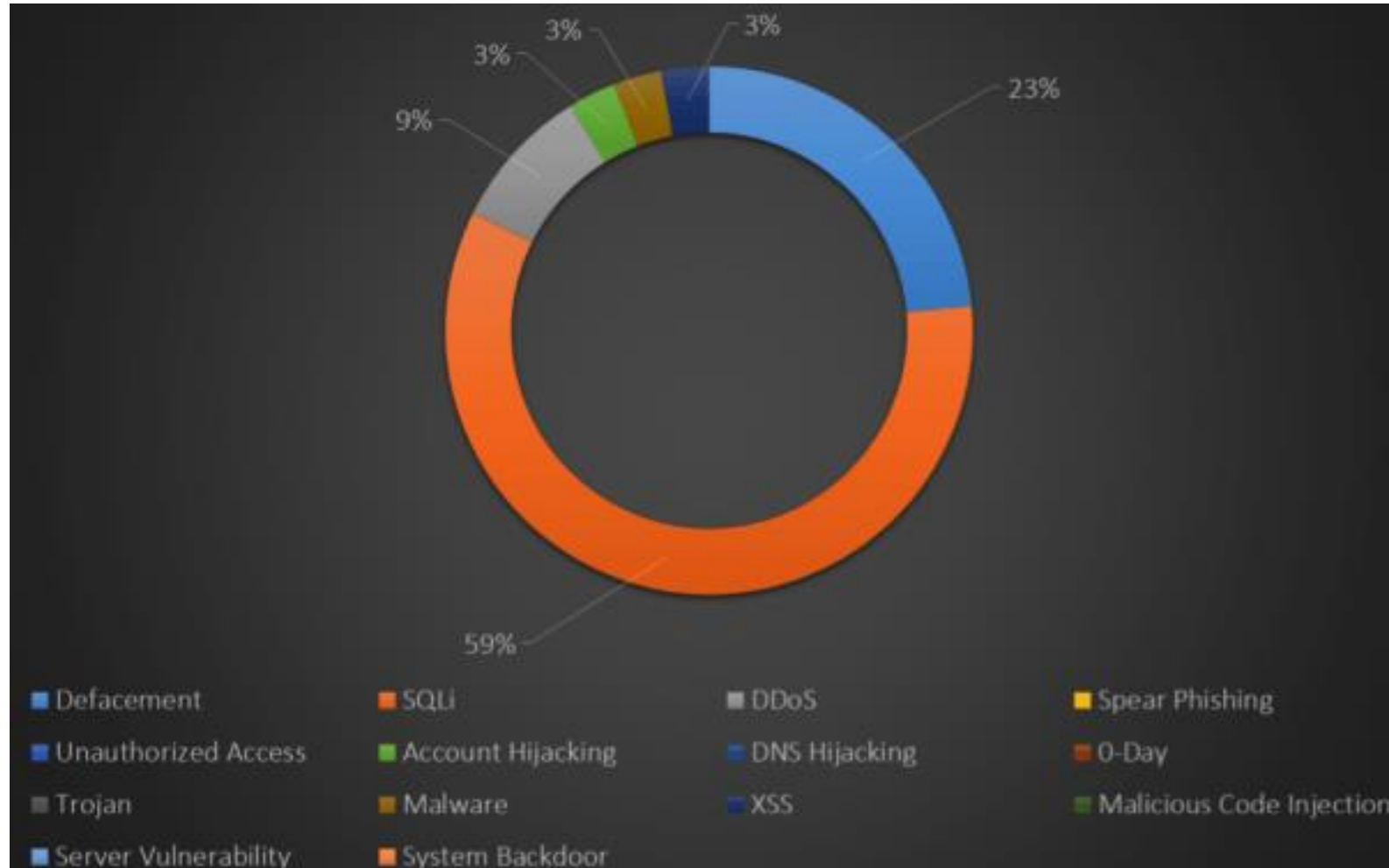


- The cloud paradigm has definitely prevailed
  - Most application are delivered following the **SaaS** model
  - Many developers rely on **PaaS** offerings for scalability
  - Nearly all underlying resources (DBs, Queues etc) are outsourced at the **IaaS** level
- Attack vectors have increased
- ‘Raw data’ are the modern hacker’s holy grail
- **The responsibility for the protection of data has shifted to the developer**



# PaaSword

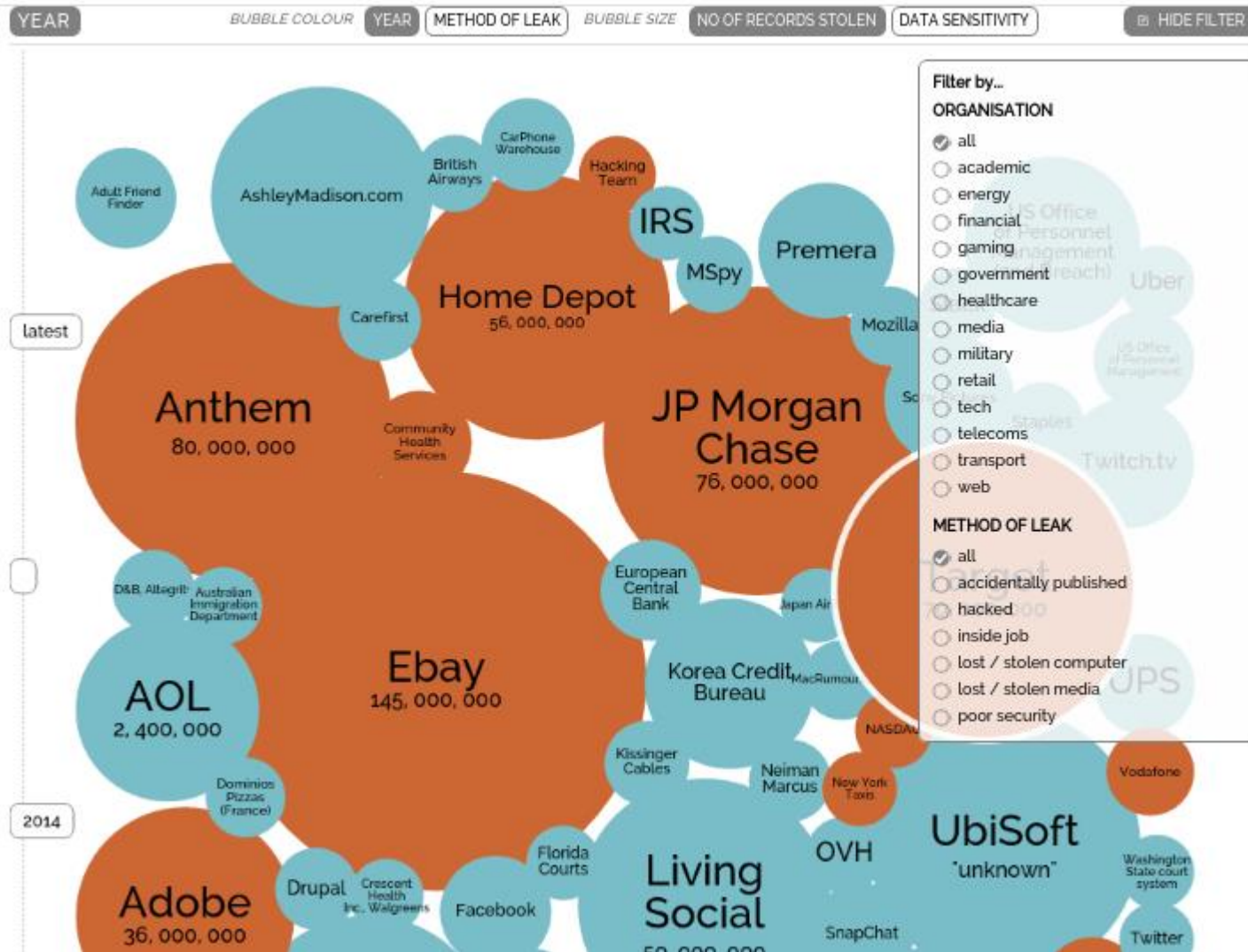
## 60% of attacks target the database





# PaaSword

# Data leaks

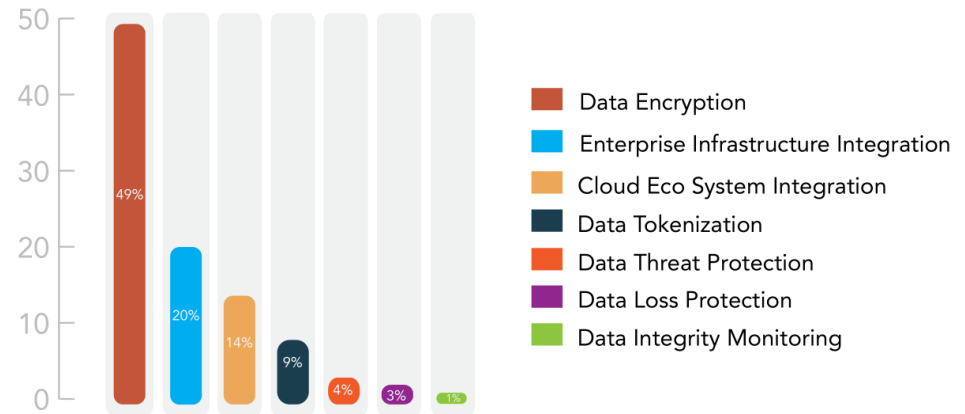
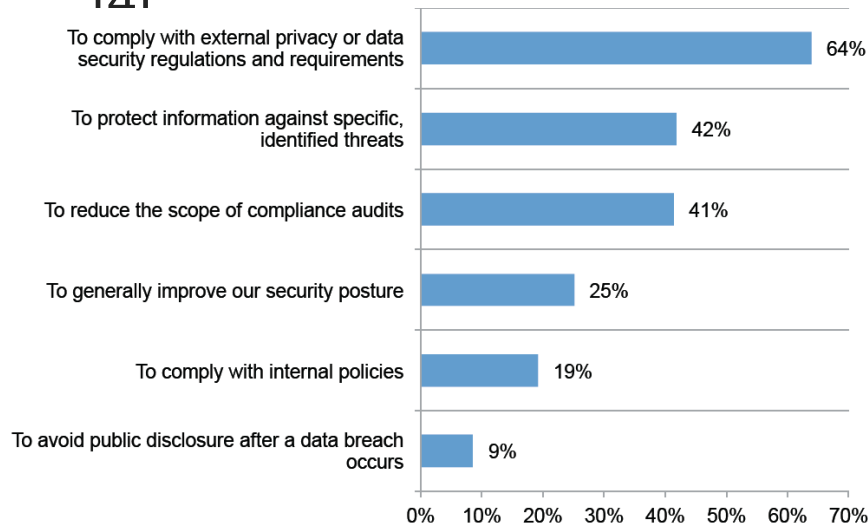




## Motivation – Security as an Enterprise Requirement

- Enterprises identify **security concerns** and **data privacy** as the most significant **barriers** of Cloud adoption;
  - In addition:
    - Compliance (e.g., legal, regulatory, industry-standard compliance)
    - Cultural resistance
- Encryption and key management as top priority requirements [3] &**

[4]



[3] P. Institute, “2015 Global Encryption & Key,” Thales, 2015.

[4] CipherCloud, “Global cloud data security report - The authority on how to protect data in the cloud,” CipherCloud, 2015.



# PaaSword

## How shall we lower the barriers?

- Security concerns
  - Protect confidential information
  - Control access
  - Trust cloud provider
  - Secure Cloud Applications
- Data privacy
  - Secure storage
    - Encryption
    - Trustable Key Management
  - Control Access to data

### PaaSword



# Problem Areas Targeted



- **Insufficient** security and **trust** of cloud infrastructures and services
- Cloud application **developers** have difficulties specifying appropriate **level of security**
- Appropriate **context-aware access control** mechanisms for cloud applications
- Ensure **protection**, privacy and integrity of **data stored** in the cloud
- **Prove** applicability, usability, effectiveness and value of **secure cloud platforms**

## MENU

[Dashboard](#)[Application](#)[Resources](#)[Activity](#)

## DEVELOPER DOCS

[Documentation](#)[Launch IDE](#)

## ADMIN

[Users](#)[/ dashboard](#)

## Dashboard

Account overview

[PaaSword Models](#) →

Access context model, expression and policy editor

[Applications \(1\)](#) →

Registered applications

[Activity \(27\)](#) →

List of activities

[Resources \(12\)](#) →

Registered PaaS and IaaS providers



### Policy Enforcement Mechanism

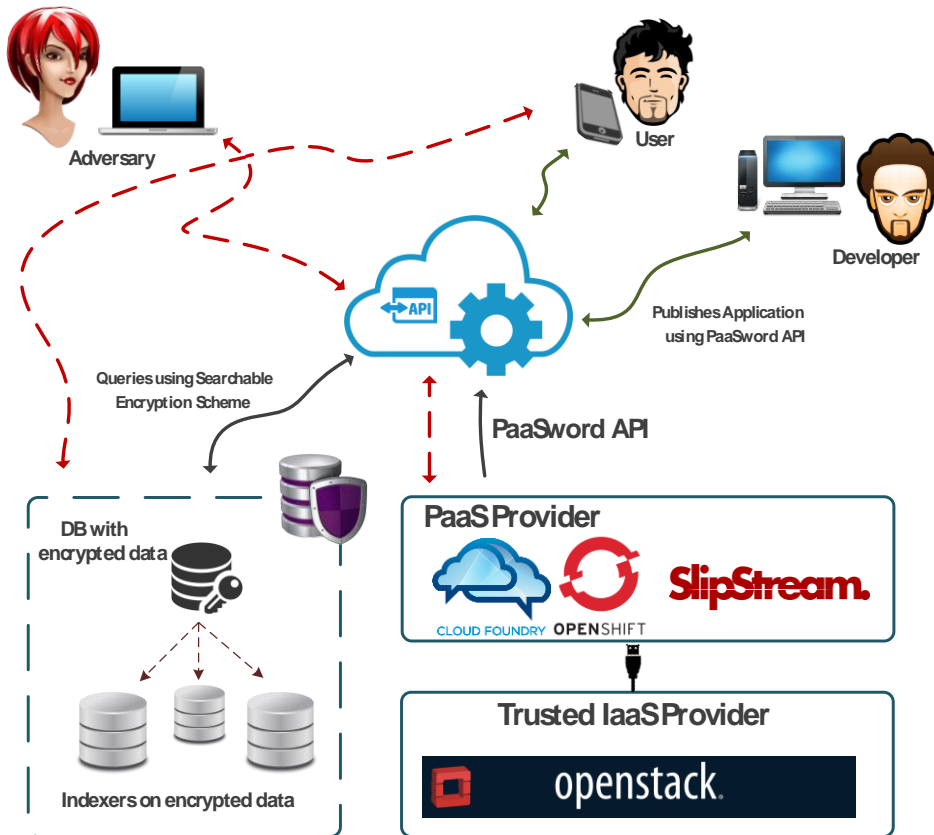
Visit [activity](#) to see performed actions from the Policy Enforcement Mechanism.



ENABLED

Synchronize





- A **security-by-design** framework which will allow developers to engineer secure applications
- **Leverage the security and trust** of data that reside on outsourced infrastructure
- Facilitate **context-aware access to encrypted** and (even) **physically distributed** datasets stored in the cloud
- Prove **applicability, usability, effectiveness** and value of our framework in real-life Cloud infrastructures, services and applications



# PaaSword

## Major Assets developed so far...

- A JAVA annotation library that can be used during development in order to annotate database models (using JPA)
  - These annotations are translated during runtime to privacy constraints that drive the fragmentation of the database
- A **virtual-database proxy** that is able to handle any SQL query by translating it in the proper format based on the fragmentation scheme
- An **XACML-compliant authorization engine** that is able to perform reasoning prior to attribute-evaluation
- An **integrated IDE environment** where developers can submit and control their PaaSword-enabled applications



# PaaSword

# Integration of Eclipse CHE IDE

Eclipse Che

Workspace Project Machine Edit Assistant Run Profile Git Subversion PaaSword Help

Upload project default CMD build

API key Add API key

Project Explorer

Application

```
1 1 /*
2 2  * Copyright 2016 PaaSword Framework, http://www.paasword.eu/
3 3  *
4 4  * Licensed under the Apache License, Version 2.0 (the "License");
5 5  * you may not use this file except in compliance with the License.
6 6  * You may obtain a copy of the License at
7 7  *
8 8  *      http://www.apache.org/licenses/LICENSE-2.0
9 9  *
10 10 * Unless required by applicable law or agreed to in writing, software
11 11 * distributed under the License is distributed on an "AS IS" BASIS,
12 12 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
13 13 * See the License for the specific language governing permissions and
14 14 * limitations under the License.
15 15 */
16 16 package com.mycompany.xerp;
17 17
18 18 import eu.paasword.paaswordlibrary.api.PaaSwordAPI;
19 19 import org.springframework.boot.SpringApplication;
20 20 import org.springframework.boot.autoconfigure.EnableAutoConfiguration;
21 21 import org.springframework.context.annotation.Bean;
22 22 import org.springframework.context.annotation.ComponentScan;
23 23 import org.springframework.context.annotation.Configuration;
24 24 import org.springframework.context.annotation.EnableAspectJAutoProxy;
25 25
26 26 @ComponentScan
27 27 @Configuration
28 28 @EnableAutoConfiguration
29 29 @EnableAspectJAutoProxy
30 30 public class Application {
31 31
32 32     public static void main(String[] args) {
33 33         SpringApplication.run(Application.class, args);
34 34     }
35 35 }
```

Consoles

DEV default SSH user@c95760c098a8:/projects\$

Terminal



# PaaSword

# Native Integration with OpenStack

/ application / xERP / instance1

← instance1

Application Instance Management

Database proxy in order to distribute your data with the chosen privacy constraints needs 4 database instances (including 2 coordination servers)

```
faculty.id, student.name, university.id,  
university.name,  
university.number_of_lecture_halls,  
university.fk_city_city, city.id, city.name,  
city.fk_country_country, country.id,  
country.name, country.inhabitants, student.id,  
student.surname, student.birth_date,  
student.gender, student.semester,  
student.fk_university_university,  
student.fk_faculty_faculty
```

```
faculty.name, student.grade
```

Fragmentation Schema exists

Instance Name:

instance1

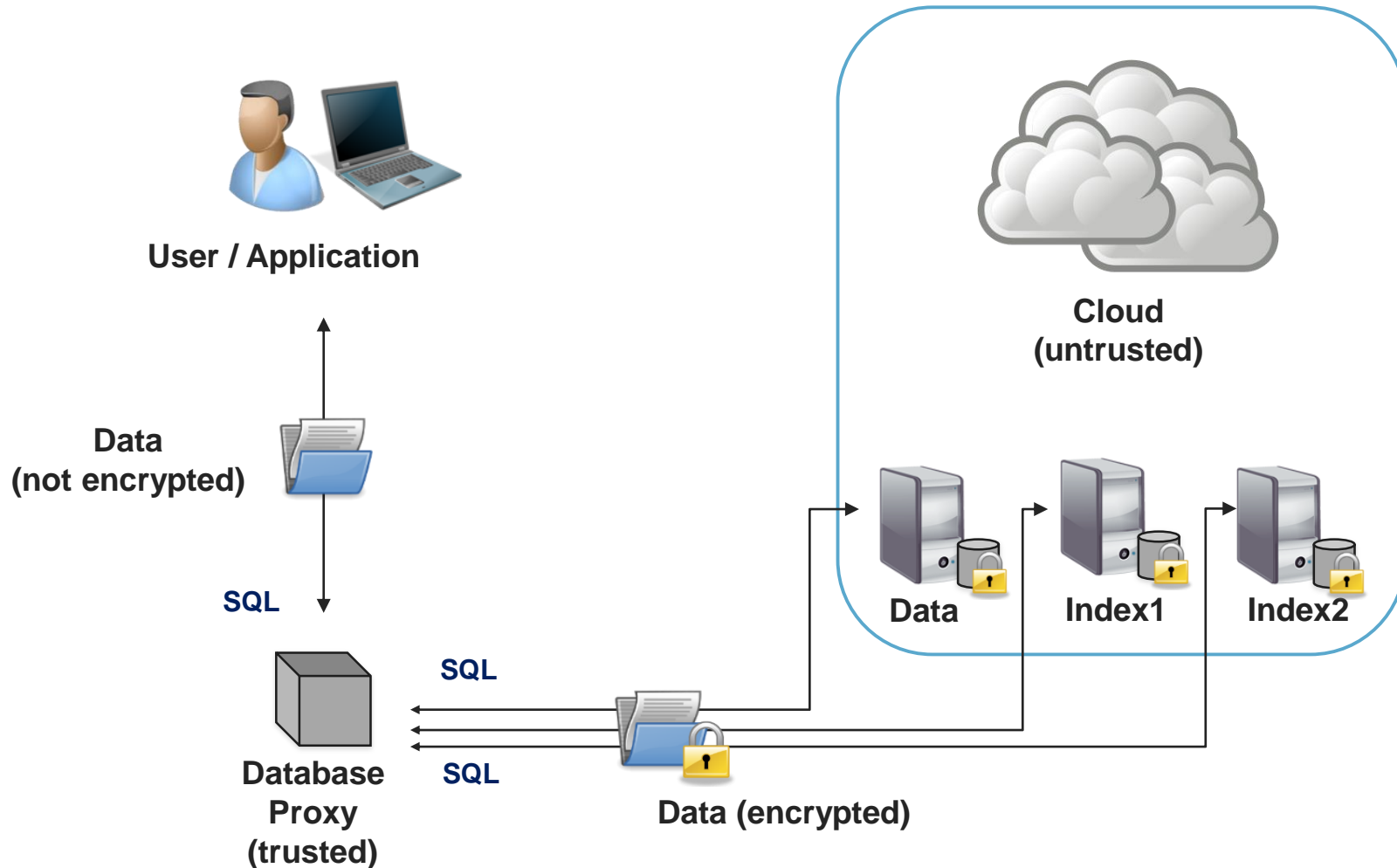
Privacy Constraints:

set1 × set2 ×

IaaS Provider: ?

- paasword-openstack-1
- paasword-openstack-2
- paasword-openstack-3
- paasword-openstack-4
- paasword-openstack-5
- paasword-openstack-6

# Asset: Virtual Database Architecture





# PaaSword

# Model-driven Expression editing

/ dashboard / model management / expression editor / edit

## ← Edit Expression

Model Management

← GO BACK

Name:

MobileOSAndroid

Namespace:

ex - http://www.example.com/test/1#

Expression:

AND OR

+ Add rule + Add group

DeviceType - hasMobileOS

equal

Android

✕ Delete

Network Location

equal

UbitechIntranet

✕ Delete

AND OR

+ Add rule + Add group ✕ Delete

-----

✕ Delete

↻ RESET

💾 SAVE



# PaaSword

## Interested in... ?

- Getting access to early results?
- Shaping and expanding PaaSword?
- Networking with leading companies & research institutes?
- Collaborating with us and the PaaSword Community?

**Join the Cloud Security Industrial Focus Group!**

Register at:

<https://www.paasword.eu/register/>





PaaSword

Join our Industrial Focus Group  
Today!

## Acknowledgements:

*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644814.*



Visit us:

[www.paasword.eu](http://www.paasword.eu)