POSEIDON

Risk Management and Data Analysis in PoSeID-on

Presenters:
Paulo Silva
Rui Casaleiro

July 11th, 2019

Funded by Horizon 2020
Framework Programme of the European Union

INDEX

PoSeID-on

Protection and control of Secured Information by means of a privacy enhanced Dashboard


PoSeID-on Goals

- **Empower data subjects**
- **Safeguard personal data**
- **Data minimization and data quality**
- **Detection of unexpected and potentially harmful behaviours**

Our challenge

Detection of unexpected
and
potentially harmful behaviours

Approach

- **Model normal behaviour of PoSeID-on**
- **Analyse contents of PII related operations**

Risk Management Module Goals

- **Model normal system behavior**
  - While being as decoupled and less intrusive as possible
- **Generate warnings each time a possible privacy risk is happening**
  - By identifying anomalous patterns in system operations
- **Manage data processor reputation**
  - According to previous good risk generating behavior

RMM Approach

Model system behaviour based on:

- Type of operations performed in the system
  - PII Permission Request, PII Access, PII Permission Revocation…
- Logs generated by each component in the system

Notify system administrators and data subjects when the pattern extracted from such info deviates from the regular pattern

T4.3 RMM – Anomaly Detection

- **Log collection**
  - Messages from components
- **Log parsing**
  - Generate log event templates
  - Fit each log into one of the template events
- **Feature extraction**
  - Count number of events happening within a window (e.g hourly window)
  - Count number of PII operations of each type happening within a window
- **Anomaly detection**
  - Create a model from regular event count per window using clustering algorithms
  - Predict cluster for upcoming logs
  - Determine distance from predicted cluster and clusters with small number of entries in order to identify anomalies
  - Update model according to new values

T4.3 RMM – Anomaly Detection

Output:

A window (sequence of events) which has been flagged as anomalous or in other words, not fitting in the regular behavior of the system. This might be:

- A privacy risk
- A system malfunction
- A non-malicious but rare pattern of logs

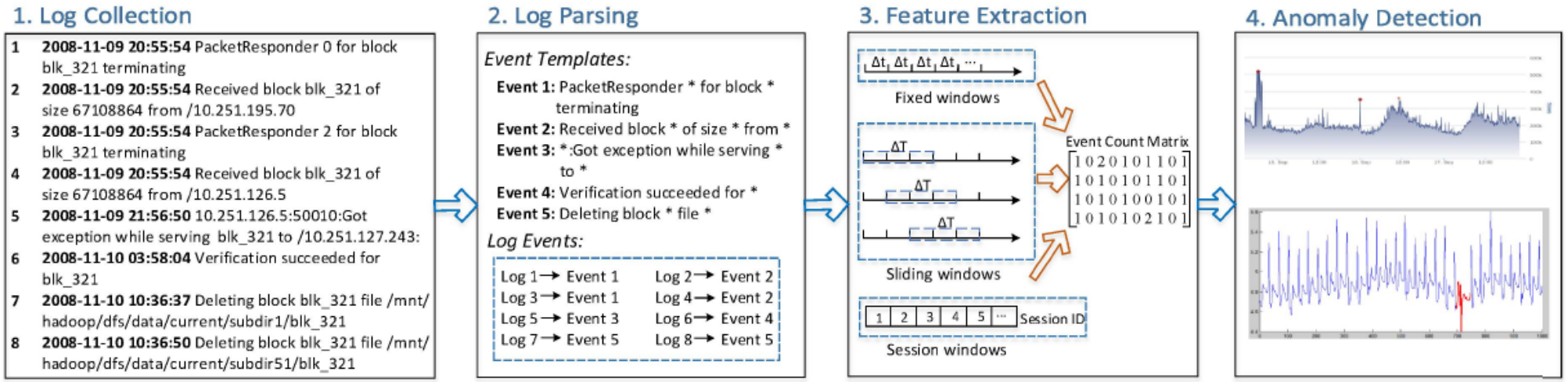
Further analysis of the identified anomalies is needed to determine if a risk is real or not.

T4.3 RMM – Anomaly Detection

Identifying which Data Subjects and Data Processors are involved in the anomalous window allows:

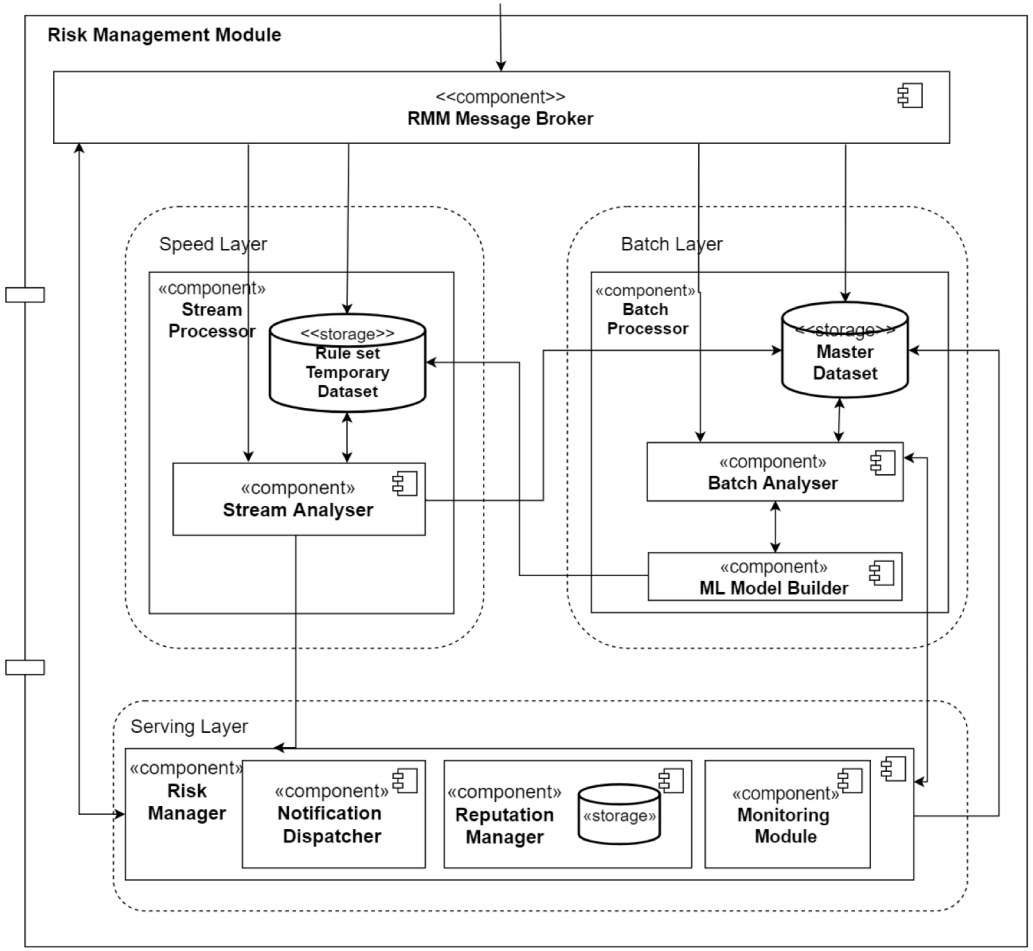
- **Updating data processor reputation accordingly**
- **Notifying involved data subjects**

T4.3 RMM – Log Anomaly Detection



[1] S. He, J. Zhu, P. He and M. R. Lyu, "Experience Report: System Log Analysis for Anomaly Detection," *2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE)*

RMM Architecture



Simplified Lambda Architecture

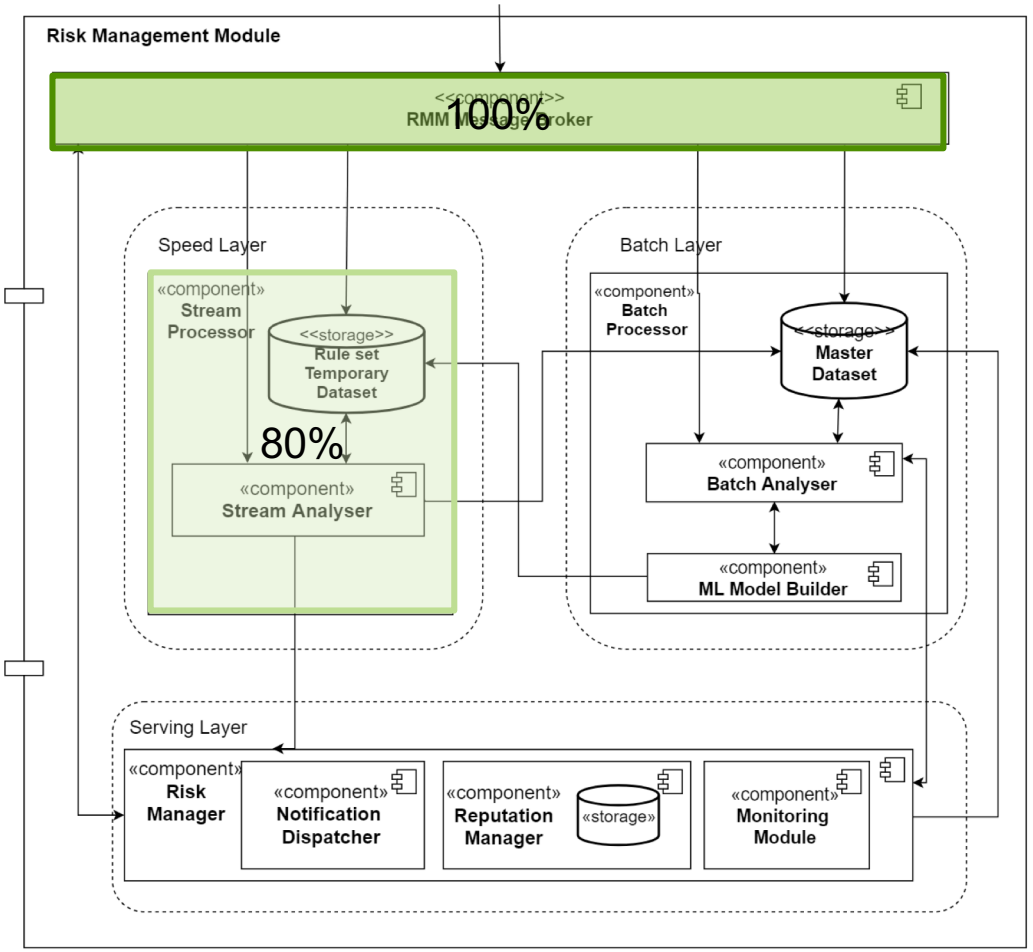
- Speed layer returns results in real-time by analysing the stream
- Batch layer stores incoming data, performs analysis over a larger dataset and trains models
- Service layer handles results, involved data subject identification and reputation metric requests

T4.3 RMM – Current status

Detailed design and architecture - 100%

Implementation - 50%

- Communication protocol (Libsodium + Protobuf)
- Integration of RabbitMQ with Spark Streaming
- Log analysis for anomaly detection pipeline
  - Extracting parameters from messages and format them to proper data structure
  - Java implementation of Drain Log Parser algorithm, adapted to work on Spark Streaming Pipeline
  - Creation of feature vector to feed clustering algorithms



T4.3 RMM - Next Steps

- **Dataset Generation**
- **Development**
  - Implementing anomaly detection
  - Implementing storage for parsed data
  - Adapting stream pipeline to batch layer
- **Configuration**
  - Distributed deployment
  - Security aspects
- **Testing and validation**

Personal Data Analyser - PDA

- **Control personal data in a transaction**
  - Personally Identifiable Information (PII)
- **Natural Language Processing & Understanding**
  - Extracting and processing information from transactions
- **Artificial Intelligence**
  - Analyze and evaluate the extracted information

PDA Goals

- **Control personal data in a transaction**
  - Detect or prevent anomalies on misbehaved transactions
- **Generate warnings each time a transaction contains non-identified PII**
  - Discovering PII and making sure existing PII is compliant with permissions
- **Generate privacy risks warnings**
  - PII analysis based on its unique degree of sensitiveness
  - PII analysis based on the correlation with other PII fields

PDA Approach

- **Analysis requests**
  - Transactions performed within PoSeID-on
  - Connection to PoSeID-on's central messaging protocol
- **Request Handling**
  - Messaging protocol
    - Protocol Buffers (protobuf)
    - Libsodium (PyNaCl)
    - RabbitMQ (pika)
- **Data extraction and parsing**
  - NLP tools
    - NLTK, Stanford CoreNLP, SpaCy
- **Data analysis**
  - ML Models for Named Entity Recognition
  - Regular Expressions
- **Privacy risks analysis**
  - PII sensitiveness
  - PII correlation
  - DP's reputation

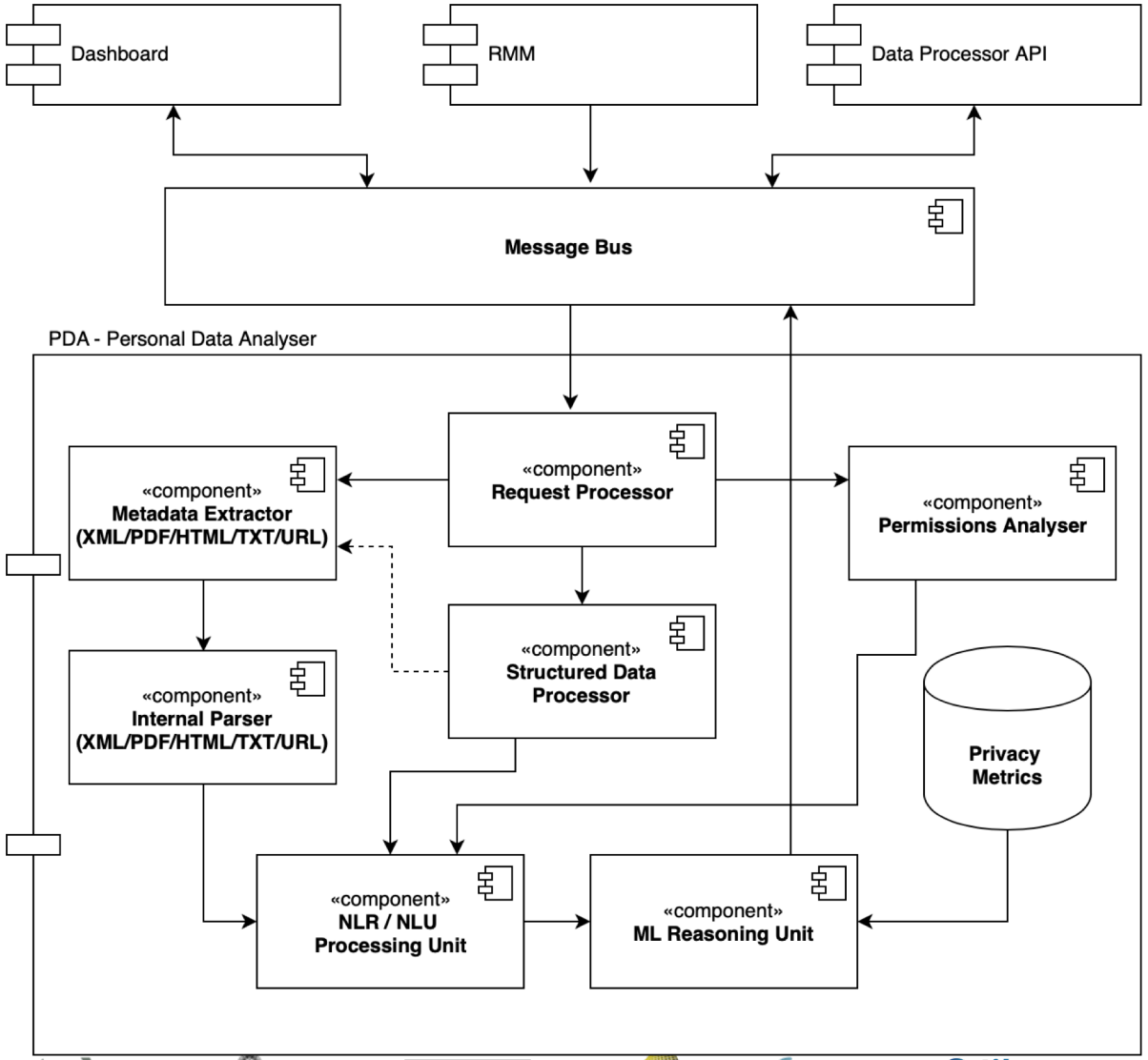
PDA PII Analysis

Levels	Description
High	Sensitive (direct identifier)
Medium	Quasi-identifier (indirect identifier)
Low	Limited effect

PII Fields	MEF	Softeam	Santander
Title	✓	✓	✓
First name	✓	✓	✓
Last name	✓	✓	✓
Email address	✓	✓	✓
Street name	✓	✓	✓
Street number	✓	✓	✓
Post code	✓	✓	✓
City	✓	✓	✓
Country	✓	✓	✓
Social security number	✓		
Bank details	✓		
Employment contract and salary information	✓		
License plate number	✓		
Gender			✓
National ID numbers			✓
Date of Birth			✓
Passport number			✓

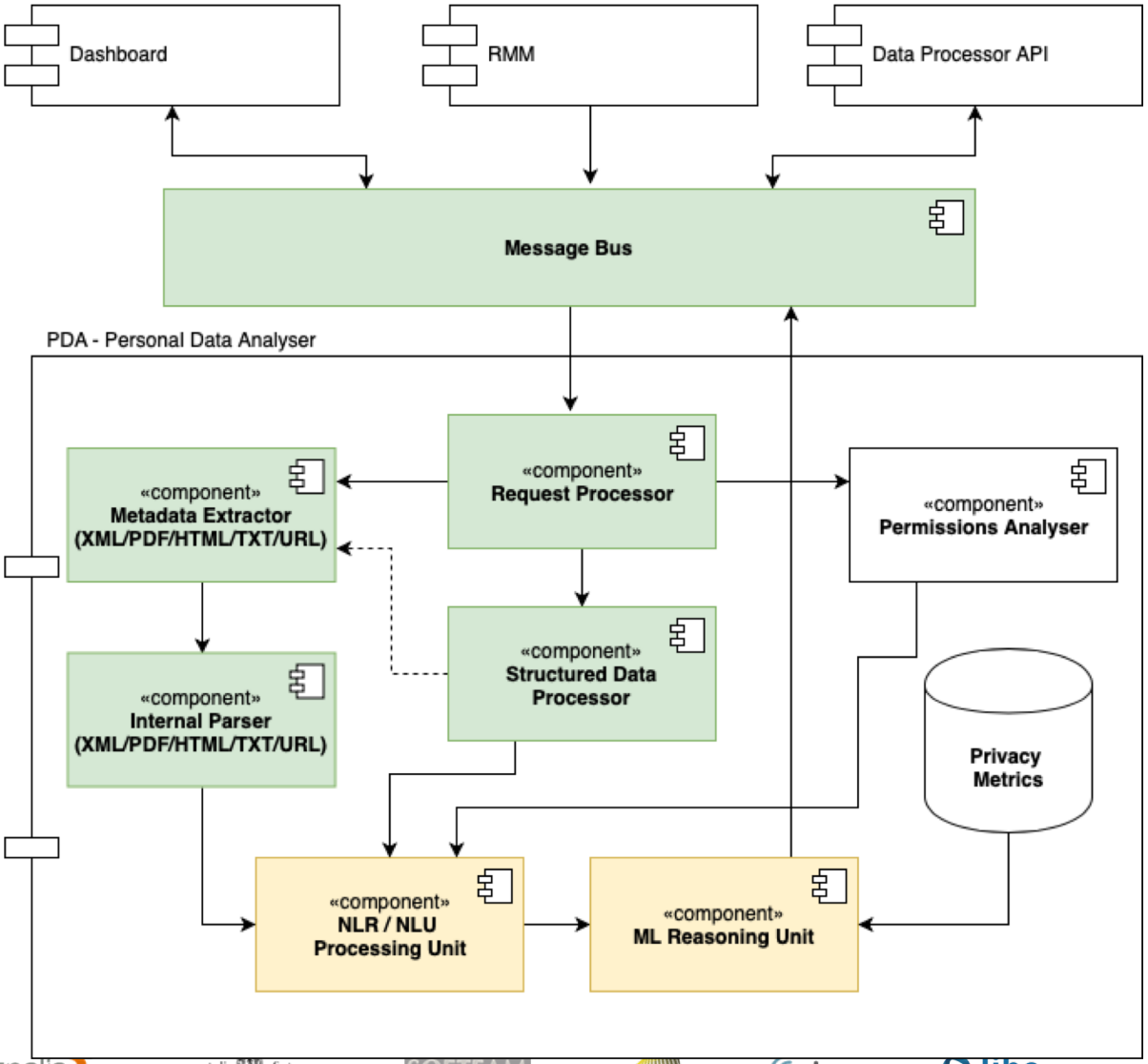
PDA Architecture

- **Incoming Requests**
  - Dashboard
  - RMM
  - Data Processor API
- **Pipeline**
  - Request Handling
  - Data Extraction / Parsing
  - NLP Processing
  - Privacy Risks Analysis



PDA
Current Status

- **Message Bus**
- **Message Handling**
- **Data Extraction / Parsing**
- **NLP Processing**
- **Integration**
  - Containerization
  - Minikube



T4.3 PDA - Next Steps

- **Development**
  - Tests and Validation
  - Create in-house models
    - With information provided by partners
    - PII Specific Information
  - Assessment and implementation of privacy metrics to be used in the analysis
  - ML Reasoning Unit development
- **Finalize first integration stage**
  - Module communication, Minikube configuration

- **Papaya collaboration**
  - Privacy-preserving Neural Networks (NN)
  - To allow a data owner either to:
    - Classify data
    - Collaboratively (with other data owners) train neural networks (NN) while ensuring data privacy
  - Analyze the requirements and conclusions taken from today's bi-lateral meeting

Final Considerations

- Development and integration progress
- State-of-the-art technologies
- GDPR compliance
- Public documentation available by the end of the month


THANK YOU
MEF
Ministero dell'Economia e delle Finanze
mita
accenture
tecnalia
Universidade de Coimbra
SOFTEAM
PNO
e-lex
Jibe