Secure Data Sharing and Processing in Heterogeneous Clouds

Bojan Suzic, Graz University of Technology
Presentation Outline

- SUNFISH Project
- Cloud Service for Public Administration
- Practical Approach
- Data Sharing and Processing
- Enforcement and Monitoring Architectures
- Summary
SUNFISH Project

- **SecURE iNFoRmATION SHaring** in federated heterogeneous private clouds

- **H2020 Project, ICT: Advanced Cloud Infrastructure and Services**

- Started in January 2015, aimed for three years

- Budget ~4.5 Mil. €

- Involves eleven partners from diverse environments, including: public bodies, universities, IT developers, R&D institutions

- Partners from six countries: Italy, UK, Israel, Estonia, Malta, Austria
Cloud Services for Public Administration

- Public Cloud Services?
  - Administrative obstacles (e.g. procurement)
  - Legal issues (e.g. data localization, cross-border transactions)
  - Security and privacy (e.g. confidentiality, integrity, accountability)

- Federation of private clouds for public administration?
  - Lack of infrastructure and technology
  - Considering public sector needs and requirements
  - Additional dimensions of efficiency, utilization, elasticity

- Challenges:
  - Heterogeneity and interoperability
  - Data security, process transparency, legal compliance
Cloud Services for Public Administration

- SUNFISH aims to address the lack of infrastructure and technology for federation of private clouds considering the needs of public sector

- Specific objectives:
  - Integrate different clouds assuring information security
  - Greater infrastructure usage efficiency thanks to a more effective workload management in shared private clouds
  - The development of services for EU citizens which use sensitive data shared securely between different private clouds
Practical Approach

- Use case 1

Data and resource sharing in federated private clouds

- Collaboration of two organizations
- Requirements: scalability and security

- Private, shared and secure zones
- Data is shared and processed in isolated instances
- Data transformation: masking sensitive information
- Monitoring the data flows and enforcement
Practical Approach

- Use case 2

Data and resource sharing in federated private – public clouds

- Secure collaboration of public entity with data providers
- Sharing the data between entities, traversing from private sector, to public, and back
- Requirements: scalability, security, interoperability

- Transforming the data, masking sensitive parts
- Performing processing in secured environment
- Monitoring the data flows and activities
Practical Approach

- **Use case 3**

Data sharing based on fine grained, dynamic policies

- Private-cloud centered
- Data shared to external entities, in controlled, transparent and traceable manner
- Requirements: security, interoperability

- Fine grained, adaptable, dynamic security policies
- Monitoring the data flows and enforcement
Data Sharing

- Data sharing
  - Conforms to common and organization-specific security policies
  - Using legislation aware approach
  - Performed using isolated and secure environment

- Data transformation based on:
  - Format-preserving encryption
  - Masking/tokenization
  - Attribute-based encryption

- Key and tokenization management using SUNFISH framework services ¹)

¹) Reimair et al. WebCrySIL - Web Cryptographic Service Interoperability Layer. (2015)
Data Processing

- Data processing
  - Common and organization-specific security policies, considering security-level objectives and legislative requirements
  - Performed in isolated and secure environment

- Data processing based on:
  - Original data, decrypted or unmasked and processed in a secure environment
  - Using secure multi-party computation

---

2) Bogdanov et al. *A universal toolkit for cryptographically secure privacy-preserving data mining*. (2012)
Enforcement Architecture

- Based on enhanced XACML architecture and policy language

- *Policy-enforcement point* ensures the conformance to security policies on the level of each zone and instance

- *Policy-decision point* is located in SUNFISH common environment, evaluates requests and checks their conformance to security policies and legal requirements
Monitoring Architecture

- Assuring security and accountability
- Exists independently of the enforcement infrastructure
- Deployed at various service and infrastructure levels, in cross-cloud setting
- Intercepts and monitors each action and interaction, on a cloud-wide basis
- Validates policy enforcement and executes the actions upon its violation
- Integrated with visual console
Summary

- Establishment of secure system for federated private clouds
- Conforming to the needs of public administrations
- Focused on security
- Neutral in the terms of vendors, platforms, systems
- Validated using real-world use cases
Any questions?

Thank you very much