Project Overview

Rui Oliveira

University of Minho & INESC TEC, Portugal
rcmo@inesctec.pt

IFIP 10.4WG - 71st Meeting - Queenstown, New Zealand, January 2017

European Commission
Horizon 2020
European Union funding
for Research & Innovation

Project Ambition

The ambition of the project can be deceivingly simple

Project Ambition

Offsite storage

Privacy, Integrity and Availability

Project Ambition

Offsite processing

Privacy, Integrity and Availability

Project Ambition

Secure communication

Privacy, Integrity and Availability of communication

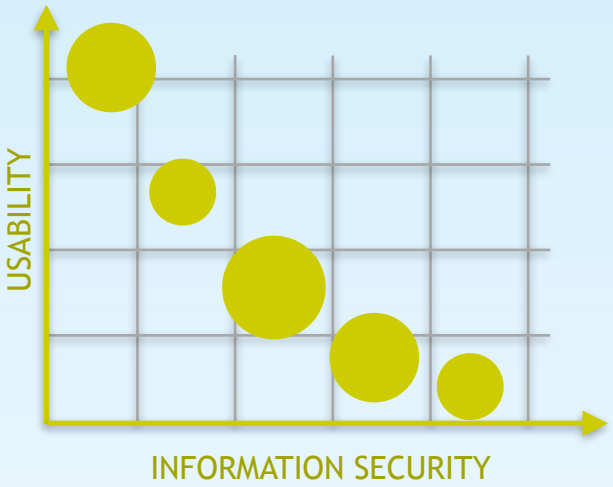
Project Vision

Holistic partitioning and entanglement

Project Vision

Assumption of non-colluding domains for partitioning

Identification of tradeoffs between usability, partitioning, entanglement and performance



Besides novel research, secure storage, secure processing and secure networking heavily leverage existing fundamental results

The focus is on coming up with a software stack that can be deployed as a PaaS and as a SaaS

Project Challenges

- Private communication middleware
  - Data integrity and anti-tampering
  - Low intrusiveness
  - Trade-offs
- Trustworthy storage
  - Data integrity and anti-tampering
  - Legal issues
  - Trade-offs
- Private data processing
  - Confidentiality and verifiability
  - Spare end-users from full fledged distributed cryptographic protocols
  - Trade-offs

Private communication middleware

- Vulnerability-tolerant channels by applying the fault tolerance paradigm to provide channels that remain secure even if there are bugs/vulnerabilities in software or cryptographic mechanism
- Novel route monitoring services that allow to detect abuses in BGP routing for the purpose of malicious Internet traffic deviation
- Exploit diversity of communication paths to make data snooping extremely hard by minimising relations between data sent in sequence

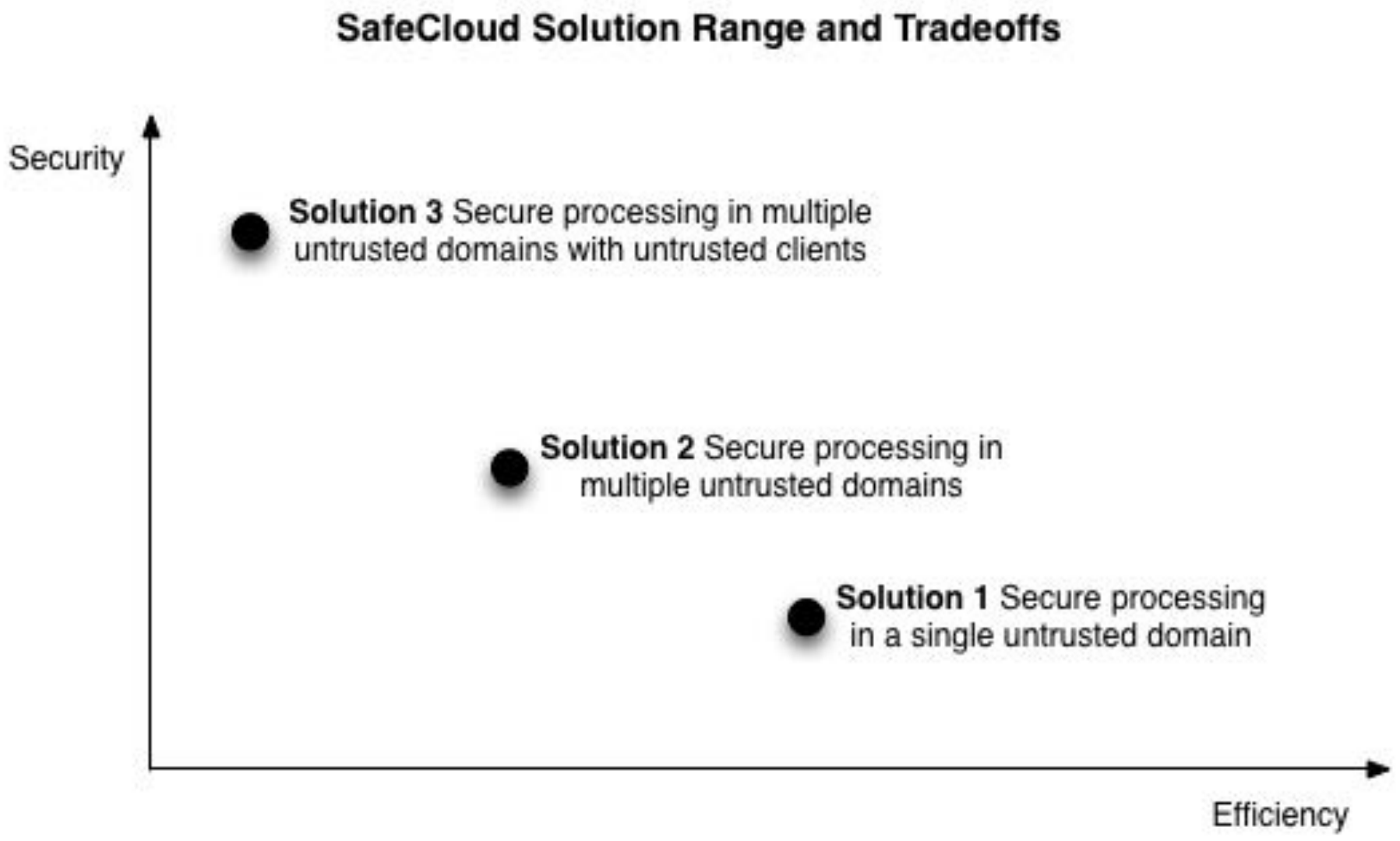
Trustworthy storage

- Future-proof, unexampled cloud data privacy by strategically partitioning data blocks across several physical locations and administrative domains
- Tamper resistance and data integrity and through data entanglement:
  - making it difficult for a powerful censor to irrecoverably destroy or tamper with archived data
  - providing verifiable guarantees to users that their data is properly, securely, and reliably archived

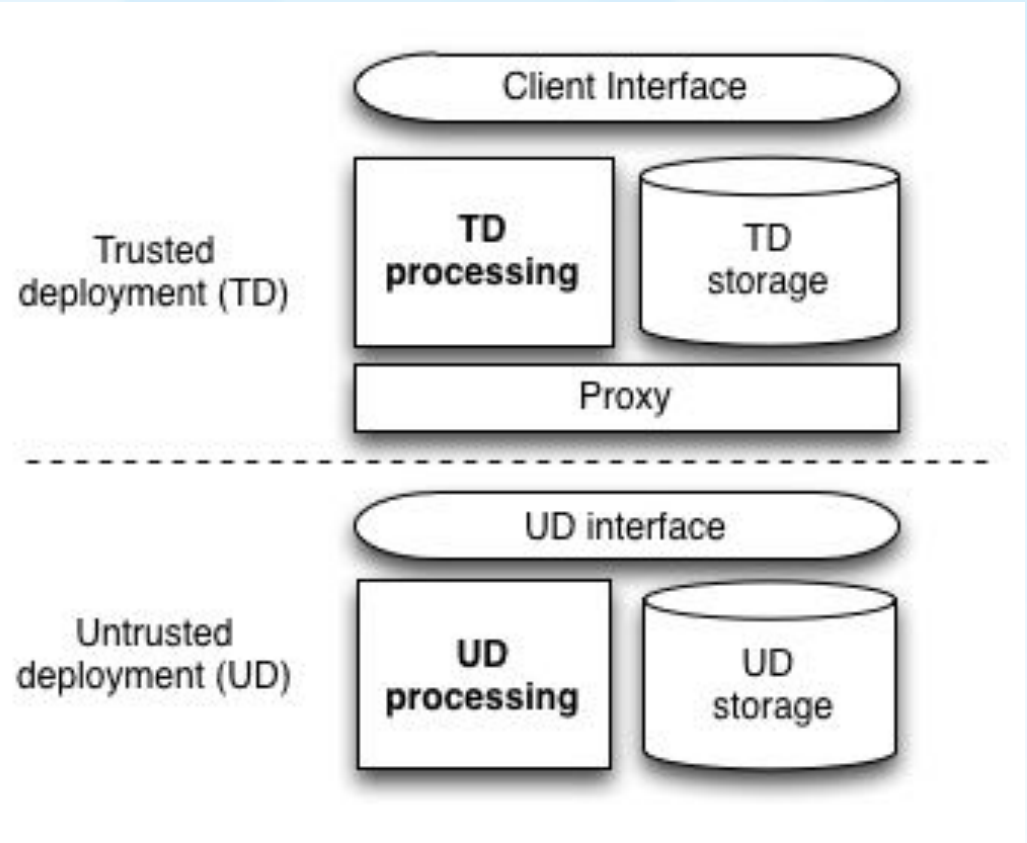
Private data processing

- SQL and NoSQL cloud processing with variable privacy and verifiability guarantees, allowing data analytics without disclosing both the original data and results
- Privacy-preserving computation leveraging a wide range of non-homomorphic encryption thechniques:
  - Deterministic encryption
  - Order-preserving encryption / searchable encryption
  - Secret sharing / multiparty computation
  - Privacy-preserving aggregation
  - Trusted hardware

Secure data processing



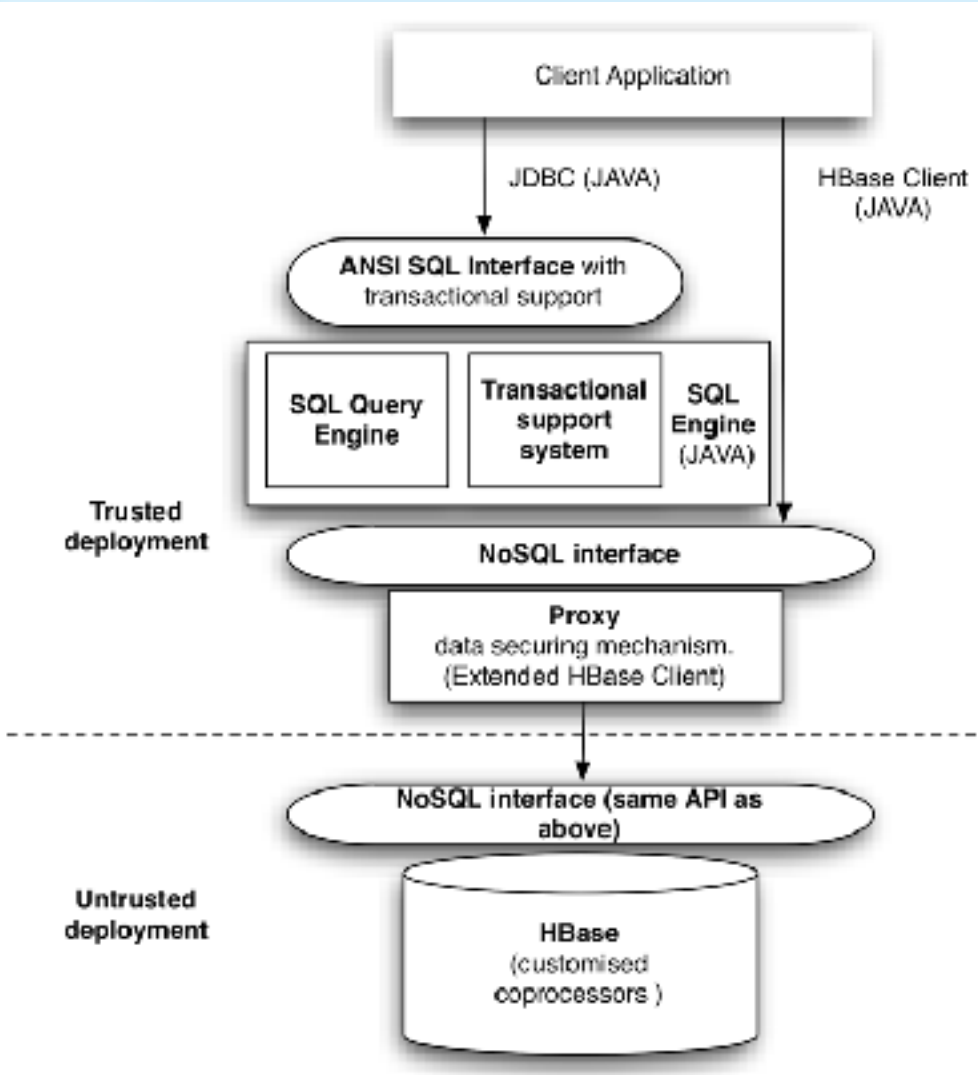
High-level architecture



- **two deployment zones**: a trusted one and an untrusted one
- in both zones it is possible to have data storage, processing and workflow logic
- **each zone can have multiple sites** (ex. multiple cloud service providers)
- for **each solution the instantiated components vary**
- **Compliant APIs: SQL and NoSQL interfaces available**

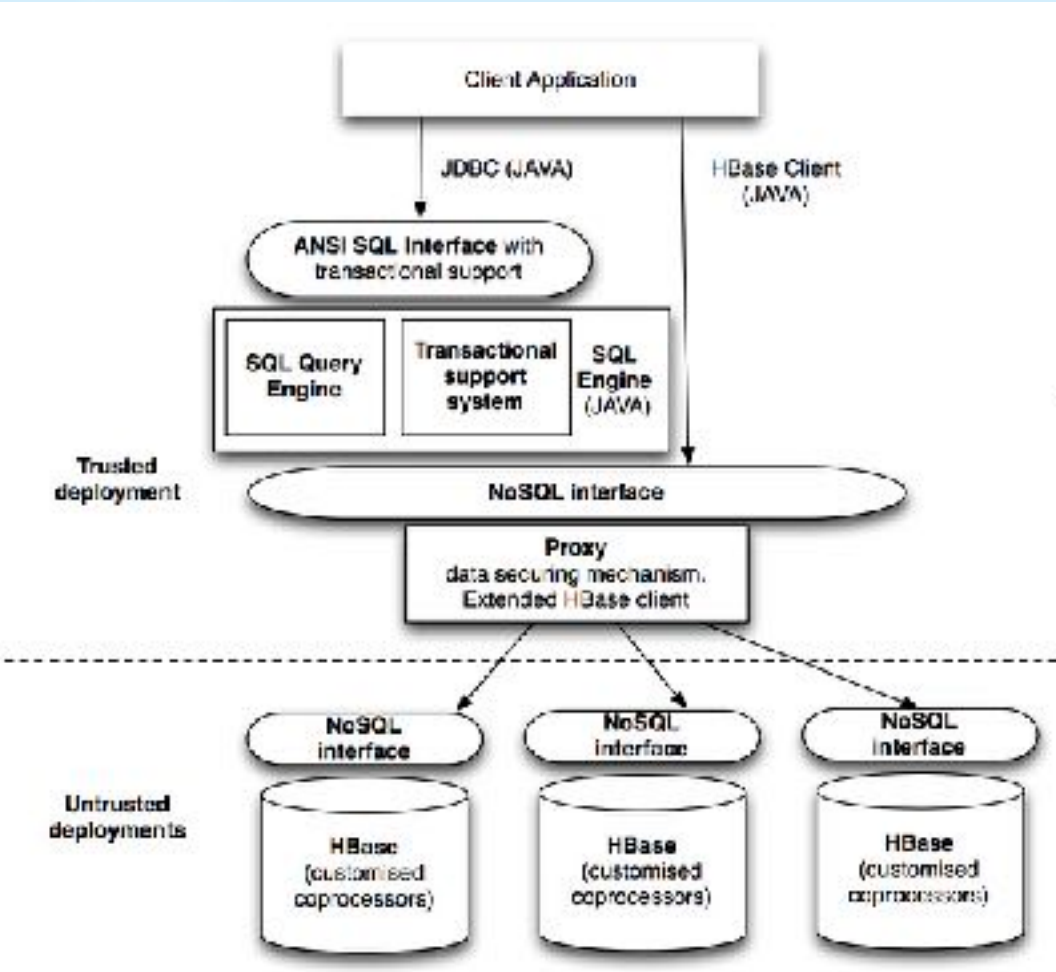
Solution 1: secure database server

- **single** trusted deployment (**client**) and **single** untrusted deployment (**server**/cloud service provider)
- highest expected performance
- **separation between query processing and storage**
- a **proxy component translates open queries in protected queries**
- data is **encrypted at the untrusted deployment**
- multiple encryption techniques possible: order preserving, searchable, symmetric, …



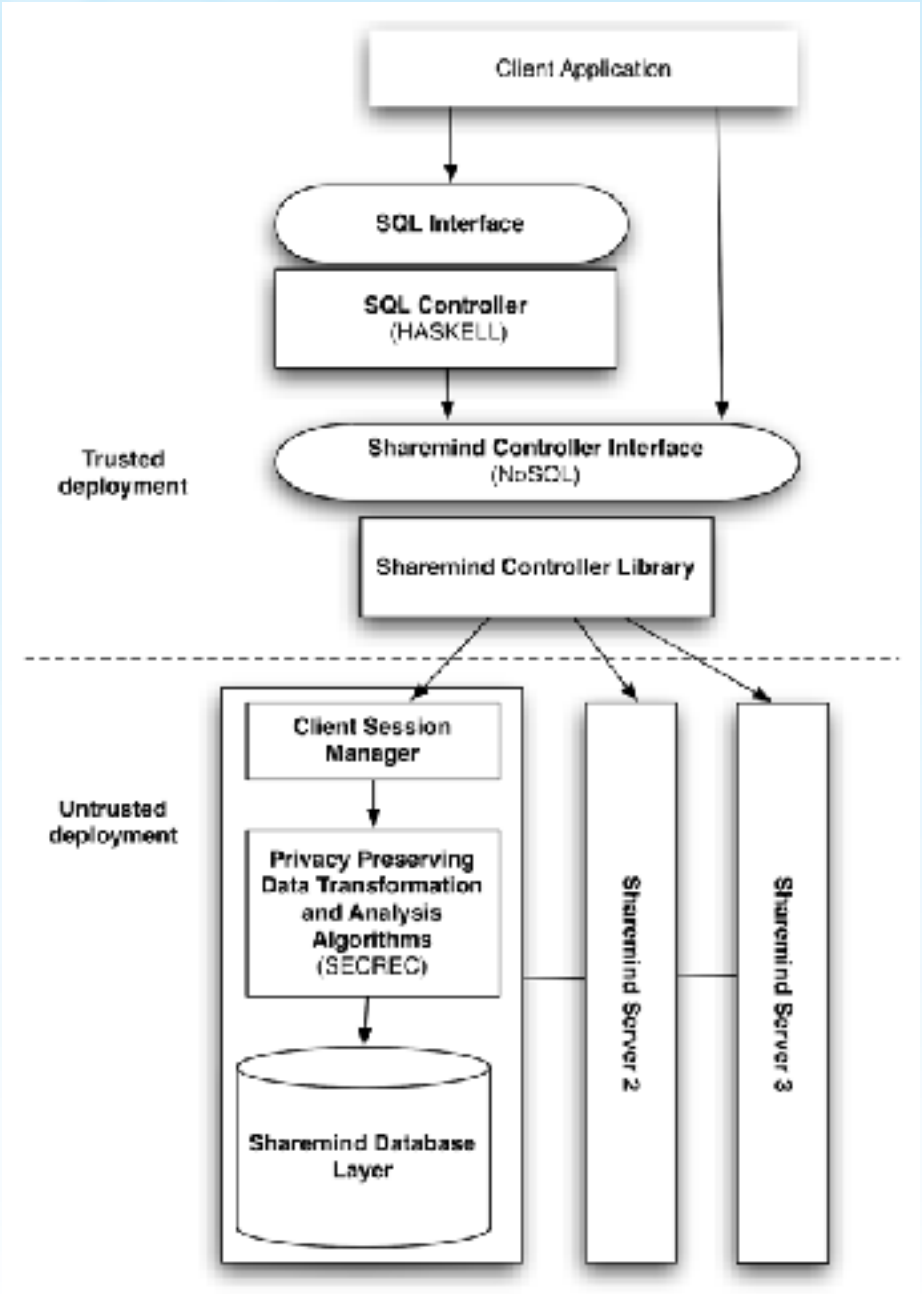
Solution 2: secure multi-cloud database server

- **single** trusted deployment and **multiple** untrusted deployments
- resorts to **multi-party computation** algorithms
- data in each untrusted deployment is, **individually, insufficient to disclose the original data**
- **processing** is done in collaboration between untrusted deployments **over the protected data**
- **query results hidden from the servers**



Solution 3: secure multi-cloud application server

- **multiple** trusted deployment and **multiple** untrusted deployments
- resorts to **multi-party computation** algorithms
- multiple parties can query the system without having to disclose their sensitive data to the other
- **only aggregate information can be retrieved from the system**



Project impact

- Exploit and integrate increased privacy technologies into mass market products
- Promote privacy-enhanced services on a large scale by showing that it can be achieved at reasonable cost and without noticeable performance degradation
- Increase the appeal of European cloud providers to long-term preservation and processing of international private and commercial entities data
- use cases:
  - European healthcare
  - European cloud storage providers
  - European privacy-preserving data processing technologies

SafeCloud Photos app

SafeCloud

your data is finally safe

Technology: infrastructure and services for private data storage
Insight: to split trust between multiple parties

Technology transfer

- Early delivery of research
- Lean startup approach
- Self-contained proofs-of-concept for validation and scouting
- Roadmap for expansion and and continuous integration of research

[Promotional video (YouTube)]