Federation-as-a-Service: the SUNFISH experience

Vladimiro Sassone
Scientific Leader
SUNFISH
Cyber Security Centre
University of Southampton
SecUrE iNFomation SHaring in federated heterogeneous private clouds

Ultimate Goal:

providing a secure by-design federation of individual clouds that enables the regulated and monitored sharing of cloud services

Horizon 2020 project consisting of:

4 Public Bodies
- Ministry of Economy and Finance (Italy)
- Ministry of Finance (Malta)
- Malta Information Technology Agency (Malta)
- South East Regional Organised Crime Unit (UK)

3 Academic Partners
- University of Roma La Sapienza (Italy)
- Technische Universität Graz (Austria)
- University of Southampton (UK)

2 Industrial Partners
- IBM Israel – Science & Technology Ltd (Israel)
- PricewaterhouseCoopers Advisory SpA (Italy)

1 public-funded non-profit association - A-Sit (Austria)
1 SME - Cybernetica (Estonia)

the SUNFISH project
Different cloud systems homogeneous aggregation of goal-oriented cloud systems

Multiple underlying motivations leading to a cloud federation:

- sharing of computing resources
- controlled usage of federated services or data
- collaboration among entities belonging to different administrative domains

Each federation aims at achieving a business need that the single clouds would not have achieved by themselves.
Cloud federation is still a quite new concept that, despite the recent large research efforts, lacks of solid proposals.

The following needs must be ensured:

- Enabling the federation and *sharing of any cloud service* (from IaaS to SaaS)
- Provisioning services according to *Access Control* and SLA policies
- Calculating *optimal workload plans* of federated resources
- *Monitoring* and *auditing* service provisioning
- Offering by design *privacy-preserving services*

The SUNFISH project aims at achieving these objectives by proposing a new and innovative cloud federation platform that private and public companies can adopt.
FaaS: Federation-as-a-Service

FaaS is a new and innovative cloud federation solution that enables the secure creation and management of cloud federations

Some FaaS functionalities:

• Dynamic federation of clouds and their services
• Advanced, innovative privacy-preserving services
• Innovative cloud federation governance

A cloud federation solution that could be widely adopted among companies, especially in the public sector, must rely on a governance that is

• distributed: no single point (of-failure) of the federation manages and stores the governance data
• democratic: all federation members have the same authorities and duties

This ensures that any governance action, e.g. the enforcement of access control policies, is carried out with the consensus of all the federation members.
FaaS permits Cloud systems to be more flexible and to better adapt to new emergent needs. More generally, it increases the operational efficiency of clouds. (e.g., optimised usage of resources and usage of advanced security service not usually widely available)

FaaS permits reducing the burden needed for sharing services among individual clouds. It strengthens each federated cloud to achieve its business goals.

Concerning the public sector, FaaS supports its digital transformation by offering a principled consolidation solution to reduce replicated IT investments and to prompt better harmonisation among systems.
FaaS at work

FaaS offers well-defined high-level operating phases supporting *cloud administrators* to

- federate cloud systems
- publish service on the platform
- leave the federation

and *cloud end-users* to

- request federated services
- use requested services
implementing FaaS: the SUNFISH platform

FaaS is supported by a software platform designed and implemented by the SUNFISH project.

The SUNFISH platform features various well-structured components whose interactions enable and support all the FaaS functionalities.

For examples, we have

- Dynamic Masking
- Data Security
- Secure Multi-Party Computation
- Runtime Monitoring
The deployment of the SUNFISH platform on the clouds must be completely distributed, to avoid centralisation or control of one cloud over another, i.e. ensuring a full democratic federation.

To this aim, we deal with these main issues:

• coherent storage and update of federation state
• monitoring of distributed components
• ensuring integrity of governance data (e.g., SLA and Access Control policies)
• distributed support for data masking

SUNFISH fosters a principled first time exploitation of blockchain technology
From Blockchain to a Blockchain-based Registry
The blockchain is a distributed public record of transactions available to everyone/allowed entities to view and verify.

A chain of blocks, where each block:
Consists of a header, hash of the previous block and transactions
Generated at pre-defined intervals

Once a block is part of the chain:
Transactions become (practically) irreversible and immutable.
An Ethereum program (called smart-contract) is like any computer program, but it is stored and executed on a blockchain.

Once a smart-contract receives input/command via transactions, it processes the input according to its logic, its own data and the global state of the chain.
A blockchain-based registry as a reliable, distributed mean to support multiple deployment of the SUNFISH platform

Regulated interactions with blockchain permit improving the assurance on each platform component (e.g., the access control system relies on no tampered policies)

Distributed ledger for a cloud federation

Non-repudiable manner (i.e. via smart contracts) of carrying out federation governance
blockchain-based functionalities

Federation contract
  avoiding the use of a “trusted third-party” to store the federation agreement contract

Federated services
  saving the current state of the federation

Access Control and SLA policies
  storing the policies of the member clouds

Federation Monitoring
  storing the logs of the Access Control system

Data Masking
  supporting storage and retrieval of tokenisation table

Data Anonymisation
  storing an history-record of released anonymised data
Balancing integrity guarantees (PoW) and better performance (Mining Rotation)

how about efficiency?
how about efficiency?

Balancing integrity guarantees (PoW) and better performance (Mining Rotation)
Balancing integrity guarantees (PoW) and better performance (Mining Rotation)

how about efficiency?
Beyond FaaS
The advent of IoT is changing modern computing systems paving always new challenges. Nowadays, IoT devices can sense any information, from temperature to electricity consumption, and be involved in any system and process, from smart-house to industrial supply chains.

Current computing systems for IoT suffer, e.g., from
• reliable means to check provenance of sensed data
• integrity-preserving data storage
• interoperable communication infrastructure
• interconnection with cloud systems to do data computation
• trusted data facilities to share data among devices
Our vision: a smart contract-based blockchain as

- reliable communication mean
- data integrity guarantor
- data provenance evidence
- interconnection with federated cloud systems
- infrastructure for data sharing among devices
On the basis of the achievement of the **SUNFISH platform**, we will have to face many more difficulties.....

- IoT devices may not be able to *interact* directly to a *blockchain*: innovative communication mechanisms will be needed

- the amount of produced data may be too large to be computed on a Cloud: an approach *à la* Edge Computing will be used

    ....but we like them!
Thank you for your attention

http://www.sunfishproject.eu/