Cross-Cloud Management of Sensitive Data via Blockchain: a Payslip Calculation Use Case

Luca Nicoletti[1], Andrea Margheri[2], Federico Lombardi[2], Vladimiro Sassone[2], and Francesco Paolo Schiavo[3]

[1] SOGEI
lnicoletti@sogei.it
[2] Electronics and Computer Science, University of Southampton
{a.margheri;f.lombardi;vsassone}@soton.ac.uk
[3] Ministero dell'Economia e delle Finanze
francescopaolo.schiavo@mef.gov.it

Abstract

Federating Cloud systems is an urgent need of the Public Sector. In this paper, we showcase a recent Cloud Federation-as-a-Service solution empowered by blockchain technology. This solution is used by the Italian Ministry of Economy and Finance to realise a cross-Cloud application for payslip calculation of Police Forces. Blockchain offers decentralised means to conciliate the need of keeping data protected while ensuring certified computation on it. This solution has been adopted as part of the project CloudifyNoiPA to re-engineer the whole payroll system of the Italian Public Administration.

1 Introduction

Nowadays, the Public Sector is equipped with a large number of private Cloud systems whose administration is becoming more expensive and less effective due to brief usage picks, barriers on flexible resource provisioning, and limited access to distributed data sources. An urgent need is to provide software infrastructures enabling secured and controlled interaction across multiple Cloud systems. The key driver for creating such cross-Cloud systems stands in the access to data and services otherwise not available, and in the better utilisation of computational resources.

Broadly speaking, the governance aspects of cross-Cloud systems are of paramount importance to encourage wide application and foster systematic integration of private Clouds in the Public Sector. European countries such as Italy and France suffer from a large proliferation of small/medium data centres concurrently supporting Public Administrations. This causes inefficiency, costly management and low resource utilisation. To tackle this issue, the SUNFISH project conceived, designed and implemented so-called Federation-as-a-Service (FaaS) [4], an innovative federation approach for Cloud systems that allows small/medium data centres to become first-class citizen in the Cloud provisioning landscape for Public Administrations. FaaS crucially relies on blockchain to realise a first-time democratic and decentralised governance model. Blockchain is exploited as an innovative underlying infrastructure underpinning trustless federated Clouds with data computation integrity and availability.

Blockchain is an innovative technology that besides fascinating properties on data integrity ensures full decentralised control on data and its computation. Upon such decentralised infrastructure, immutable programs named *smart contracts* can execute ensuring non repudiable guarantees to all involved parties. Besides Bitcoin and Ethereum, a large number of blockchain systems targeting private settings such as cross-Cloud integrations have appeared on the market. Hyperledger Fabric (www.hyperledger.org/projects/fabric) is a prominent solution that offers, among others, controls on data visibility and on where smart contracts are executed.

Use Case. The Italian Ministry of Economy and Finance (MEF) is currently facing the issue of overcoming segregation of Public Bodies data among Clouds for calculating payslips of Police Forces. Specifically, the Italian legal framework forces the Ministry of Interior (MIN) to be the exclusive controller of Police Force sensitive data. However, MEF needs access to such data to correctly compute payslips (for the cognitive, local taxes must be computed on actual residence, which is however sealed for data classification purposes within the MIN). To overcome this issue, MEF has put in place an intricate cooperation with MIN which locally performs part of the payroll tax computation then to be used by the MEF. However, this has lead to uncontrolled cooperations prone to mistake and malicious subversions, e.g. to avoid tax payment or to grant huge pay rise all of a sudden. Such frauds are subtle to discover and, most of all, MEF is liable for it even though it has no control on the full payroll data. Therefore, MEF requires different deployment of such use case to introduce adequate computation guarantees both on the used sensitive data and on the performed computations.

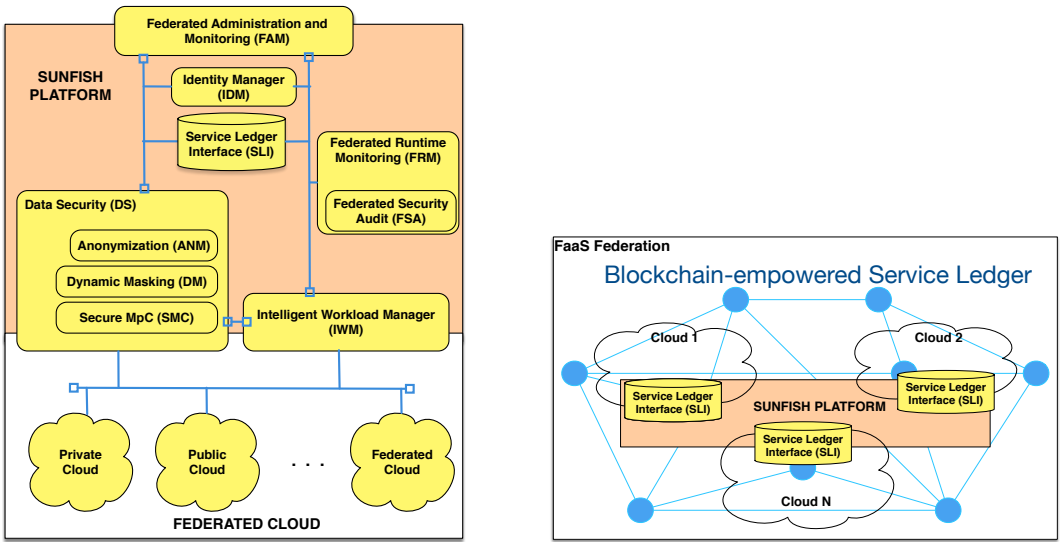
In the following, we first outline the SUNFISH FaaS solution emphasising the role of blockchain, then we comment on its exploitation for the presented use case.

2 The SUNFISH Cloud Federation Solution

Federation-as-a-Service (FaaS) is implemented via the SUNFISH software platform depicted in Fig. 1(a). Crucially, the platform is conceived to be deployed in a distributed manner on top of all federated Clouds, thus to avoid any *centralised control and component*.

The software platform features state-of-the-art Cloud management technology and advanced security and privacy-preserving functionality. Intuitively, we can logically identified components related to *Data Security*, *Federation Monitoring* and *Federation Management*.

The *Data Security* relies on a distributed attributed-based access control system acting as a backbone of the overall infrastructure [5]. Privacy-preserving components secure *storage*,



(a) Software Platform (b) Service Ledger

Figure 1: The SUNFISH FaaS Solution

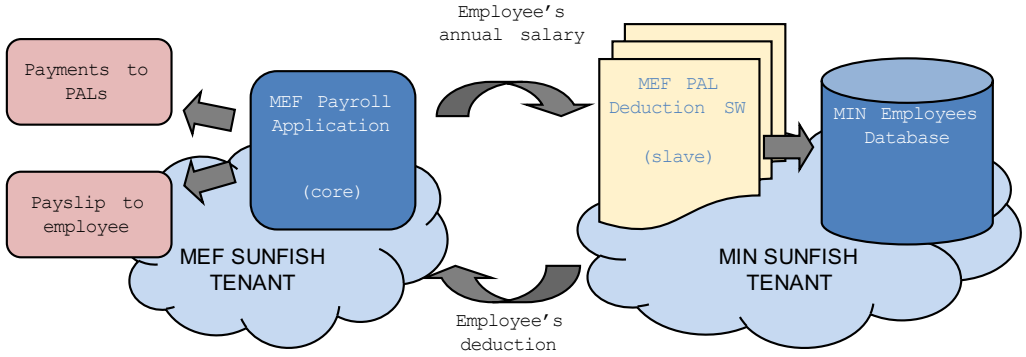


Figure 2: Cross-Cloud Payroll Calculation (where PAL stands for Local Public Administration)

sharing and *computation* of sensitive data; respectively, DM, ANM and SMC components.

The *Federation Monitoring* consists of both a runtime monitoring and offline auditing, the FRM and FSA components, respectively.

The *Federation Management* supports the creation and management of cloud federations. The IWM enforces optimised workload strategies, while the FAM provides an administration console to manage, control and monitor the state of the federation. Notably, via the SLI, all the governance data of a federation, e.g. SLA and access control policies, are stored on the *blockchain-empowered Service Ledger* and make available to components accordingly.

Service Ledger Infrastructure. The corner stone of FaaS is an innovative democratic governance of Cloud federations [3]: none of the federated Cloud rules on the others, but each of them shares the same authorities and duties. The governance is carried out and enforced in a decentralised manner via smart contracts. Besides representing the governance rules negotiated among the federation participants, smart contracts support democratic e-voting and strengthen the security assurance of data security functionality and Cloud applications.

The underlying blockchain infrastructure named *Service Ledger* (see Fig. 1(b)) offers resilient data storage and a decentralised computation facility at hand [1, 2] that alleviates the need for a trusted-third-party and reduces systemic risks of disputes and frauds in cross-Cloud interactions.

To improve security assurance of privacy-preserving services, smart contracts are used to shield key ingredients from tampering attacks, e.g. the key used in the masking process and anonymisation history record of released datasets. Most of all, smart contracts can be used by cross-Cloud application to enjoy decentralised computation and non repudiable guarantees. As a matter of fact, part of the logic of a cross-Cloud application can be moved into a smart contract to benefit of its distinguishing properties.

3 Cross-Cloud Payslip Calculation

To address the use case previously introduced, MEF and MIN must balance two contrasting needs: certifying to MEF the computation of sensitive data, keeping sensitive data within the perimeter of MIN. This potential conundrum can be overcome via FaaS and its blockchain-empowered Service Ledger infrastructure.

Intuitively, the use case can be seen as in Figure 2. The payroll application is split into two parts, one logically placed on MEF to compute the bulk payroll computation and one logically placed on MIN to process localised sensitive data. To realise such infrastructure the

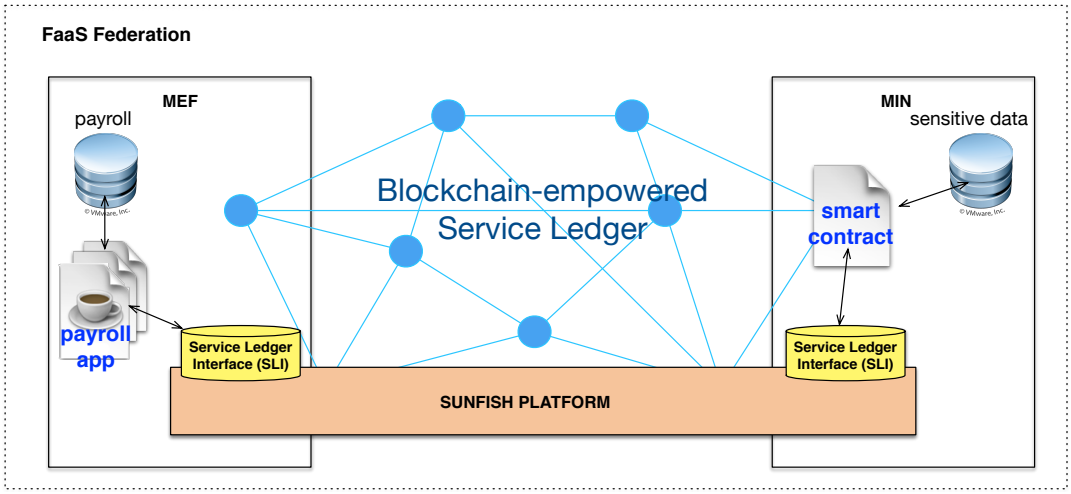


Figure 3: Use Case Architecture (where MIN's smart contract is the certified payroll tax calculation logic provided by the MEF and running on the Service Ledger peer part of the MIN)

following is needed: (i) MEF and MIN Clouds must be securely federated, hence there cannot be unsecured interactions among themselves travelling via the Internet; (ii) MIN's slave payroll application must be tamperproof thus offering to MEF the expected assurances on what is actually computed on MIN side.

From a practical point of view, this boils down to deploy part of the application logic—viz. the MIN's slave—on an infrastructure where there is no single-point-of-control and strong guarantees on logic executions, i.e. non repudiation, accountability and immutability. Such infrastructure is the SUNFISH Service Ledger.

3.1 The SUNFISH Solution

Being the Clouds of MEF and MIN securely federated via FaaS, thus to enable controlled and secured inter-Cloud communication, the SUNFISH Service Ledger can be used to implement the proposed use case achieving all required guarantees on data and code execution. Specifically, we use a smart contract to certify the code computing the local taxes on sensitive data. Such execution will be carried out within the boundaries of the MIN, but it will ensure strong accountability to the MEF.

Practically, the use case is implemented by exploiting the SUNFISH platform as graphically depicted in Figure 3. On the MEF side, the main payroll application is deployed and interacts with the localised payroll datasources. The certified code to compute local taxes is provided by the MEF in the form of a smart contract to be deployed on the Service Ledger. Such deployment prescribes a localised installation (as per Hyperledger's jargon) on one of the peer of the MIN. This peer will then get access to the sensitive data to locally and correctly compute taxes via the smart contract logic. The tax computation will result into an immutable transaction replicated throughout the blockchain (hence also on the MEF side) and will allow MEF to have at disposal all the needed guarantees on computed taxes. Specifically, the generated transactions will store in plain text the computed tax amounts (which are not sensitive as needed for completing MEF's payroll computation) and in an encrypted format the sensitive inputs use by the smart

contract. The latter inputs are encrypted with MIN's private key and they never leave in plain text the MIN Cloud. Such inputs ensure that disputes between MEF and MIN on used data cannot happen and, most of all, constrain liability on managing sensitive data just to the MIN.

To sum up, this principled exploitation of smart contract and blockchain made possible the realisation of a cross-Cloud application otherwise hardly possible. The added value of such Service Ledger is to foster integration between companies (in this case two Public Body Clouds) while keeping effective control on data, service and access to them. As a matter of fact, this solution has been adopted as part of the CloudifyNoiPA project, an innovative Cloud-based solution to re-engineer the whole Italian payroll system for the Public Administration.

4 Conclusion

This use case is a significant blockchain pilot, developed under the SUNFISH project, concerning a cross-Cloud payroll calculation for the Italian Public Sector. Blockchain permits overcoming the fragmentation of fiscal information of the Police personnel across the departments of MIN and MEF, ensuring correctness of tax calculation and payroll accountability. The combined used of encryption, certified smart contract and decentralisation ensures that tax calculation for payroll is correct, that no private data is leaked from MIN to MEF, and that there is no trusted-third-party carrying out part of the computation.

Broadly speaking, the Ministry of Economy and Finance, who coordinates the SUNFISH project, has recognised in practice the great potential of blockchain and is currently leading a national initiative to provide the Italian Public Sector with a blockchain-based infrastructure to foster integration among Government departments and underpin national digital services.

Demonstrator. The use case will be firstly introduced by highlighting its real-world key drivers and challenges to address. Then, the usage of the SUNFISH platform will be demonstrated, both from logical and infrastructural point of views. The cross-Cloud application empowered by the Service Ledger will be showcased pointing out the added value of relying on blockchain.

Acknowledgments

This work has been supported by the EU H2020 project SUNFISH, grant N.644666.

References

[1] Leonardo Aniello, Roberto Baldoni, Edoardo Gaetani, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database. In *EDCC*. IEEE, 2017.

[2] Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Blockchain-based database to ensure data integrity in cloud computing environments. In *ITA-SEC*, volume 1816. CEUR-WS.org, 2017.

[3] Andrea Margheri, Md. Sadek Ferdous, Mu Yang, and Vladimiro Sassone. A distributed infrastructure for democratic cloud federations. In *CLOUD*, pages 688–691. IEEE, 2017.

[4] Francesco Paolo Schiavo, Vladimiro Sassone, Luca Nicoletti, and Andrea Margheri (Eds.). Faas: Federation-as-a-service. *CoRR*, abs/1612.03937, 2016.

[5] Bojan Suzic, Bernd Prünster, Dominik Ziegler, Alexander Marsalek, and Andreas Reiter. Balancing Utility and Security: Securing Cloud Federations of Public Entities. In *C&TC*, volume 10033 of *LNCS*, pages 943–961. Springer, 2016.