Demonstrating Liability and Trust Metrics for Multi-Actor and Dynamic Edge and Cloud Microservices

Yacine Anser
Chrystel Gaber
Romain Cajeat
Jean-Philippe Wary
name.surname@orange.com
Orange Labs
Châtillon, France

Samia Bouzefrane
Méziane Yacoub
CEDRIC Lab, Cnam
Paris, France
name.surname@cnam.fr

Onur Kalinagac
Gürkan Gür
Zurich University of Applied Sciences (ZHAW)
Switzerland
{kalo,gueu}@zhaw.ch

ABSTRACT

Transitioning 5G, edge and cloud computing towards service-based architecture increases their complexity as they become even more dynamic and intertwine more actors or delegation levels. In this paper, we demonstrate the Liability-Aware security manager Analysis Service (LAS), a framework that uses machine learning techniques to compute liability and trust indicators for service-based architectures such cloud microservices. Based on the commitments of Service Providers and real-time observations collected by a Root Cause Analysis (RCA) tool GRALAF, the LAS computes three categories of liability and trust indicators, specifically, a Commitment Trust Score, Financial Exposure, and Commitment Trends.

CCS CONCEPTS

• **Networks → Cloud computing**; • **Social and professional topics → Quality assurance**.

KEYWORDS

Edge and cloud computing, Applications of machine learning, Liability, Trust, Service Level Agreement (SLA)

ACM Reference Format:
Yacine Anser, Chrystel Gaber, Romain Cajeat, Jean-Philippe Wary, Samia Bouzefrane, Méziane Yacoub, Onur Kalinagac, and Gürkan Gür. 2023. Demonstrating Liability and Trust Metrics for Multi-Actor and Dynamic Edge and Cloud Microservices. In *Proceedings of The 29th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '23).* ACM, New York, NY, USA, 3 pages. https://doi.org/XXXXXXX.XXXXXXX

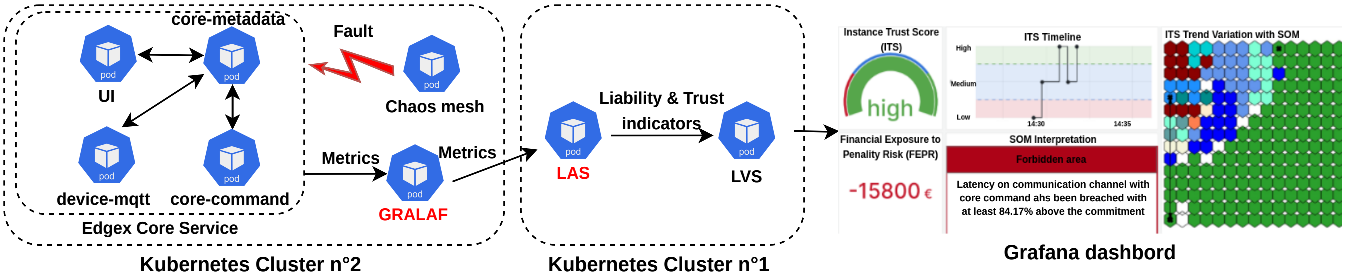
1 INTRODUCTION

Microservice architecture is widely adopted for modern software systems, providing scalability, flexibility, and easy maintenance [2]. By breaking down applications into smaller, independent services with well-defined APIs, microservices enable faster development cycles and independent deployments. They are a cornerstone in the operators' strategy to transition 5G edge and cloud computing towards service-based architecture. However, decomposing applications into independent services results in a dynamic environment characterized by active participation from various stakeholders and hierarchical delegation of responsibilities. Consequently, effective management of liability and trust within microservices architecture presents a significant challenge that must be tackled with. We contribute to address it by creating liability and trust indicators.

This demonstration shows a working prototype of the LAS (LASM Analysis Service), a module of the Liability-Aware Security Manager (LASM) presented in [3, 4]. The LAS computes three categories of liability and trust metrics. The first one is Commitment Trust Scores and aims at categorizing the trust that an instance, all instances of a microservice or all microservices of a provider will behave as expected by the commitments taken in Service Level Agreement (SLAs). The second category, Financial Exposure, measures the amount of money that the overall microservice architecture provider might potentially lose with the current composition of microservices given the SLA violation risk associated with each one of them. Finally, the third category, Commitment Trends, follows trends of SLA Violation Rates (SVR) and Commitment Trust of an instance of microservice.

ACM MobiCom '23, Oct 02-06, 2023, Madrid, Spain

ACM ISBN 978-1-4503-9990-6
Version of Record: https://doi.org/10.1145/3570361.3614086



Latency on communication channel with core command ahs been breached with at least 84.17% above the commitment

Figure 1: Overview of the demo setup

2 FRAMEWORK DESIGN

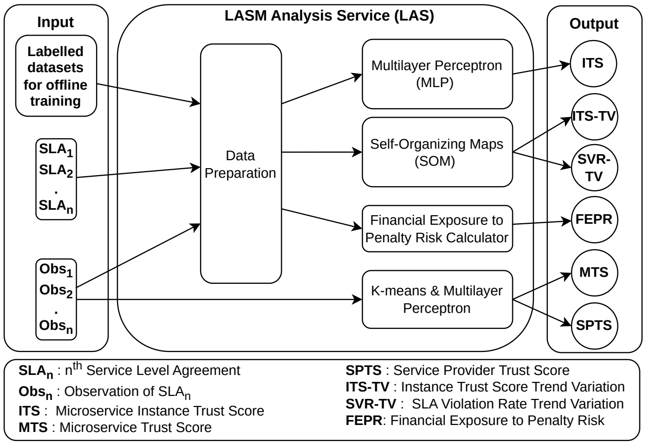

Input
Labelled datasets for offline training
SLA_1
SLA_2
.
SLA_n
Obs_1
Obs_2
.
Obs_n
LASM Analysis Service (LAS)
Data Preparation
Multilayer Perceptron (MLP)
Self-Organizing Maps (SOM)
Financial Exposure to Penalty Risk Calculator
K-means & Multilayer Perceptron
Output
ITS
ITS-TV
SVR-TV
FEPR
MTS
SPTS
SLA_n : n^{th} Service Level Agreement
Obs_n : Observation of SLA_n
ITS : Microservice Instance Trust Score
MTS : Microservice Trust Score
SPTS : Service Provider Trust Score
ITS-TV : Instance Trust Score Trend Variation
SVR-TV : SLA Violation Rate Trend Variation
FEPR: Financial Exposure to Penalty Risk

Figure 2: Overview of LASM Analysis Service (LAS).

Figure 2 highlights the components of the LAS framework. It uses labelled datasets provided by risk management experts, and the SLAs committed by Service Providers to generate the microservice Instance Trust Score (ITS), Microservice Trust Score (MTS) and Service Provider Trust Score (SPTS). To achieve this, it uses a Multi-Layer Perceptron (MLP) - a fully connected feedforward Artificial Neural Network (ANN), and k-means clustering. The LAS computes the Financial Exposure to Penalty Risk (FEPR), inspired by investment metrics [5]. Finally, two types of Commitment Trends are generated. Using a different type of ANN known as a Self-Organizing Map (SOM) [7], the LAS tracks the changes of the ITS and the SLA Violation Risk over time. This generates two other outputs, namely the Instance Trust Score Trend-Variation (ITS-TV) and the SLA Violation Risk Trend-Variation (SVR-TV).

3 SET-UP AND SCENARIO

Figure 1 illustrates the setup for the demonstration, consisting of two Kubernetes clusters. The first cluster hosts the LAS and the LVS (LASM Visualization Service), which is a module based on Grafana used to display the indicators. In the second cluster, we deploy Edgex, an open source framework that facilitates device and application interoperability at the edge of the IoT network [1]. The Edgex service is divided into four sub-services, Each service consists of microservices. For the demonstration, we focused on the core service. In order to calculate the MTS and the SPTS, we deploy Edgex across two additional clusters, resulting in three separate instances. Additionally, we deploy Chaos Mesh, an open-source platform that simulate various failure scenarios. The LAS receives service metrics from the GRALAF (Graph-Based Liability Analysis Framework) described in [6]. The provider of core service committed to three SLAs namely availability (SLA_0), latency (SLA_1), and error rate (SLA_2). In this demonstration, we are going to deliberately violate this SLAs and monitor the progression of the liability and trust indicator on the Grafana dashboard. For that, we use chaos variables provided by Chaos Mesh. These variables include network outages, memory and CPU stress, latency injection, and pod termination events. Table 1 exhibits a representative sample within the scenario demonstrated with the evolution of the ITS. intially, the service achieves a steady state, meeting all SLAs. Subsequently, we initiate service degradation by violating the SLAs. As the service degrades further, the ITS decreases. During the demonstration, we'll introduce complex scenarios by disturbing the three instances. Participants can explore MTS, SPTS, and ITS-TV using a SOM map.

Table 1: A scenario's representative sample (TW : Time Window, Comply : as expected, ↓ : lower than expected, ↑ : higher than expected)

	TW0	TW1	TW2	TW3	TW4	TW5
SLA_0	Comply	Comply	0.0053% ↓	Comply	0.0053% ↓	Comply
SLA_1	Comply	13% ↑	Comply	48% ↑	Comply	10% ↑
SLA_2	Comply	Comply	Comply	Comply	13% ↑	9% ↑
ITS	High	Medium	Low	Low	Low	Low

REFERENCES

[1] 2022. EdgeX Foundry homepage. https://www.edgexfoundry.org.

[2] Nuha Alshuqayran, Nour Ali, and Roger Evans. 2016. A Systematic Mapping Study in Microservice Architecture. In *2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA)*. 44–51. https://doi.org/10.1109/SOCA.2016.15

[3] Yacine Anser, Chrystel Gaber, Jean-Philippe Wary, Sara Nieves Matheu García, and Samia Bouzefrane. 2022. TRAILS: Extending TOSCA NFV profiles for liability management in the Cloud-to-IoT continuum. In *2022 IEEE 8th International Conference on Network Softwarization (NetSoft)*. 321–329. https://doi.org/10.1109/NetSoft54395.2022.9844027

[4] C. Gaber, J. S. Vilchez, G. Gür, M. Chopin, N. Perrot, J.-L. Grimault, and J.-P. Wary. 2020. Liability-Aware Security Management for 5G. In *2020 IEEE 3rd 5G World Forum (5GWF)* (2020-09). 133–138. https://doi.org/10.1109/5GWF49715.2020.9221407

[5] Philippe Jorion and GARP (Global Association of Risk Professionals). [n. d.]. *Financial Risk Manager Handbook*. John Wiley & Sons. Google-Books-ID: uGgrMwDfBRsC.

[6] Onur Kalinagac, Wissem Soussi, and Gürkan Gür. 2023. Graph Based Liability Analysis for the Microservice Architecture. In *Proceedings of the 18th International Conference on Network and Service Management* (Thessaloniki, Greece) *(CNSM '22)*. International Federation for Information Processing, Laxenburg, AUT, Article 51, 3 pages.

[7] T. Kohonen. 1990. The self-organizing map. *Proc. IEEE* 78, 9 (Sept. 1990), 1464–1480. https://doi.org/10.1109/5.58325 Conference Name: Proceedings of the IEEE.