End-to-end data protection through the computing continuum in smart environments

Klaas Baert*, João Garcia †, Jens Kuhr‡, Eliot Salant§, Robert Seidl‡and Ricardo Vitorino†

*VRT, Belgium. Email: klaas.baert@vrt.be
†Ubiwhere, Aveiro, Portugal. Emails: {jmgarcia, rvitorino}@ubiwhere.com
‡Nokia, Germany. Emails: {jens.kuhr, robert.seidl}@nokia.com
§IBM Haifa Research Labs. Email: salant@il.ibm.com

ABSTRACT — FOGPROTECT:

Protecting Sensitive Data in the Computing Continuum is a Research and Innovation action funded by the European Union's Horizon 2020 Programme. It delivers new and advanced architectures, technologies, and methodologies for ensuring end-to-end data protection across the computing continuum, from cloud data centres through fog nodes to end devices. This paper introduces three real-world use cases that demonstrate the applicability of FogProtect solutions in multiple contexts and the impact of the project's novel solutions for data protection. Three complementary smart environments demonstrate the applicability of FogProtect solutions to multiple contexts and the impact of the project's novel solutions for data protection: smart cities, smart manufacturing and smart media.

I. INTRODUCTION

FogProtect combines four main technology innovations: (1) secure data container technology for data portability and mobility, (2) data-protection-aware adaptive service and resource management, (3) advanced data protection policy management, (4) dynamic data protection risk management models and tools [1]. FogProtect provides the essential building blocks to empower data protection, supporting resilience, trustworthiness and human centricity in the Next Generation Internet. The FogProtect solutions are generic and can be used in multiple contexts to support many types of applications and services. Three complementary real-world use cases demonstrate the applicability of FogProtect solutions to multiple contexts and the impact of the project's novel solutions for data protection: smart cities, smart manufacturing and smart media.

II. SMART CITIES

The Smart Cities scenario (Fig. 1) describes a network of CCTV Cameras (Closed Circuit Television) that monitor selected places of a city. The acquired data can be accessed by First Responders that can request the original video data from the fog nodes to evaluate additional steps. To protect the citizens' privacy, the data must be secured from unauthorized access. Therefore, the CCTV Cameras are connected to fog nodes that pre-process the received video streams effectively anonymising sensitive data from the videos. In order to anonymise the captured video, Convolutional Neural Networks are used to detect personal data (i.e. people in the video). When a detection is made, the area of the detection is blurred, hiding the personal data but allowing the video to still be visualized. The video stream and extracted meta data are sent to a Cloud Centre which streams the anonymous video with additional analytic data and detected incidents to an external Monitoring Platform. This Monitoring Platform is hosted on a third-party cloud platform and can receive incident reports from multiple sources, such as pedestrians reports sent through a mobile application.

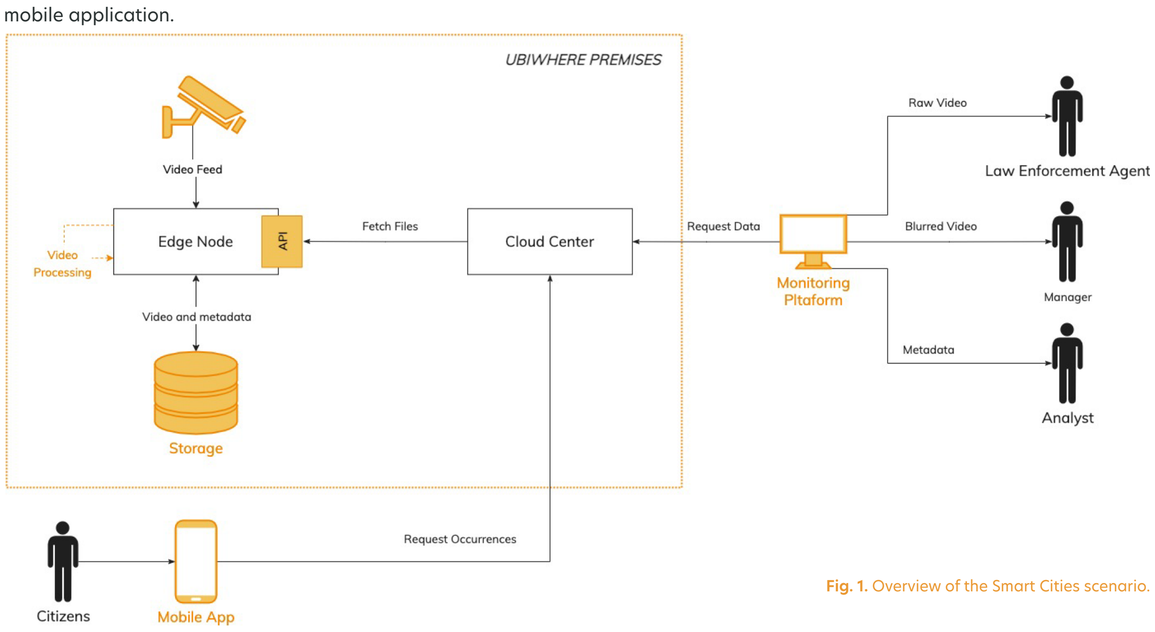

Fig. 1. Overview of the Smart Cities scenario.

FogProtect ensures that the correct security measures are in place in order to avoid data leakage and data theft along the whole data pipeline that takes the video feed from the camera in the fog to the authorised end-users accessing it from the cloud. The transmission, processing and storage of the data from the Fog Node require different types of care at each stage. Using FogProtect's capabilities, the correct policies can be put in place to guarantee that no unauthorised person can access or interfere with the personal data involved in this Use Case. Furthermore, given the possibility that the location of each component of the system may change, FogProtect ensures that the correct policies are in place to accommodate these changes.

III. SMART MANUFACTURING

The Smart Manufacturing scenario (Fig. 2) describes a process using the capabilities of the cloud and a shipping container equipped with robots and computing resources to eliminate non-value-adding transportation time. The cloud holds all necessary data for the manufacturing of products and is divided into two parts. The first one is responsible for storing information like orders and details about the production process, and is hosted by a Third Party SaaS Provider. The shipping container is equipped with machines to manufacture products that are ordered by Customers through the cloud.

Using this container makes it possible to produce or refine a specific product during the time in which raw material is shipped overseas by also transporting the needed machines. Moreover, this smart manufacturing environment can help in overcoming shortage of manufacturing capabilities, as it can be placed next to a grounded factory in need of additional manufacturing capabilities.

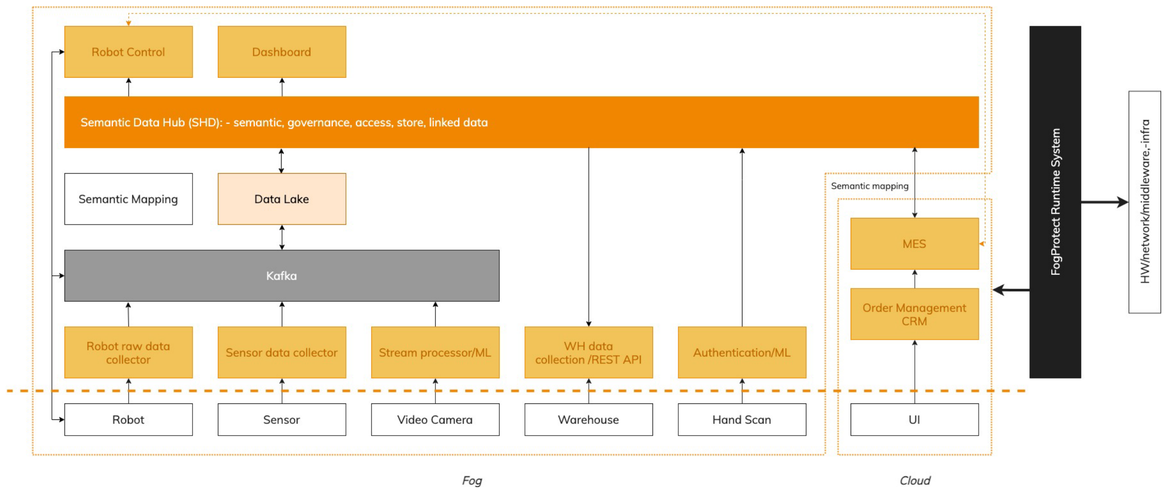

Fig. 2. Overview of the Smart Manufacturing scenario.

From the various ways FogProtect can help to improve security for a Factory-In-A-Box solution, three aspects are of immediate benefit. Currently, the external access from cloudbased software or from an administrator requires hard-coded VPN connections, password protection and a manual credential administration. FogProtect automates the risk analysis, the deployment and the configuration of protection technologies. The shipping container also hosts many different compute units with different levels of security measures. It is expected that there will be frequent rearrangements of the software components, requiring automated adjustment of security measures, which turns out to be an important feature for remotely located manufacturing sites. Lastly, a technology that enables detailed configuration of application-specific data access helps data sharing within a manufacturing ecosystem.

IV. SMART MEDIA

The Smart Media scenario (Fig. 3) features the possibility to contribute user-generated videos recorded either on a Smartphone or in a portable video booth to a video production. A component called Chatterbox Service which is located in the cloud provides a set of questions. These questions are made available to the Guest via a computer which is located in a portable video booth, where videos can be recorded with a professional Camera. The videos are stored on an external HDD Storage if there is no sufficient bandwidth for the connection to the cloud. AI Services located in both the cloud and the portable video both are used to analyse the videos and extract metadata from them, which are of two types. The first one is directly provided by the Guest and includes personal data like contact information. The second one are the metadata that are extracted from the videos by the AI Service, such as: the time it takes a Guest to answer the questions and the emotions he or she displays while answering the questions. The meta data are stored in the cloud. The HDD Storage and the Computer are considered to be fog nodes and the AI Service in the portable video booth is hosted by within a fog node. A Story Maker component, which is located in a second cloud, can access the video and the metadata. The Story Maker is used to generate editorial videos using the videos and their metadata. It only accesses the files for processing and does not store the video itself.

FogProtect ensures that the correct security measures are in place in order to avoid data leakage along the whole media meta data pipeline that records a video message and makes it, together with the according metadata, available from the cloud to the authorised end-users, that might belong to different organizations. The access to personal data is restricted and may differ between certain roles of authorised users. With FogProtect, it is possible to define and enforce the necessary security and access policies in a centralized location.

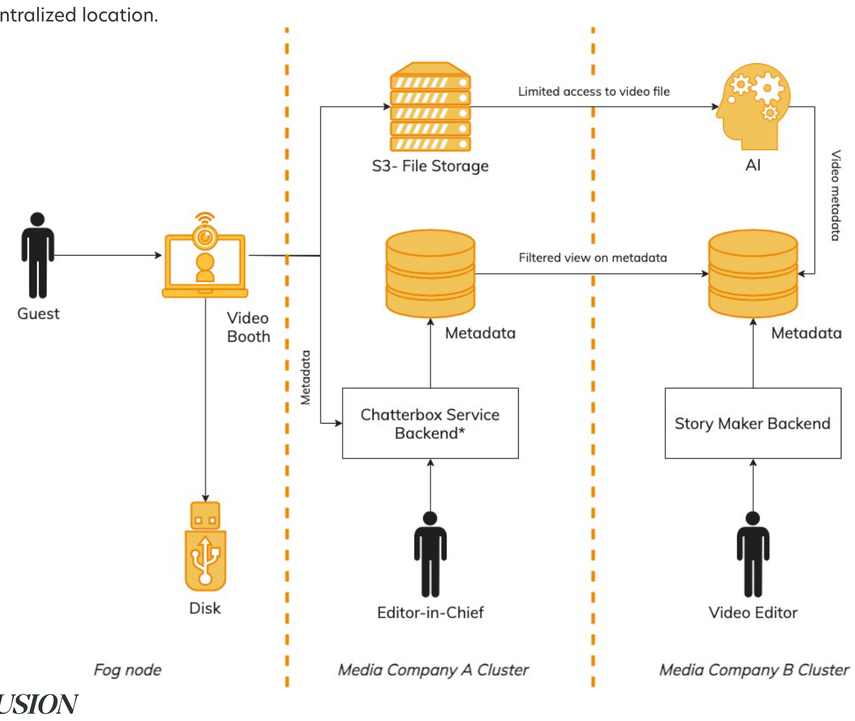

Fig. 3. Overview of the Smart Media scenario.

V. CONCLUSION

While the integration of the FogProtect architecture within the presented scenarios is ongoing, this poster abstract leverages on the innovation aspects that have been identified up to this moment and that can be extrapolated to virtually any smart scenario in the cloud computing that deals with security issues. The agnostic FogProtect solution brings different innovative aspects to a wide range of smart environments. In smart manufacturing, FogProtect enables GDPR compliance for legacy software applications. For the smart city environment, the added value resides in the implementation of a city surveillance system over a framework that provides data privacy and assesses risk out of the box. For the smart media environment, the novelty resides in the implementation of a safe, privacy aware, physical video booth and user generated content management platform with enhanced risk assessment.

ACKNOWLEDGMENT

The research leading to these results has received funding from the **European Union's Horizon 2020 Research and Innovation Programme** under grant agreement **No. 871525**. The authors would like to acknowledge the FogProtect Consortium, who contributed conceptually to the work presented in this paper.

REFERENCES

[1] D. Ayed, E. Jaho, C. Lachner, Z. Mann, R. Seidl, and M. Surridge, "Fogprotect: Protecting sensitive data in the computing continuum," in 8th European Conference on Service-Oriented and Cloud Computing (ESOCC), (online), Oct. 2020.