Contribution ID: **112** Type: **Oral Presentation**

Secure Cloud-Native Infrastructure for AI-Based Tumor Tissue Analysis: A Collaborative Approach

Thursday, 19 March 2026 11:22 (22 minutes)

The integration of artificial intelligence (AI) into biomedical research is transforming the analysis of complex datasets such as high-resolution images of tumor tissues. As part of a collaboration between the Italian EOSC and BBMRI-ERIC nodes, INFN and BBMRI-ERIC have launched a joint initiative to define and deploy a secure and scalable infrastructure capable of supporting AI-driven workflows for histopathological image analysis. This effort has been supported by the CERIT-SC team at Masaryk University, which successfully hosts a small-scale, secure, AI-ready computing environment known as SensitiveCloud.

INFN contributed by designing and deploying a cloud-native platform tailored to the specific requirements of medical data handling within an Information Security Management System (ISMS). The ISMS infrastructure is built on a Kubernetes (K8s) cluster composed of virtual machines provisioned via OpenStack. Each VM runs a hardened operating system, and the cluster is orchestrated using RKE2 with Center for Internet Security (CIS) benchmarks enforced, ensuring compliance with best practices for secure configuration.

To facilitate controlled access to applications and data, the platform integrates Keycloak as an external identity and access management system. This setup enables federated authentication and fine-grained authorization policies, supporting multi-institutional collaboration while preserving data privacy and integrity. Integration with the LifeScience Authentication and Authorization Infrastructure (AAI) is currently under evaluation to further enhance interoperability and user trust. This system underpins authentication in the BBMRI-ERIC EOSC Node and is fully compatible with the EOSC AAI, including support for government-backed eID identities.

The infrastructure hosts AI pipelines designed to analyze digitized tumor tissue samples, leveraging deep learning models for feature extraction, classification, and pattern recognition. These workflows are containerized and deployed within the RKE2 cluster, benefiting from the elasticity and isolation provided by Kubernetes. The entire infrastructure was developed as part of the BioMedAI project at Masaryk University and transferred to INFN as Docker containers for the relevant components (mlFlow, JupyterHub with custom images, xOpat viewer). The platform also supports reproducibility and traceability through integrated logging and monitoring tools.

These activities demonstrate the synergy between infrastructure providers and domain experts, paving the way for scalable, secure, and privacy-preserving AI applications in the health and life sciences.

Primary authors: SINISI, Francesco (INFN); BRÁZDIL, Tomáš (Faculty of Informatics, Masaryk University); COSTANTINI, Alessandro (INFN); GASPARETTO, Jacopo (INFN); HEJTMÁNEK, Lukáš (Institute of Computer Science, Masaryk University); HOLUB, Petr (BBMRI-ERIC & Institute of Computer Science, Masaryk University); HORÁK, Jiří (BBMRI-ERIC & Faculty of Informatics and Institute of Computer Science, Masaryk University); MARTELLI, Barbara (INFN); MUSIL, Vit (Faculty of Informatics, Masaryk University); SERGI, Giusy (INFN); TUERK, Andreas (BBMRI)

Presenter: SINISI, Francesco (INFN)

Session Classification: Infrastructure Clouds and Visualisations - I (11:00 - 12:40)

Track Classification: Track 8: Infrastructure Clouds and Virtualizations