Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

Leveraging confidential computing technologies for secure medical image processing: the ENCRYPT initiative

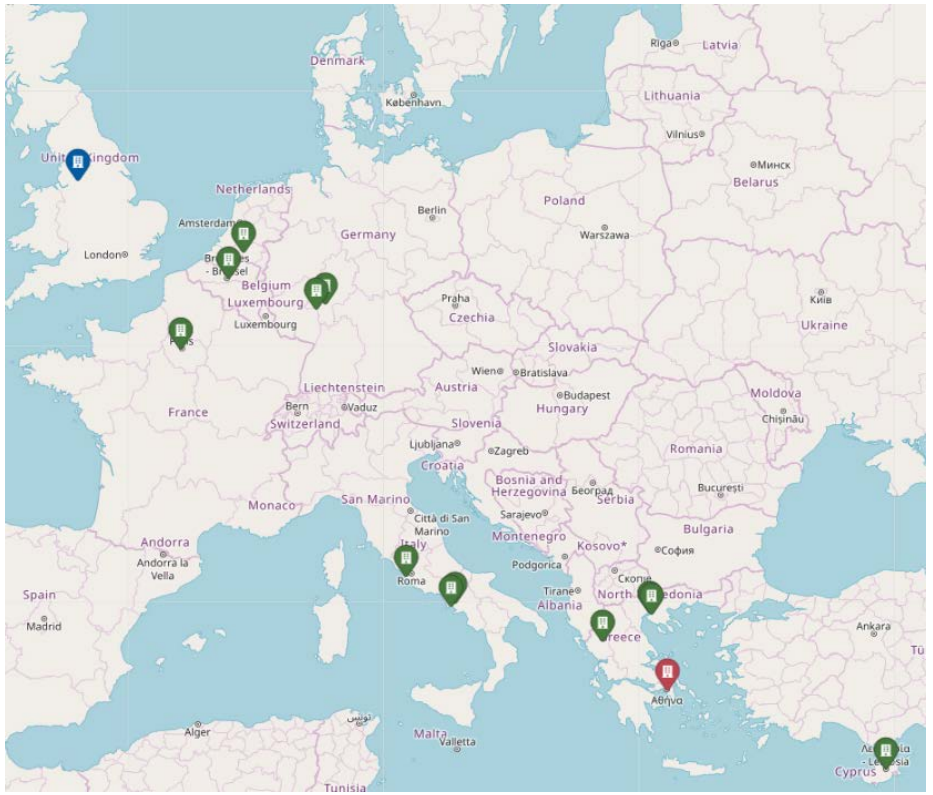
HEALTHCARE CLAIMS FUTURE Workshop, Cesena, December 13th, 2023

Salvatore D'Antonio [TRUSTUP – University of Naples Parthenope]

ENCRYPT Facts and Figures

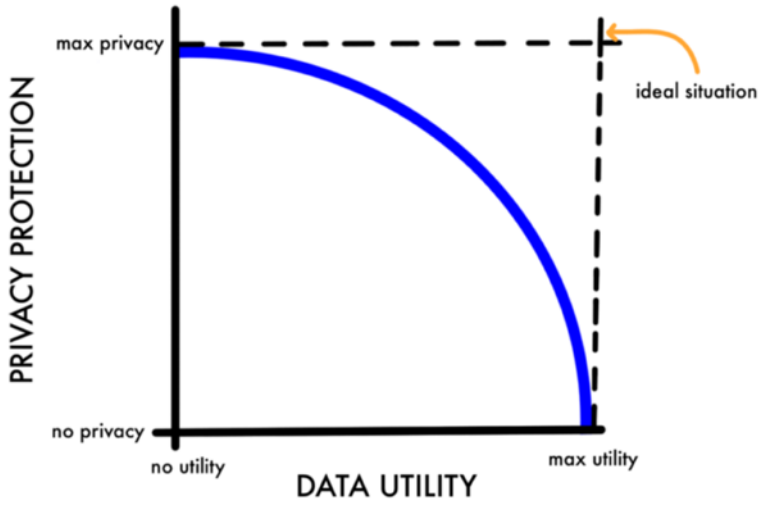
- **Project Short Name:** ENCRYPT (A SCALABLE AND PRACTICAL PRIVACY-PRESERVING FRAMEWORK)
- **Grand Agreement ID**: 101070670
- **HORIZON-CL3-2021-CS-01-04** - Scalable privacy-preserving technologies for cross-border federated computation in EU involving personal data
- **Funding Scheme:** Research and Innovation Action (RIA)
- **Total Funding:** 4,392,540 €
- **Duration:** 36 Months (July 2022 – June 2025)
- **Consortium:** 14 partners, 8 countries
  - ✓ 1 start-up (TRUSTUP)
  - ✓ 3 x SMEs (EXUS, 8BELLS, DBC)
  - ✓ 2 x Enterprises (ENG, EPIBANK)
  - ✓ 8 Research Institutes (CERTH, AUTH, UNIMAN, TIU, CEA, UNINA, GUF, UMC-Mainz)

- **Coordinator:** EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS (EXUS) – Greece
- **Website**: https://encrypt-project.eu/



Challenges and ENCRYPT Vision

- Huge amounts of data are available in new fields, such as Industry 4.0, Health, Finance, and Research
  - ✓ In some cases the need arises to deal with sensitive information
  - ✓ Researchers and service providers working with personal data need to process them in a privacy-preserving fashion
  - ✓ State-of the-art Privacy-Preserving technologies, such as Homomorphic Encryption, Differential Privacy, suffer from scalability issues
  - ✓ Trade-off between privacy protection and data efficiency



- ENCRYPT will deliver a scalable, practical, adaptable privacy-preserving framework facilitating the GDPR-compliant processing of data stored in federated cross-border data spaces by exploiting
  - Privacy-preserving computation technologies
  - Supporting technologies, including a recommendation system and a methodological framework to assess the level of privacy risk and the impact of a data breach on enterprise or organizational goals and objectives
  - Validation in 3 real-world use cases

encrypt

ENCRYPT High Level Objectives

1. To **improve the applicability** and **performance** of Privacy-Preserving technologies towards GDPR compliant, cross-border federated processing of sensitive data by developing an integrated service platform

2. To **improve the user-friendliness** of Privacy-Preserving technologies by facilitating their identification, understanding, selection, and adoption **by all involved actors**

3. To foster and inherently support **interoperability of** Privacy-Preserving **processing technologies when dealing with similar data types** across different organisations and across different sectors

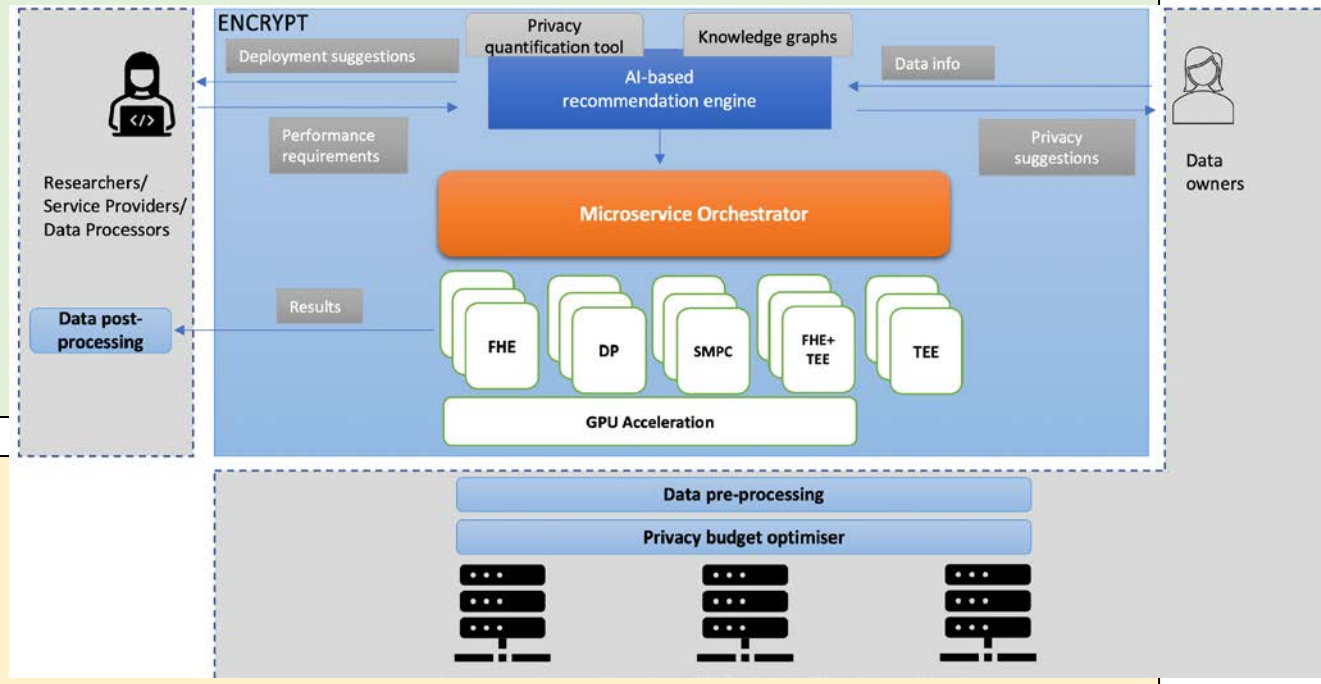
4. To promote GDPR-compliant common **European Data Spaces** and facilitate the **exchange of information**, liaising with relevant initiatives and projects

5. To ensure the **applicability** of the developed solutions, by **co-designing them with end-users**, and validating them in **realistic use cases** including federated data infrastructures

6. To **strengthen the ecosystem** of open-source developers and researchers of privacy-preserving solutions by disseminating and exploiting open-source project results

ENCRYPT Key Technologies and results

- **Privacy –Preserving Computation Solutions**
  - ✓ Fully Homomorphic Encryption (FHE)
  - ✓ Trusted Execution Environment (TEE)
  - ✓ Differential Privacy (DP)
  - ✓ Combined FHE+TEE, FHE+DP
  - ✓ Acceleration Service based on GPU hardware



- **Privacy-Supporting Tools**
  - ✓ Advanced data-preprocessing
  - ✓ Knowledge Graphs
  - ✓ Methodological Framework for privacy risk assessment
  - ✓ AI–powered Recommendation system
  - ✓ Front-end and back-end services

encrypt

Use cases and cyber risk differentiation

Health domain: Cooperative Oncology	Cybersecurity domain: Cyber Threat Intelligence information sharing	Fintech domain: Data Analytics
Cybersecurity risk: security-induced safety implications	Cybersecurity risk: data breaches and illegal use of CTI information	Cybersecurity risk: data subject reidentification

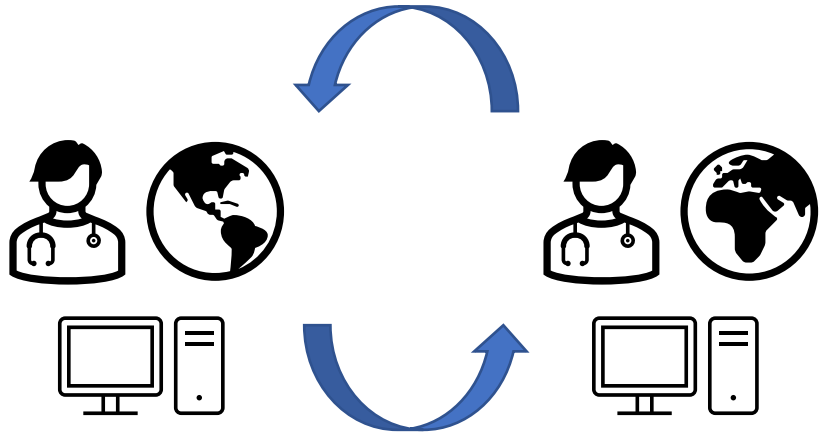
ENCRYPT Use Case in the health domain: Cooperative oncology

Description

- Cancer management is a very challenging task
- Different medical specialists from various medical disciplines need to cooperate in order to evaluate and analyze the same patient from different perspectives
- In case of radiotherapy treatment, continuous exchange of information between different actors as well as between technological equipment is necessary
- Health care professionals (HCP) need to process and share large amounts of medical data, often in real time and across different hospitals or units
- Data integrity and confidentiality are essential requirements to be met by data processing systems

Sub Use case #1: UNINAREPORT

- Patient comes to the institute for diagnostic tests
- Personal data (name, date and place of birth, address, telephone number) are given to the administrative office to insert the patient into the hospital database system
- Physicians collect clinical data and imaging procedures are performed by a physician and a radiology technician
- Patients may undergo ultrasound (US) imaging, radiography, computed tomography (CT), magnetic resonance imaging (MRI), positron emission tomography (PET) or other nuclear medicine procedures, according to the clinical needs
- The physician, after evaluating the images, writes up the report

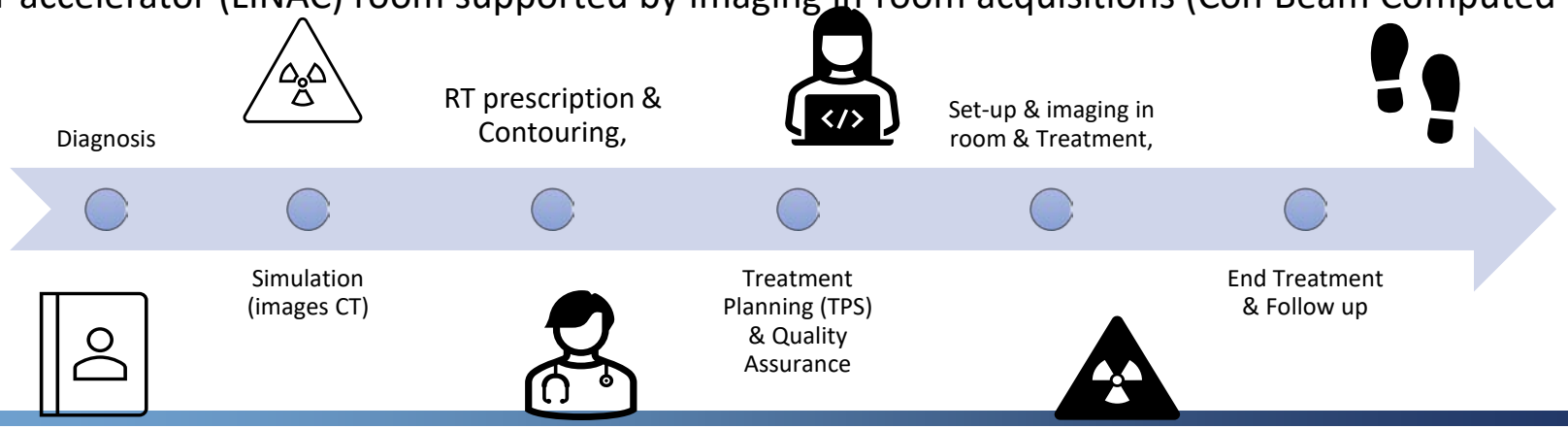


Sub Use case #1: UNINAREPORT

- ✓ **Usage scenario #1: Cooperative reporting** → Radiologist needs to consult another radiologist from a different hospital, for a second opinion
- ✓ **Usage scenario #2: Multidisciplinary team** → Clinical case needs to be further analysed by a surgeon, an oncologist, a radiotherapist, and another radiologist from other departments or hospitals to review all the clinical data and images, and to make the clinical/therapeutic decision
- ✓ **Usage scenario #3: Quality control** → Technician notices that the acquired images need a double-check quality control or he/she deems different imaging reconstruction by external software necessary to perform a more accurate measurement of the malignant mass

Sub Use case #2: UNINART

- After cancer diagnosis is confirmed, patient is moved to the Radiotherapy Unit
- Malignant tumor must be identified (size, position) through imaging (CT, PET, MRI)
- Radiotherapist determines whether treatment is necessary
- Simulation CT scan is performed to identify the exact position of the tumor and to draw its contours (contouring system)
- Later, the case is passed to the medical physicist for treatment planning
- The treatment plan is approved by the radiotherapist
- The medical physicist provides the quality assurance protocol by a Quality Assurance Phantom (dose measurement and verification, QA system)
- Data are entered into a Record and Verify System, used to store and control the planned and delivered data
- Patient set-up is performed in the Linear accelerator (LINAC) room supported by imaging in-room acquisitions (Con Beam Computed Tomography, CBCT)
- The scheduled treatment is delivered



encrypt

Challenges of ENCRYPT Medical domain use case

Problem statement

- Personal and sensitive data (metadata) are accessible to all the doctors and researchers who can login to the hospital system
- Medical images (DICOM files) acquired by diagnostic scanner are visible to doctors, technicians and other professionals, and are stored/transferred to the Picture Archiving and Communication System (PACS)
- Reports are written using the Radiology Information System (RIS)
- Treatment data and machine log files are transferred between the systems involved in the radiotherapy workflow: PACS, contouring and co-registration system, treatment planning system, quality assurance phantom, Record and Verify System, linear accelerator.
- The state-of-the-art data protection measure consists in removing the sensitive data by implementing a non-standardized anonymization procedure

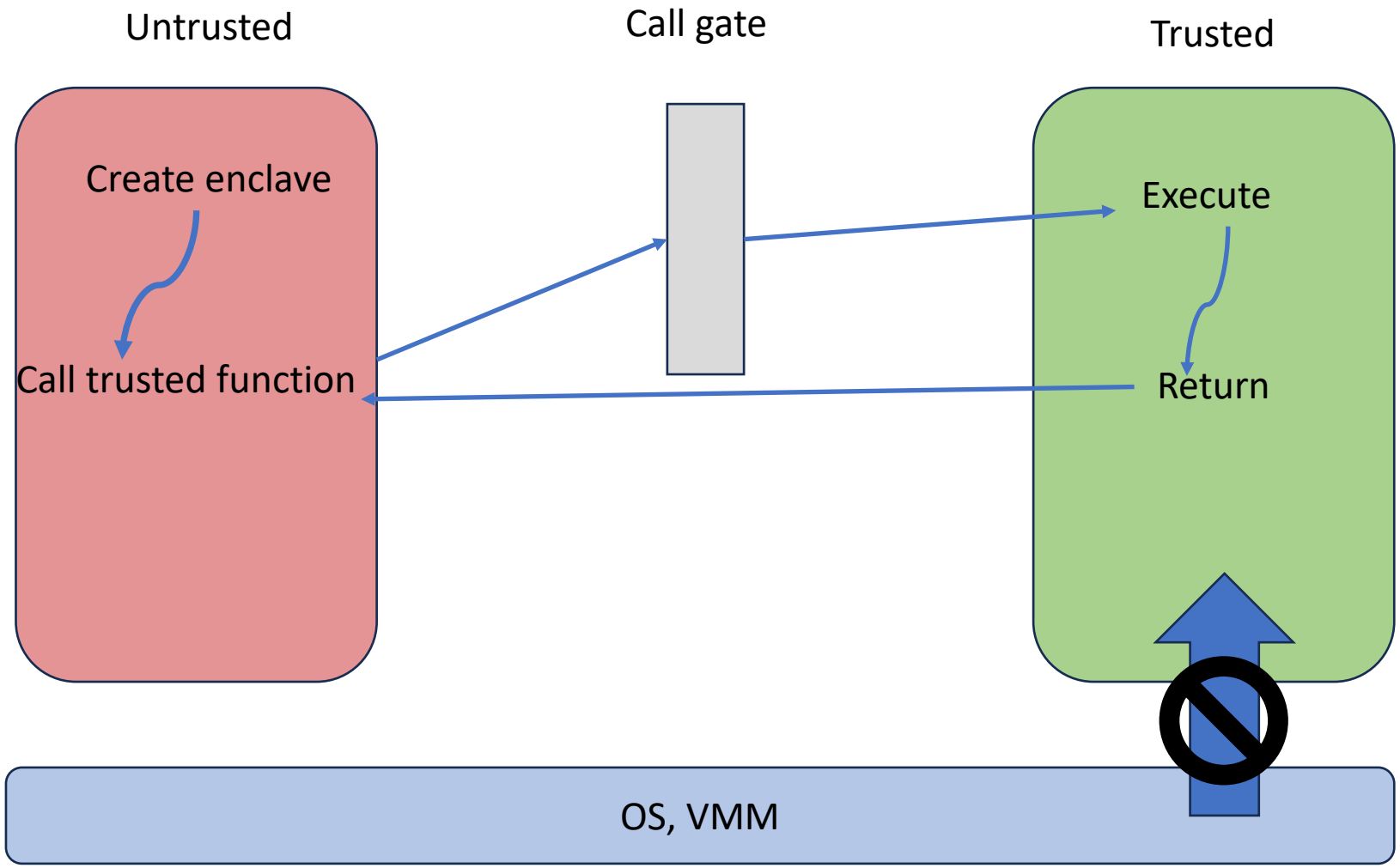
ENCRYPT Privacy-preserving Technologies - TEE

- While standard secure protocols and technologies already exist to protect data in transit, ENCRYPT is focusing on security of data in use and confidential computing
  - ✓ Use of Trusted Execution Environment Technologies (Intel SGX, ARM TrustZone, AMD SEV)
  - ✓ wrt Intel SGX, an extension to CPU ISA allows user-level code to allocate private regions of memory, called Secure Enclaves
  - ✓ The trust model foresees that everything outside the secure enclave is untrusted, including the OS, Hypervisor, and firmware
    - This implies that system calls are not allowed in the enclave
  - ✓ Limitation: enclave page cache (EPC) size

TEE functionalities

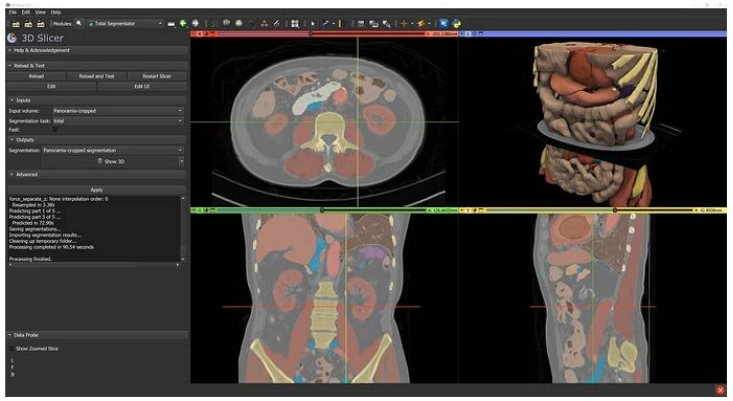
- An isolated environment for code execution that cannot be accessed or manipulated by other software running on the same platform
- A remote attestation mechanism that ensures the integrity of code loaded into TEE
- A tamper-resistant design to ensure that data used inside of the TEE cannot be accessed or manipulated externally and that data never leaves the TEE without being encrypted

Intel SGX architecture



Data processing by 3D-Slicer

- ✓3D Slicer is a free, open-source largely used software tool for visualization, processing, segmentation, registration, and analysis of medical, biomedical, and other 3D images and meshes
- ✓It includes an application for visualization and analysis of medical images data sets. Specifically, analysis tasks performed by 3D Slicer include segmentation, registration, and various quantifications
- ✓Data sets supported by 3D Slicer comprise images, segmentations, surfaces, annotations, transformations in 2D, 3D, and 4D
- ✓In the context of the UNINART use case 3D slicer represents a powerful tool thanks to the 3DslicerRT extension
- ✓Although it has not a direct clinical application yet, 3DslicerRT allows for offline management of data used in Adaptive RT and Image-Guide-RT scenarios as well as dose comparison between different algorithms and treatment planning systems



encrypt

TEE-secured Machine learning -1

- Machine Learning framework TensorFlow is a flexible, high-performance serving system for machine- learning models designed for production environments
- It leverages an end-to-end PPML (Privacy-Preserving Machine Learning) solution based on Intel® Software Guard Extensions (SGX) technology
- LibOS Gramine is used to run TensorFlow Serving into Intel® SGX Enclave, with no source code changes
- Secure capability of protecting the confidentiality and integrity of the model is provided, by establishing a secure communication link from end-user to TensorFlow Serving with mutual Transport Layer Security (TLS) authentication

TEE-secured Machine learning -2

- To verify the untrusted runtime hardware environment, the solution uses the Remote Attestation of Intel® SGX technology to verify the Intel® SGX Enclave, where the applications are running
- To keep models out-of-enclave at-rest safe, this solution encrypts models with cryptographic (wrap) key and sends these protected files to the remote storage accessible from the Intel® SGX platform
- To keep data in-transition safe, this solution establishes a secure channel by using a private key and certificate generated from the client to support avoidance of illegal access
- It also encrypts the key and certificate with a wrap key to avoid any man-in-the-middle attacks and put them in TensorFlow Serving

Conclusions

- Using the ENCRYPT platform, the protection of data communication between health care professionals is ensured
- The ENCRYPT features allow the user to protect DICOM image metadata and annotation data while they are in use
- Critical functions of medical image processing and segmentation software are executed inside TEE
  - ✓ Code and data are protected even from cyberattacks launched by high-privilege users
- Data and code integrity is ensured and patient's privacy is preserved

Thanks a lot for your attention !

Contact info: salvatore.dantonio@uniparthenope.it