# Homomorphic Encryption for EDSS Classification: Safeguarding Patient Privacy in MRI-Based Assessment of Multiple Sclerosis

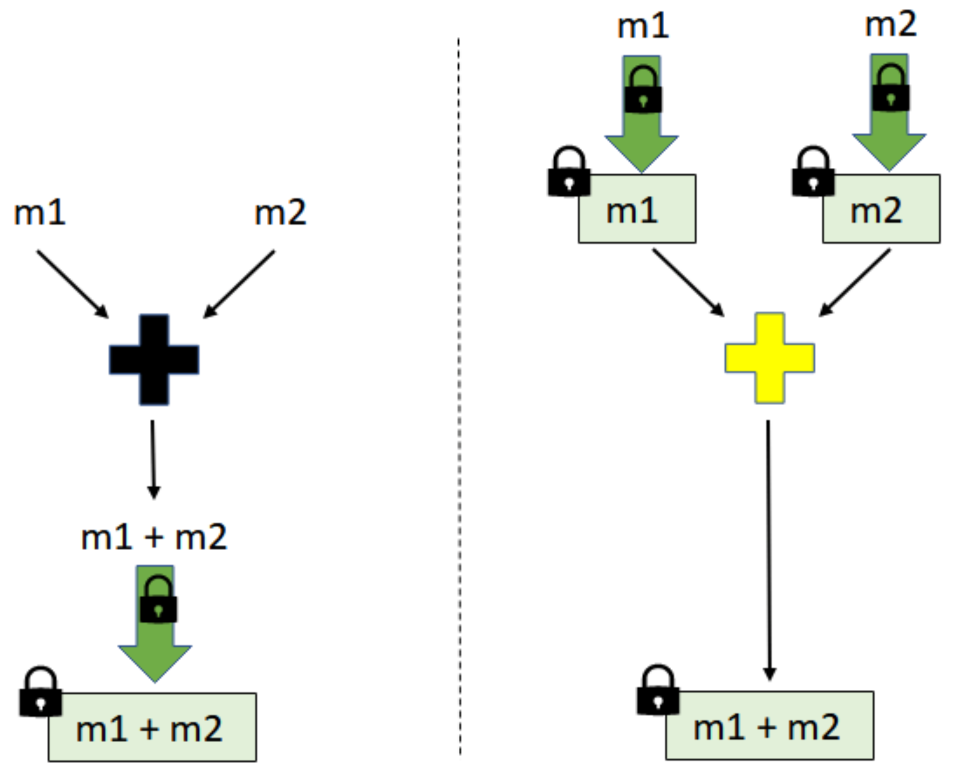
**Stefano Cirillo**, Vincenzo Deufemia, Luigi Di Biasi,
Giuseppe Polese, Giandomenico Solimando, Genoveffa Tortora
University of Salerno
Department of Computer Science
scirillo@unisa.it

# Barriers to Data Sharing in Healthcare

- Hospitals collect large amounts of **sensitive patient data**
  - MRI Scans, Clinical Records, OCT, …
- These data are essential for **developing Computer-Aided Diagnosis** (**CAD**) and **Clinical Decision Support Systems** (**CDSS**)
- Main challenge: Strict Privacy and Security Constraints limit data sharing
- **Risks**:
  - Accidental Exposure, Misuse, and Re-Identification of patients
- **Consequences**:
  - Slow development of collaborative diagnostic systems and AI-based models
  - Hospitals (often) **don't share** their data!

# Homomorphic Encryption

- A cryptographic technique that enables computations directly on encrypted data without requiring decryption
- Results remain encrypted and can only be accessed by authorized parties with the secret key.
- **Advantages in healthcare**:
  - **Continuous protection** of sensitive **patient data** during analysis and inference.
  - Enabling **collaborative learning across institutions** without exposing raw data
  - Securely compute encrypted data **as if it were unencrypted**!



# Multiple Sclerosis

- Multiple sclerosis (MS) is a **chronic autoimmune disease of the central nervous system** in which the immune system mistakenly attacks the **nerve fibers**, leading to disrupted communication between the **brain** and the **rest of the body**

### MS neurologists

**700**
neurologists who specialise in MS. This means there is 1 MS neurologist for every 182 people with MS

### MS nurses

**350**
nurses who specialise in MS. This means there is 1 MS nurse for every 364 people with MS

**The latest edition of the Atlas of MS shows there are 2.9 million people living with multiple sclerosis around the world.**

The Atlas of MS is a powerful advocacy tool for MS organisations and advocates to drive policy changes that can remove obstacles for people with MS and their families in their country. The data is a key way of shining a spotlight on MS to increase awareness and understanding around the world.

atlasofms.org/fact-sheet/italy

### Who is affected?

**30**
years is the average age of an MS diagnosis.

**67%**
of people with MS are women.

### Number of people with MS?

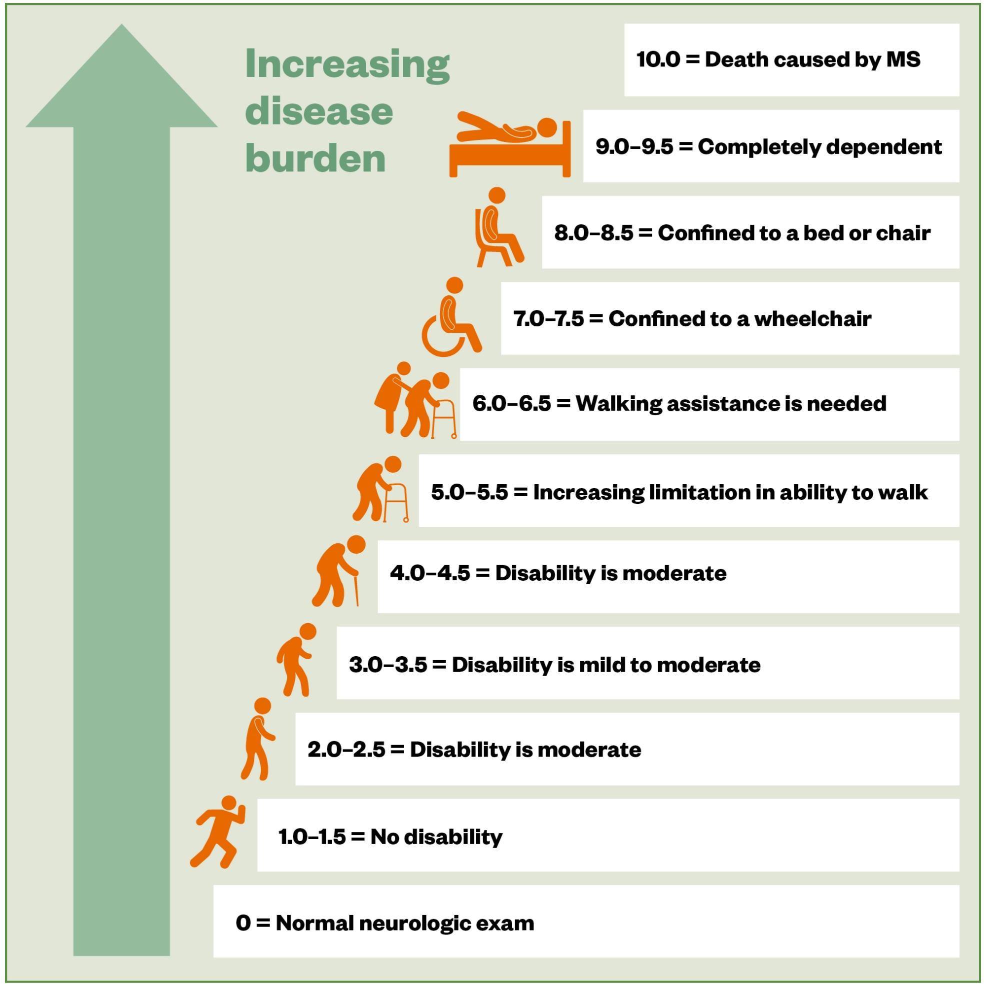
**133,000**
people are living with MS. This equates to 1 in every 500 people.

**8,500**
children under the age of 18 are living with MS.

### Diagnosis of MS?

**3,600**
new people are diagnosed each year. That's 300 diagnosed every month.

**90%**
of people are initially diagnosed with relapsing-remitting MS. 10% have progressive MS.




# Expanded Disability Status Scale (EDSS)

- The **EDSS** is a widely used ordinal scale (0-10 in 0.5 increments) that quantifies **disability in multiple sclerosis**, based on neurological examination and evaluation of **eight functional systems**
    - Pyramidal, cerebellar, sensory, visual, cerebral, bowel
- Scores from **0 to 4.5** indicate full ambulatory capacity
- Scores **5.0 and above** reflect progressive loss of walking ability and increasing disability
- The EDSS is the most commonly tool for **tracking disease progression** and **assessing treatment efficacy** in clinical trials

Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
PNC
Piano nazionale per gli investimenti complementari al PNRR
Ministero dell'Università e della Ricerca
D3 4HEALTH
Digital Driven Diagnostics, prognostics and therapeutics for sustainable Health care

# Hybrid AHE-CNN

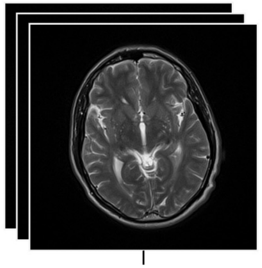
- **Problem**:
  - Design a privacy-preserving deep-learning model that can determine the degree of EDSS combining MRI images and clinical encrypted data
- With Homomorphic Encryption we can share **processable** encrypted data

Client-Side

Hospital

Initial Clinical Data

| | PatientID | Age | SystolicBP | Pain | ChiefComplaint | GeneticRisk | EDSS |
|---|---|---|---|---|---|---|---|
| $t_1$ | MSP-0001 | 42 | 125 | 5 | Numbness in limbs | Yes | High |
| $t_2$ | MSP-0002 | 36 | 118 | 4 | Fatigue and Vision problems | No | Low |
| $t_3$ | MSP-0003 | 51 | 135 | 6 | Muscle weakness | Yes | Medium |
| $t_4$ | MSP-0004 | 47 | 130 | 7 | Fatigue and Balance issues | Unknown | Medium |
| $t_5$ | MSP-0005 | 39 | 122 | 3 | Balance issues | No | Low |
| $t_6$ | MSP-0006 | 45 | 128 | 6 | Dizziness and Numbness in limbs | Yes | High |
| $t_7$ | MSP-0007 | 33 | 115 | 2 | Tingling sensation | Unknown | High |
| $t_8$ | MSP-0008 | 58 | 140 | 7 | Fatigue and Cognitive difficulties | Yes | Medium |
| $t_9$ | MSP-0009 | 49 | 132 | 5 | Muscle spasms. Vision problems | No | Medium |
| $t_{10}$ | MSP-0010 | 41 | 127 | 4 | Gait disturbances | Yes | Low |



Selection of Sensitive Values

Homomorfic Encryption

Preprocessed Data

| | PatientID | Age | SystolicBP | Pain | ChiefComplaint | GeneticRisk | EDSS |
|---|---|---|---|---|---|---|---|
| $t_1$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 125 | 5 | Numbness in limbs | 101010100 101010001 101010110 101010101 110010101 011010101 | 2 |
| $t_2$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 118 | 4 | Fatigue and Vision problems | 101010100 101010001 101010110 101010101 110010101 011010101 | 0 |
| $t_3$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 135 | 6 | Muscle weakness | 101010100 101010001 101010110 101010101 110010101 011010101 | 1 |
| $t_4$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 130 | 7 | Fatigue and Balance issues | 101010100 101010001 101010110 101010101 110010101 011010101 | 1 |
| $t_5$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 122 | 3 | Balance issues | 101010100 101010001 101010110 101010101 110010101 011010101 | 0 |
| $t_6$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 128 | 6 | Dizziness and Numbness in limbs | 101010100 101010001 101010110 101010101 110010101 011010101 | 2 |
| $t_7$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 115 | 2 | Tingling sensation | 101010100 101010001 101010110 101010101 110010101 011010101 | 2 |
| $t_8$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 140 | 7 | Fatigue and Cognitive difficulties | 101010100 101010001 101010110 101010101 110010101 011010101 | 1 |
| $t_9$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 132 | 5 | Muscle spasms. Vision problems | 101010100 101010001 101010110 101010101 110010101 011010101 | 1 |
| $t_{10}$ | 10101 10101 10100 10101 11101 10101 | 101 001 100 111 101 110 | 127 | 4 | Gait disturbances | 101010100 101010001 101010110 101010101 110010101 011010101 | 0 |

MRI Preprocessing

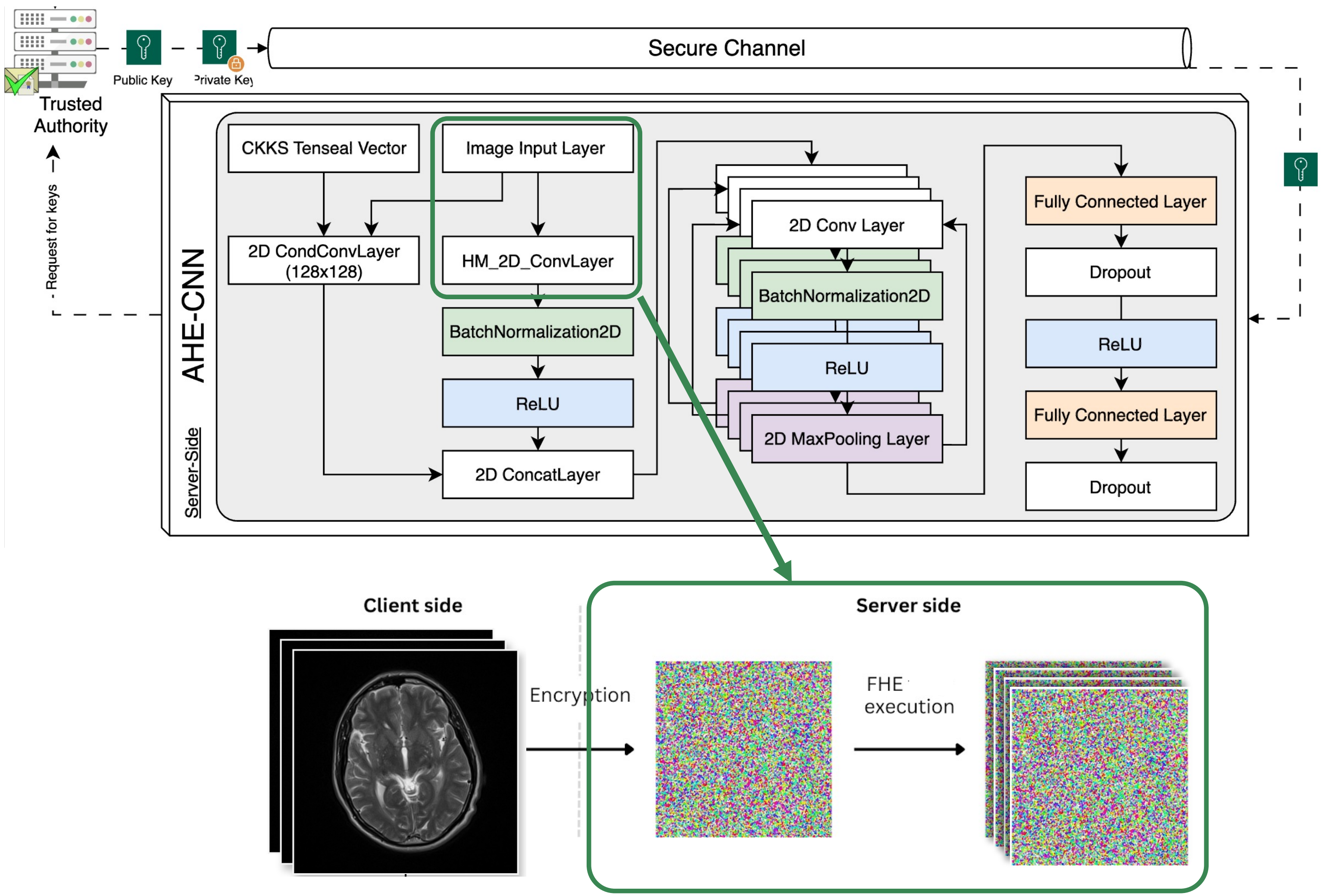
Request for keys

Trusted Authority

Secure Channel

# Hybrid AHE-CNN

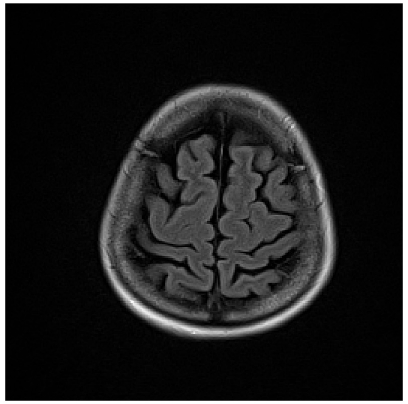
- **Problem**:
  - Design a privacy-preserving deep-learning model that can determine the degree of EDSS combining MRI images and clinical encrypted data
- With Homomorphic Encryption we can share **processable** encrypted data
- **Solution**:
  - A hybrid CNN capable of processing encrypted MRI images and performing encrypted convolution operations
  - Additionally, AHE-CNN **processes** and is able to **exchange** layer **weights** in an **encrypted** manner



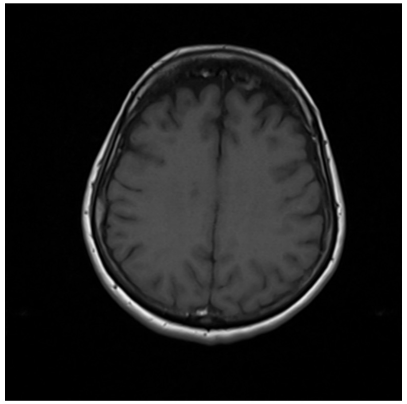

Encrypted Convolution and Processing

# Brain MRI Dataset

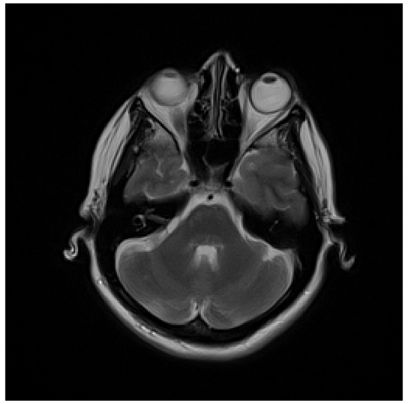
- **60 patients** with Multiple Sclerosis (MS) [1]
- 4,189 MRI images segmented and validated by radiologists and neurologists
- Includes multi-sequence scans:
  - T1-weighted
  - T2-weighted
  - FLAIR (Fluid-Attenuated Inversion Recovery)
- Provides both imaging data and clinical metadata (e.g., age, diagnosis, disability status)
- Enables exploration of MS severity classification and supports both binary (**≤2.0** vs **>2.0** EDSS) and multiclass (**Normal**, **Medium**, **Severe**) tasks



(a) FLAIR



(b) T1



(c) T2

[1] MUSLIM, Ali M., et al. *Brain MRI dataset of multiple sclerosis with consensus manual lesion segmentation and patient meta information*. *Data in Brief*, 2022, 42: 108139.

# Experimental Evaluation and Results

- **Results:**
  - Comparable performance between encrypted and plaintext models.
  - **Binary task**: Hybrid AHE-CNN reached up to 84% accuracy with SMOTE and 90% on the original dataset

| Dataset | Support | Hybrid AHE-CNN | | | | Plaintext CNN | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Accuracy | Precision | Recall | F1 | Accuracy | Precision | Recall | F1 |
| Original | 4189 | 0.90 | 0.32 | 0.33 | 0.31 | 0.99 | 0.33 | 0.33 | 0.33 |
| Undersampling | 823 | 0.69 | 0.73 | 0.59 | 0.65 | 0.68 | 0.70 | 0.68 | 0.67 |
| Oversampling | 3982 | 0.67 | 0.64 | 0.76 | 0.69 | 0.82 | 0.84 | 0.82 | 0.82 |
| SMOTE | 3982 | 0.84 | 0.80 | 0.85 | 0.82 | 0.82 | 0.81 | 0.82 | 0.82 |

# Experimental Evaluation and Results

**Insight:** Homomorphic encryption enables privacy-preserving classification with **only slight performance degradation** compared to plaintext models

- **Results:**
  - Comparable performance between encrypted and plaintext models.
  - **Binary task**: Hybrid AHE-CNN reached up to 84% accuracy with SMOTE.
  - **Multiclass task**: More challenging (accuracy < 50% in most cases), but encrypted model showed better recall and F1 for minority classes
    - **Problems with Multiclass**: Minority classes (“Mild” and “Severe”) had fewer samples compared to “Normal”, limiting the model’s ability to learn representative features

| Dataset | Support | Hybrid AHE-CNN | | | | Plaintext CNN | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Accuracy | Precision | Recall | F1 | Accuracy | Precision | Recall | F1 |
| Original | 4189 | 0.52 | 0.49 | 0.52 | 0.49 | 0.64 | 0.67 | 0.51 | 0.50 |
| Undersampling | 885 | 0.38 | 0.39 | 0.38 | 0.36 | 0.31 | 0.32 | 0.33 | 0.31 |
| Oversampling | 2071 | 0.39 | 0.40 | 0.39 | 0.38 | 0.33 | 0.33 | 0.33 | 0.32 |
| SMOTE | 2071 | 0.43 | 0.44 | 0.43 | 0.42 | 0.49 | 0.39 | 0.49 | 0.33 |

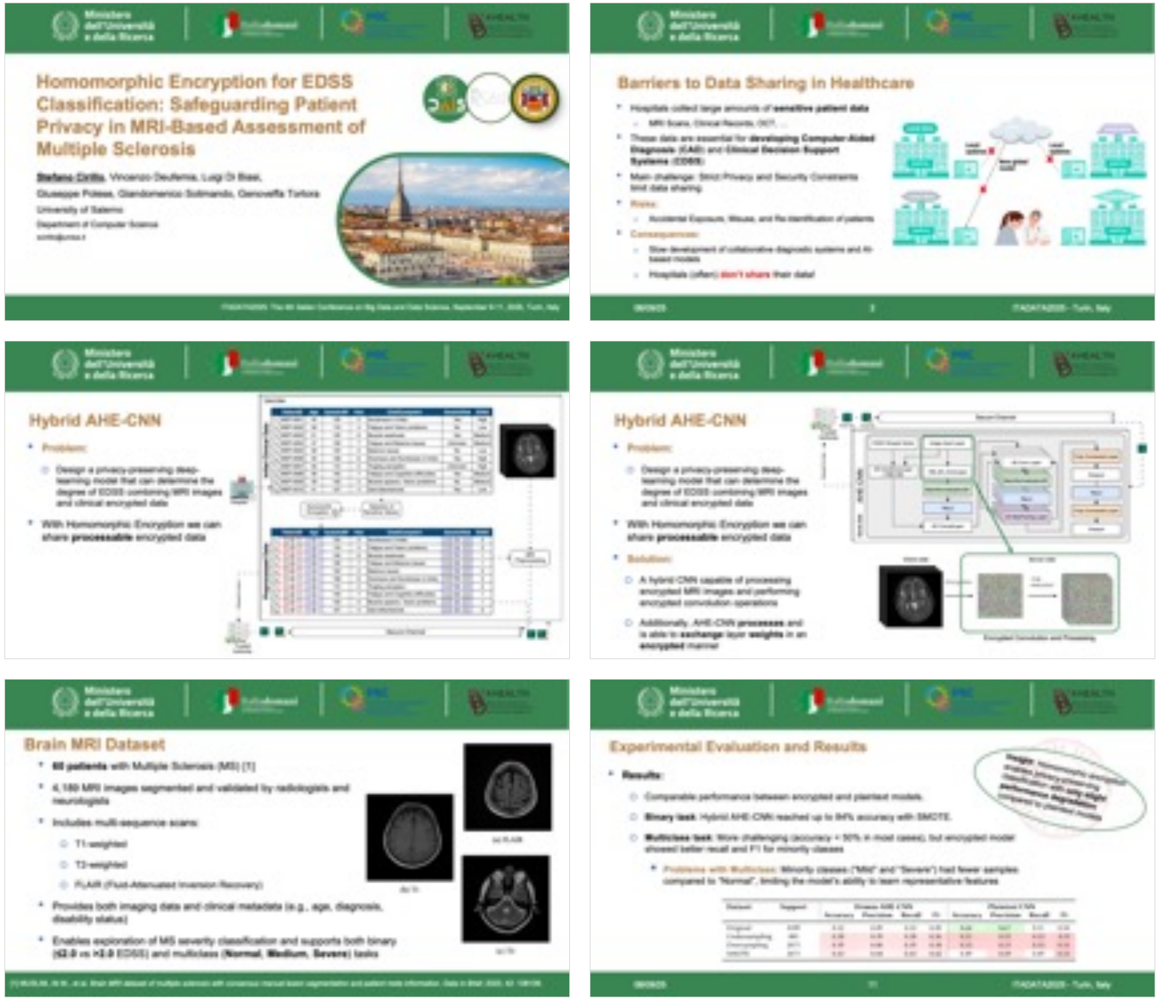
# Conclusion and Future Works

Desing a Federated Environment to enable **secure cooperative training** among clients

Explore **low-precision / quantized networks** to reduce encrypted computation cost

Improve **key management** and integration into clinical workflows for real-world deployment

**Optimize** HE pipeline with ciphertext packing, faster bootstrapping, key-switching, …



# THANK YOU

Stefano Cirillo

University of Salerno

Department of Computer Science

scirillo@unisa.it