|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | INTERNATIONAL TELECOMMUNICATION UNION  **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2022-2024 | | FG-AI4H-S-039 | |
| **ITU-T Focus Group on AI for Health** | |
| **Original: English** | |
| **WG(s):** | | Plenary | Geneva, 3-5 July 2023 | |
| **DOCUMENT** | | | | |
| **Source:** | | Inpher | | |
| **Title:** | | Neuroimaging Based Diagnosis of Alzheimer’s Disease Using Privacy-Preserving Machine Learning | | |
| **Contact:** | | Manuel Capel, MSc Inpher SàRL Switzerland | | Email: [manuel@inpher.io](mailto:manuel@inpher.io) |
| **Contact:** | | Dr. Dimitar Jetchev Inpher SàRL Switzerland | | Email: [dimitar@inpher.io](mailto:dimitar@inpher.io) |

|  |  |
| --- | --- |
| **Abstract:** | Despite intensive efforts to better understand the preclinical manifestation of dementia and Alzheimer’s Disease (AD), current clinical research is still short of providing the relevant means for screening, diagnosis, monitoring and outcome prediction. Existing theoretical models demonstrate that early intervention with an impact on AD’s progress will reduce healthcare treatment costs [estimated at $1 trillion](https://www.ajmc.com/view/economic-burden-of-alzheimer-disease-and-managed-care-considerations).  A steadily accumulating body of empirical evidence showed the potential of machine learning algorithms for brain imaging-based diagnosis of AD. Using non-invasive Magnetic Resonance Imaging (MRI) and state-of-the-art feature extraction methods, Machine Learning (ML) models have been trained to achieve accurate diagnosis of AD in different stages of the disease process. To achieve clinical relevance, these ML models have to be trained and tested beyond a single data center. The privacy of patients’ data poses a real challenge for aggregating training and testing datasets across hospitals, research institutions and pharma companies.  This two-part blog series presents a viable solution designed by clinical researchers at CHUV and Inpher aiming to build privacy-preserving neuroimaging-based ML models of AD using Inpher’s XOR Platform. We specifically show how data providers can securely collaborate to build linear and logistic regression models that clinical and non-clinical researchers can use. With the rising hopes for efficient disease-modifying drugs, our clinically relevant concept of accurate ML-based diagnosis will help clinicians to efficiently stratify patients for clinical trials and finally deliver better care. |
| **References** | Neuroimaging Based Diagnosis of Alzheimer’s Disease Using Privacy-Preserving Machine Learning Part I <https://inpher.io/blog/diagnosis-of-alzheimers-disease-using-privacy-preserving-machine-learning-part-1/> and Part II: <https://inpher.io/blog/neuroimaging-based-diagnosis-of-alzheimers-disease-using-privacy-preserving-machine-learning-part-2/> by Inpher  The Privacy Risk Right Under Our Nose in Federated Learning <https://inpher.io/blog/the-privacy-risk-right-under-our-nose-in-federated-learning-part-1/>  Manticore: Efficient Framework for Scalable Secure Multiparty Computation Protocols <https://eprint.iacr.org/2021/200.pdf> by Inpher.  UN Handbook on Privacy-Preserving Computation Techniques provides an overview of PETs <https://arxiv.org/ftp/arxiv/papers/2301/2301.06167.pdf> as well as the UN Guide on Privacy Enhancing Technologies for Official Statistics <https://unstats.un.org/bigdata/task-teams/privacy/guide> citing Inpher.  EDBP Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> citing Secure Multiparty Computation. |
|  |  |

*Authors: Prof.*[*Bogdan Draganski*](https://www.linkedin.com/in/bogdan-draganski-9a542689/?originalSubdomain=ch)*(Director, LREN), Dr.*[*Ferath Kherif*](https://www.linkedin.com/in/ferath-kherif-355b8618/recent-activity/posts/)*(Vice Director, LREN),*[*Claudio Calvaruso*](https://www.linkedin.com/in/claudio-calvaruso/)*(Technical Account Manager, Inpher) and Dr.*[*Dimitar Jetchev*](https://www.linkedin.com/in/jetchev/?originalSubdomain=ch)*(CTO, Inpher)*

*Editors Note: This is the first in a series of articles that LREN – CHUV and Inpher are jointly publishing to show how privacy-preserving machine learning allows for neuroimaging-based diagnosis of Alzheimer’s disease that is readily applicable in a federated network. Read Part 2*[*here*](https://inpher.io/journal-blog/neuroimaging-based-diagnosis-of-alzheimers-disease-using-privacy-preserving-machine-learning-part-2/)

1. **Introduction**

The devastating impact of the COVID-19 pandemic on *public* health, social and economic life comes as a reminder to also turn our attention and apply the lessons learned to a “silent” epidemic – Alzheimer’s disease (AD) and other dementias. The current estimates of 50 million individuals with dementia worldwide [are predicted to triple by the year 2050](https://www.sciencedaily.com/releases/2021/07/210727171713.htm). Compared to cardio-vascular, cerebro-vascular and infectious diseases, the dynamic of AD – the most frequent cause of dementia, shows a different pattern. It has a progressive time course with insidious onset and a preclinical phase of approximately 20 years before the onset of clinical signs. ADs symptoms cover a whole range of memory, language, visual and behavioural dysfunction that profoundly impact individuals’ autonomy at the stage of major neurocognitive disorder. In addition, the progressive nature of neuronal cell loss, the ageing-associated accumulation of risk factors and comorbidities represents a continuous challenge for diagnosis, prognosis and symptomatic treatment. Therefore, specialists seeing patients with dementia continuously expand their diagnostic armament that can include besides the clinical and neuropsychological evaluation, Magnetic Resonance Imaging (MRI) or Positron Emission Tomography (PET) sensitive to the brain glucose metabolism or the proteins beta-amyloid and tau. The diagnostic work-up can be completed with quantification of the beta-amyloid and tau proteins in the cerebrospinal fluid.

There is a steadily accumulating body of empirical evidence showing the potential of digital technologies and machine learning (ML) algorithms for obtaining a robust and reliable diagnosis of dementia. However, data providers – hospitals, radiology laboratories, research institutes, and pharmaceutical companies are hesitant to share individuals’ data due to data privacy and security concerns. Considering the sensitivity of patients’ data, it is vital to design systems that protect privacy while advancing the research.  Similarly, digital technologies have to be integrated into existing public health care systems to conform with interoperability of data sources, harmonization of minimal data sets, standardization of data formats within a flexible, though ‘proportionate, ethical, and privacy-preserving data governance system. At last, the efficacy and clinical validity of a given digital technology will ensure the public’s trust and engagement.

1. **Building ML Models While Respecting Patient Privacy**

Building on the neuroimaging research expertise of Dr. Ferath Kherif and Prof. Bogdan Draganski in the field and on a recent report employing patients with COVID-19 (Dayan et al., 2021), together with Inpher’s expertise in Privacy Enhancing Technologies, here it is described as a privacy-preserving federated learning architecture for diagnosis of Alzheimer’s disease where different hospitals, private clinics, and research labs participate in sharing sensitive MRI images as well as other clinical data.  For more on how Federated Learning works, see our previous blog post [The Privacy Risk Right Under Our Nose in Federated Learning (Part 1)](https://inpher.io/journal-blog/the-privacy-risk-right-under-our-nose-in-federated-learning-part-1/)

A picture containing circle, clock

Description automatically generated

*Figure 1: Collaborative Model Development Using Privacy-Preserving Technique*

In short, the diagnosis and prognosis of Alzheimer’s disease (AD) could be seen from two different perspectives:

* Researchers can use the framework to identify MRI-derived brain anatomy patterns associated with the disease that go beyond demographic or other factors with a strong impact on the brain. A linear regression model is used.
* Clinicians can use the framework to estimate an AD risk score for a given individual. The score can be used to support clinical decision-making. A logistic regression model is used.

The framework relies on training a model of Alzheimer disease’s related patterns using demographics, brain imaging, clinical phenotyping data and available biomarkers from various sites without moving or centralizing the data and keeping it private and secure throughout the entire process.

Brain MRI scans are chosen as the main brain imaging input for the model for three reasons:

* High diagnostic value in neurodegenerative and cerebro-vascular diseases
* Non-invasiveness
* Lower cost of MRI compared with PET
* Established framework for feature extraction and statistical analysis in 3-dimensional brain space

1. **Data Preprocessing**

Before MRI data are used by ML algorithms to train linear and logistic regression models, there is a dimensionality reduction step. This is performed using the Statistical Parametric Mapping ([SPM](http://www.fil.ion.ucl.ac.uk/spm)) framework that automatically classifies brain MRI data into 3-D probabilistic maps corresponding to gray matter, white matter, and cerebrospinal fluid compartments. In the same step, all individuals’ brains are spatially transformed to a standardized cartesian space (stereotaxic space). Finally, the regional expansions or contractions are encoded and mapped at the level of each image unit (voxel – i.e. 3D pixel), using the Jacobian determinant. In the example below (Figure 2), the top row shows an original brain MRI that is classified in grey matter (2nd row), white matter (3rd row) and cerebro-spinal fluid (bottom row) probabilistic maps.

A collage of images of the brain

Description automatically generated with low confidence

*Figure 2: Brain tissue classification in a Bayesian probabilistic framework*

Following this step, the brain tissue-specific 3-D matrices are aligned with submillimeter precision in the same standard space. The last step involves spatial smoothing with a Gaussian 3-D kernel that renders the data normally distributed and minimizes spatial registration errors. After this, the data are ready for statistical parametric mapping – i.e. statistical modelling.

To allow interpretation of statistical results as volume differences or voxel changes, one uses the Jacobian determinant at the voxel level. The latter describes the expansions and contractions of a subject-specific probabilistic mapping needed to match a 3-D template in the standard space (Figure 3). Unexpected to the authors of a recent ML study, the use of Jacobian-scaled (modulated) grey matter maps as features for pattern recognition showed higher prediction accuracy for autism, schizophrenia, body mass index, age and gender (doi: 10.1016/j.neuroimage.2018.05.065).

A close-up of a brain

Description automatically generated with medium confidence

*Figure 3: A Jacobian determinant of individual AD patient – dark shades signify contraction, light – expansion. Exemplary case with volume loss in the hippocampus (black) and dilation of the ventricles (white).*

1. **Alzheimer’s Disease Models with XOR Secret Computing Platform**

Researchers understand that data available at the local healthcare facility is not enough to obtain a meaningful and unbiased prediction model. However, data providers such as hospitals, research labs, and pharmaceutical companies are hesitant to share individuals’ data due to privacy and security concerns. Inpher’s [XOR™ Platform](https://inpher.io/xor-secret-computing/) is built specifically to address this problem – allowing organizations to develop models with sensitive data distributed across teams, geographies and even other organizations. Healthcare researchers can extract rich insights with the XOR Platform by securely using datasets from multiple data sources for model evaluation and training.

Powered by Secure Multi-Party Computation, an advanced cryptographic technique, the XOR Platform delivers a comprehensive solution for privacy-preserving machine learning and federated learning (through secure aggregation). Python library (XOR-py), Jupyter notebook integration, and REST APIs empower data scientists to build models without requiring cryptographic expertise. The XOR Platform is available today [AWS](https://aws.amazon.com/marketplace/seller-profile?id=10d13418-25a8-400e-92aa-785cc347b250) and [GCP](https://console.cloud.google.com/marketplace/product/inpher-public/xor?pli=1) marketplace. Additionally, data scientists can try out our [free trial](https://www.inpher.io/trial)environment with predefined datasets across representative example use cases.

[SMPC](https://inpher.io/technology/what-is-secure-multiparty-computation/) is one of the most popular Privacy Enhancing Technologies that enables several parties, each holding a private input dataset, to jointly evaluate a publicly known function without revealing anything about the inputs except what is implied by the output of the function.  See the diagram below for the overall architecture for PPML with SMPC among hospitals, research institutions and a private radiology lab:

A picture containing text, diagram, screenshot, line

Description automatically generated

*Figure 4: Workflow Illustration for PPML with SMPC*

To make a concrete example, suppose that the hospital uses a private value*v* = 5 (in a real-world MRI scenario, this can be a vector or a tensor of voxel values). The hospital secret shares this value among itself, a private radiology laboratory, and a research institute by generating two random integers (secret shares)  Sradio\_lab=125621 and Sr\_institute = 56872 and by sending out these shares to the radiology lab and the research institute, respectively. It then keeps the secret share

 Shospital= *v* – Sradio\_lab – Sr\_institute = -182488.

This ensures that collaboratively, the three parties can recover the secret value, yet, the coalition of the research institute and the radiology lab recovers nothing about the hospital’s secret value. Further examples and explanations could be found in the [Inpher’s Secret Computing Explainer Series](https://inpher.io/learn/resources/).

In [Federated Learning](https://en.wikipedia.org/wiki/Federated_learning), multiple clients locally train models with their local private data (in plaintext) and the resulting local models are centrally aggregated to build a global model. Even if the aggregating server does not see the original local private data, if it is exposed to the local models (in plaintext), it is possible to reverse engineer the process and obtain sensitive information about the local data (the so-called [model-inversion attacks](https://inpher.io/journal-blog/the-privacy-risk-right-under-our-nose-in-federated-learning-part-1/)). Thus, to design a secure system, it is important to protect the local models from the aggregating server leading to the concept of PrivacyPreserving Federated Learning (PPFL). One way to protect the local models is via SMPC. See the diagram below for the overall architecture of a PPFL system with secure aggregation via SMPC.

A picture containing text, diagram, font, design

Description automatically generated

*Figure 5: Workflow Illustration for PPFL with SMPC secure aggregation*

The choice between machine learning with SMPC and PPFL largely depends on the use case as the following table illustrates:

A picture containing text, screenshot, font, number

Description automatically generated

1. **Conclusion**

While there is no established treatment for Alzheimer’s disease yet, with the help of privacy-enhanced techniques, hospitals, and healthcare providers can develop highly accurate and precise models that will allow them to screen, diagnose, monitor and predict outcomes at a larger scale and with higher accuracy. Researchers can expand our knowledge about the pathophysiology of dementias, build models of disease progression and adjust these for interindividual differences. At the same time, clinicians can estimate an accurate risk score and propensity for neuromodulatory treatment for a given patient that would, in turn, help support better clinical decision-making.

Here, we share our current experience with state-of-the-art imaging neuroscience tools that render complex MRI images suitable for training. Finally, we highlight two different techniques, namely, Privacy-Preserving Machine Learning (PPML) and Privacy-Preserving Federated Learning (PPFL), that can be used to collaborate with other hospitals, pharma companies, and research labs to build Alzheimer’s disease models.

The usage of privacy-enhanced technologies is still in the early stages, but its potential, especially for healthcare providers, is clear. [Part 2](https://inpher.io/journal-blog/neuroimaging-based-diagnosis-of-alzheimers-disease-using-privacy-preserving-machine-learning-part-2/) in this blog series will delve into the specific workflow to building Linear Regression and Logistic Regression models using Multi-Party Computation and the XOR Platform.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_