جامعة عبد المالك السعدي
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵏ ⵄⴰⴱⴷⵍⵎⴰⵍⵉⴽ ⵙⵙⴰⵄⴷⵉ
Université Abdelmalek Essaadi

Pole for Doctoral Studies
Center for Doctoral Studies Sciences and Techniques and Medical Sciences

ANNOUNCEMENT OF DOCTORAL THESIS DEFENSE

Ms. AASOUM Nouhaila

Will present their research work with the aim of earning a Doctorate

Doctoral program: Mathematical Sciences, Physics and New Technologies (SMPNT)
Discipline: Computer Science
Specialty: Computer Science and Artificial Intelligence

On 26/06/2026 at 16H00 at the Thesis Defense Hall, Faculty of Sciences of Tetouan, UAE
Under the Theme

Privacy-Preserving Machine Learning for Imbalanced Healthcare Data: Analysis, Impact, and Frameworks

Front of the jury composed of :

First Name & Last Name	Establishment	Designation
Pr. ABDOUN Otman	FS of Tetouan, UAE	President
Pr. EL GAROUANI Said	FS of Fez, USMBA	Reviewer
Pr. BENAMEUR Lamia	FS of Tetouan, UAE	Reviewer
Pr. BEN-HDECH Adil	FS of Tetouan, UAE	Reviewer
Pr. LAZAAR Saiida	ENSA of Tangier, UAE	Examiner
Pr. EL MHOUTI Abderrahim	FS of Tetouan, UAE	Examiner
Pr. JELLOULI Ismail	EST of Kenitra, UIT	Co-Supervisor
Pr. AMJAD Souad	FS of Tetouan, UAE	Supervisor

Host Research Structure: Intelligent Systems Design Laboratory

Abstract

The rapid digitalization of healthcare has led to a growing dependency on smart systems for clinical decision support. However, implementing machine-learning models brings significant challenges in maintaining patient privacy, clinical usefulness, and fairness in algorithms. This issue is especially pronounced in real-world medical datasets, which often have a severe imbalance where important minority conditions are underrepresented. Common privacy-preserving methods, like Differential Privacy (DP), can actually worsen this imbalance. They often impose heavy performance costs on already marginalized patient groups, creating a difficult balance between privacy, utility, and fairness.

This thesis addresses this challenge through three interconnected contributions. First, a Systematic Literature Review (SLR) synthesizes existing studies on DP and imbalanced healthcare data, organizing mitigation strategies into a three-tiered taxonomy and identifying critical methodological gaps. Second, a comprehensive empirical study compares major DP paradigms across different privacy budgets on imbalanced population health datasets, revealing key determinants of DP robustness and highlighting equity disparities linked to demographic factors. Third, a privacy-preserving federated learning framework for disease detection integrates formal DP guarantees with an innovative quality-weighted aggregation strategy to mitigate non-Independent and Identical Distribution (IID) data across institutions. The framework demonstrates that rigorous privacy protection and strong clinical utility can be achieved simultaneously.

Overall, this thesis shows that the three-way challenge of privacy, utility, and fairness in imbalanced healthcare Artificial Intelligence (AI) is tractable through co-design. It provides a systematic analytical framework, cross-paradigm empirical baselines, and a favorable federated implementation, offering a complete research-to-deployment pathway for responsible privacy-preserving healthcare AI.

Keywords: Privacy-Preserving, Healthcare AI, Differential Privacy, Imbalanced Datasets, Federated Learning.