ENSA
ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES
KHOURIBGA

جامعة السلطان مولاي سليمان
Université Sultan Moulay Slimane

ENSA KHOURIBGA ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES

Avis de soutenance de thèse de Doctorat

Le Directeur de l'École Nationale des Sciences Appliquées de Khouribga annonce que :

Monsieur Anass Misbah

Soutiendra publiquement sa thèse de Doctorat

Le Mardi 23 Juin 2026 à 12h30 à l'amphithéâtre de conférence de l'ENSA Khouribga

Intitulé de la thèse:

SECURING THE INTERNET OF MEDICAL THINGS: FEDERATED LEARNING, EDGE-EFFICIENT DIMENSIONALITY REDUCTION, AND EXPLAINABILITY

Devant le jury composé de :

Nom et Prénom	Grade	Établissement	Fonction
Pr. ABOUTABIT Noureddine	PES	Université Sultan Moulay Slimane, ENSA Khouribga	Président/Rapporteur
Pr. SOUSSI Nassima	MCH	Université Sultan Moulay Slimane, ENSA Khouribga	Rapporteure
Pr. LACHGAR Mohamed	MCH	Université Cadi Ayyad, ENS Marrakech	Rapporteur
Pr. GHAZDALI Abdelghani	MCH	Université Sultan Moulay Slimane, ENSA Khouribga	Examinateur
Pr. LAMGHARI Nidal	MCH	Université Sultan Moulay Slimane, ENSA Khouribga	Examinatrice
Pr. HAFIDI Imad	PES	Université Sultan Moulay Slimane, ENSA Khouribga	Directeur de thèse

Résumé de la thèse

L'Internet des objets médicaux (IoMT) interconnecte des dispositifs de détection, des systèmes cliniques et des réseaux hospitaliers, permettant une surveillance continue et des soins fondés sur les données. Cependant, cette connectivité élargit également la surface d'attaque cybernétique, tout en renforçant les contraintes liées à la confidentialité, à la latence et à la gouvernance, ce qui rend le partage centralisé des données de plus en plus difficile dans les environnements médicaux.

Cette thèse développe un cadre de sécurité intégré, respectueux de la confidentialité et explicable pour l'IoMT. Elle synthétise cinq travaux de recherche évalués par les pairs autour de trois axes de contribution étroitement liés : la détection d'intrusions fédérée, l'apprentissage de représentations et l'agrégation efficaces en périphérie, ainsi que l'explicabilité à double niveau pour un déploiement digne de confiance.

La première contribution étudie la détection d'intrusions fédérée à travers dix clients périphériques simulés, en utilisant des apprenants locaux hétérogènes, notamment Random Forest, AdaBoost, SVM et des modèles profonds légers, dans des partitions non IID. L'agrégation est réalisée par vote majoritaire et empilement, tandis que la surcharge de communication est réduite grâce à des politiques de synchronisation inspirées de l'agrégation dynamique. La confidentialité est renforcée par l'agrégation sécurisée et l'injection optionnelle de bruit différentiel.

La deuxième contribution, sous la forme d'un pipeline de type EdgeShield, combine la sélection de caractéristiques avec l'Analyse en Composantes Principales (ACP) afin de compresser des caractéristiques de trafic à haute dimension en une représentation compacte, adaptée aux dispositifs périphériques aux ressources limitées. Elle introduit également une fusion de forêts au niveau des estimateurs, qui assemble un modèle Random Forest global à partir des arbres locaux des clients, sans aucun réentraînement. Cette approche permet d'obtenir une réduction de dimensionnalité de 96 %, tout en conservant une précision de classification supérieure à 99,2 %.

La troisième contribution intègre un cadre d'explicabilité à double niveau dans le système fédéré de détection d'intrusions. SHAP, ou SHapley Additive exPlanations, est utilisé au niveau de la couche d'agrégation cloud afin de fournir des attributions globales des caractéristiques à l'échelle du modèle, avec un accord de classement de Kendall inter-clients de τ = 0,953, avec un intervalle de confiance à 95 % de [0,950 ; 0,956]. LIME, ou Local Interpretable Model-agnostic Explanations, est exécuté au niveau périphérique afin de générer des justifications décisionnelles propres à chaque instance en seulement 40,70 ± 1,93 ms, répondant ainsi aux exigences de temps réel des environnements cliniques.

Les deux couches d'explication sont complémentaires : SHAP soutient la gouvernance au niveau du modèle, l'audit et l'analyse de cohérence entre clients, tandis que LIME soutient le tri opérationnel et l'investigation des alertes par les opérateurs.

Ainsi, cette thèse étend la détection d'intrusions IoMT préservant la confidentialité vers un modèle opérationnel plus fiable, auditable et conforme aux attentes réglementaires émergentes, notamment dans le cadre de l'AI Act européen, du RGPD et de la HIPAA.

En utilisant le benchmark multi-protocole CICIoMT2024, composé de 667 187 échantillons, de 18 catégories d'attaques et de 10 types de dispositifs IoMT, le modèle Random Forest fédéré atteint une précision de 99,05 %. Ce résultat est inférieur de seulement 0,13 point de pourcentage au modèle Random Forest centralisé correspondant, et supérieur de 21,31 points de pourcentage au modèle MLP FedAvg utilisé comme référence comparative. La couche XAI post-hoc laisse le classificateur sous-jacent inchangé.

Le cadre proposé est ainsi reproductible, efficace en matière de communication, sensible aux exigences réglementaires et adapté à des scénarios de déploiement où la confidentialité, la bande passante et les capacités de calcul sont fortement contraintes.

Mots-clés : Internet des objets médicaux (IoMT) ; apprentissage fédéré ; système de détection d'intrusions ; intelligence artificielle explicable (XAI) ; SHAP ; LIME ; sélection de caractéristiques ; analyse en composantes principales ; edge computing ; préservation de la confidentialité ; données non IID ; agrégation au niveau des estimateurs ; AI Act européen ; conformité réglementaire