College of Engineering and Computer Science
Office of the Dean
777 Glades Road, EE96, Room 308
Boca Raton, FL 33431
561.297.3400

FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Theyab Alsolami

for the degree of Doctor of Philosophy (Ph.D.)

Privacy-Preserving Intrusion Detection for the Internet of Medical Things Using Ensemble Machine Learning and Federated Learning

April 02, 2026, at 2:00 p.m. EE96/ Room # 405
777 Glades Road
Boca Raton, FL

DEPARTMENT: Department of Electrical Engineering & Computer Science

ADVISOR:
Mohammad Ilyas, Ph.D.
PH.D. SUPERVISORY COMMITTEE:
Imadeldin Mahgoub, Ph.D.
Shihong Huang, Ph.D.
Dingding Wang, Ph.D.

Abstract of dissertation

The rapid proliferation of the Internet of Medical Things (IoMT) has transformed healthcare by enabling continuous monitoring, intelligent diagnostics, and data-driven clinical decision-making. However, this increased connectivity has significantly expanded the attack surface of healthcare systems, exposing sensitive patient data and critical medical devices to cyber threats such as intrusion and data exfiltration attacks. Ensuring both strong security and strict privacy preservation in IoMT environments remains a fundamental and unresolved challenge.

This dissertation investigates the design and evaluation of robust and privacy-preserving intrusion detection systems (IDS) for IoMT networks using advanced machine learning techniques. The research first examines the effectiveness of ensemble learning–based IDS models in centralized settings, evaluating Stacking, Bagging, and Boosting approaches with Random Forest and Support Vector Machine base learners on the WUSTL-EHMS-2020 dataset. Experimental results demonstrate that ensemble learning significantly enhances detection performance, with the Stacking model achieving an accuracy of 98.88%, followed by Bagging at 97.83%, while Boosting exhibits comparatively lower performance.

Building on these findings, the dissertation extends intrusion detection to decentralized and privacy-sensitive IoMT environments through a federated learning (FL) framework integrated with Differential Privacy (DP) and secure aggregation mechanisms. Multiple experimental configurations are systematically ana-

College of Engineering and Computer Science
Office of the Dean
777 Glades Road, EE96, Room 308
Boca Raton, FL 33431
561.297.3400

lyzed, including raw imbalanced data, centralized SMOTE, and clientside (per-client) SMOTE under varying privacy budgets (ϵ = 3.0, 10.0, and non-private baselines). Results show that privacy-preserving federated models frequently match or exceed non-private baselines. In particular, raw imbalanced and per-client SMOTE configurations achieve high detection accuracy (approximately 94.6%) even under strict privacy constraints (ϵ = 3.0), demonstrating effective learning with minimal utility loss. Furthermore, client-side data balancing consistently outperforms centralized balancing, providing improved training stability while maintaining full data decentralization and patient confidentiality.

Overall, this dissertation presents a comprehensive, scalable, and privacy-compliant intrusion detection framework for IoMT systems. By integrating ensemble learning, federated learning, class imbalance mitigation, and differential privacy, the proposed approach successfully balances detection accuracy, privacy preservation, and computational efficiency. The findings provide both theoretical insights and practical guidelines for deploying secure and regulation-compliant IDS solutions in real-world healthcare IoMT environments.

Biographical Sketch:

Theyab Alsolami received a Bachelor of Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia, and a Master of Computer Science in Information Technology from Sacred Heart University, Fairfield, Connecticut, United States. He is currently pursuing a Ph.D. in Computer Science at Florida Atlantic University in Boca Raton, Florida.
Alsolami's academic journey reflects a strong commitment to advancing knowledge in computer science and Cybersecurity in IoMT. Through rigorous study and research, he continues to build expertise in the field and pursue scholarly and professional growth.

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: Summer 2021 – Present (approximately 5 years)

Qualifying Examination Passed: Fall 2021

Published Papers:

- **Alsolami, T., Balhareth, G., & Ilyas, M. (2023). *Survey for Security in IoT in E-Healthcare*. Proceedings of the 14th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC), International Institute of Informatics and Systemics, Virtual Conference, pp. 94–97. https://doi.org/10.54808/IMCIC2023.01.94 (Published).**

- **Balhareth, G., Alsolami, T., & Ilyas, M. (2023). *IoT Big Data Privacy Using Blockchain Technology: A Survey*. Proceedings of the 14th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC), International Institute of Informatics and Systemics, Virtual Conference, pp. 58–63. https://doi.org/10.54808/IMCIC2023.01.58 (Published).**

- **Alsolami, T., Alsharif, B., & Ilyas, M. (2024). *Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things*. *Sensors*, 24(18), 5937. https://doi.org/10.3390/s24185937 (Published).**

- **Alsolami, T., & Ilyas, M. (2026). *FedSMOTE-DP: Privacy-Aware Federated Ensemble Learning for Intrusion Detection in IoMT Networks*. *Sensors*, 26(5), 1592. https://doi.org/10.3390/s26051592 (Published).**