Announces the Ph.D. Dissertation Defense of

# Yazeed Alotaibi

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

## "Enhancing IoT Devices security: Ensemble Learning with classical approaches for Intrusion Detection system"

October 31, 2023, Time 9:00 PM - 10:30 AM.
Building, Room EE 405
777 Glades Road
Boca Raton, FL

DEPARTMENT:

Department of Electrical Engineering and Computer Science

ADVISOR:

Mohammad Ilyas, Ph.D.

PH.D. SUPERVISORY COMMITTEE:

Mohammad Ilyas, Ph.D., Chair
Imadeldin Mahgoub, Ph.D.
Waseem Asghar, Ph.D.
Dingding Wang, Ph.D.

ABSTRACT OF DISSERTATION

Enhancing IoT Devices security: Ensemble Learning with classical approaches for Intrusion Detection system.

The Internet of Things (IoT) refers to a network of interconnected nodes constantly engaged in communication, data exchange, and the utilization of various network protocols. Previous research has demonstrated that IoT devices are highly susceptible to cyber-attacks, posing a significant threat to data security. This vulnerability is primarily attributed to their susceptibility to exploitation and their resource constraints. To counter these threats, Intrusion Detection Systems (IDS) are employed. This study aims to contribute to the field by enhancing IDS detection efficiency through the integration of Ensemble Learning (EL) methods with traditional Machine Learning (ML) and deep learning (DL) models. To bolster IDS performance, we initially utilize a binary ML classification approach to classify IoT network traffic as either normal or abnormal, employing EL methods such as Stacking and Voting. Once this binary ML model exhibits high detection rates, we extend our approach by incorporating a ML multi-class framework to classify attack types. This further enhances IDS performance by implementing the same Ensemble Learning methods. Additionally, for further enhancement and evaluation of the intrusion detection system, we employ DL methods, leveraging deep learning techniques, ensemble feature selections, and ensemble methods. Our DL approach is designed to classify IoT network traffic. This comprehensive approach encompasses various supervised ML, and DL algorithms with ensemble methods. The proposed models are trained on TON-IoT network traffic datasets. The ensemble approaches are evaluated using a comprehensive matrix and compared for their effectiveness in addressing this classification tasks. The ensemble classifiers achieved higher accuracy rates compared to individual models, a result attributed to the diversity of learning mechanisms and strengths harnessed through ensemble learning. By combining these strategies, we successfully improved prediction accuracy while minimizing classification errors. The outcomes of these methodologies underscore their potential to significantly enhance the effectiveness of the Intrusion Detection System.

BIOGRAPHICAL SKETCH
Born in Tabuk, Tabuk, Saudi Arabia
B.S., Imam Mohammad Ibn Saud University (IMSIU), 2012.
M.S., Rochester Institute of Technology, Rochester, New York, 2018.
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2023.

**Time in Preparation:** 2021 - 2023

**Qualifying Examination Passed: Semester** Spring 2021

**Published and Submitted Papers:**

Alotaibi, Y., & Ilyas, M. (2022). Security risks in internet of things (IoT): a brief survey. In Proceedings of the 26th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2022), pp. 1-5.

Alrefaei, A., Alotaibi, Y., & Ilyas, M. (2023). Detection Techniques on the Internet of Things (IoT): A Survey of Current Challenges and Open Issues. *Proceedings of the 14th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2023),* pp. 51-57.

Alotaibi, Y., & Ilyas, M. (2023). Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security. Sensors, 23(12), 5568., pp. 1-20.

Alotaibi, Y., & Ilyas, M. (2023). Improving IoT Intrusion Detection with Deep and Ensemble Learning Feature Selection. Sensors (Submitted).

Alotaibi, Y., & Ilyas, M. (2023). Enhancing IoT Attacks Detection Through Ensemble-Based Multiclass Attacks Classification. IEEE 20Th HONET (Submitted).