COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Ahmed Alrefaei

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

"MULTI-CLASS CLASSIFICATION TECHNIQUE TO DETECT IOT ATTACKS IN REAL-TIME"

September 12, 2024, 10:30 a.m. to 12:00 p.m.
Engineering East building, Room #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
Dissertation Title
MULTI-CLASS CLASSIFICATION TECHNIQUE TO DETECT IOT
ATTACKS IN REAL-TIME

Internet of Things (IoT) has undergone remarkable expansion in recent years, leading to a proliferation of devices capable of connecting to the internet, collecting data, and sharing information. However, this rapid growth has also introduced a myriad of security challenges, resulting in an uptick in cyber-attacks targeting IoT infrastructures. To mitigate these threats and ensure the integrity of data, researchers have been actively engaged in the development of robust Intrusion Detection Systems (IDS) utilizing various machine learning (ML) techniques. This dissertation presents a comprehensive overview of three distinct approaches toward IoT intrusion detection, each leveraging ML methodologies to enhance security measures. The first approach focuses on a multi-class classification algorithm, integrating models such as random forest, logistic regression (LR), decision tree (DT), and Xgboost. Through meticulous evaluation utilizing evaluation metrics including F1 score, recall, and precision under the Receiver Operating Characteristics (ROC) curve, this approach demonstrates a remarkable 99 % accuracy in detecting IoT attacks. In the second approach, a deep ensemble model comprising Multilayer Perceptron (MLP), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) architectures is proposed for intrusion detection in IoT environments. Evaluation on the UNSW 2018 IoT Botnet dataset showcases the proficiency of this approach, achieving an accuracy of 98.4 % in identifying malicious activities. Lastly, the dissertation explores a real-time Intrusion Detection System (IDS) framework deployed within the Pyspark architecture, aimed at efficiently detecting IoT attacks while minimizing prediction time. Employing the OneVsRest (OVR) technique and the IoT-23 dataset, this approach employs various ML algorithms, with Extreme Gradient Boosting achieving the highest accuracy of 98.89 %. Notably, Random Forest exhibits superior training and prediction times, with a mere 0.0311 seconds required for prediction. Through a thorough examination of these methodologies and their corresponding results, this dissertation underscores the significance of employing ML techniques in fortifying IoT security infrastructures. By leveraging advanced algorithms and evaluation metrics, the proposed approaches offer valuable insights into enhancing intrusion detection accuracy in IoT environments while addressing real-time constraints.

BIOGRAPHICAL SKETCH
Born in Yanbu, Saudi Arabia

B.S., Taibah University, Yanbu, Madinah, Saudi Arabia, 2014
M.S., Hood College, Frederick, Maryland, 2019
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2024

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 2021 - 2024

Qualifying Examination Passed: Spring 2021

Published Papers:

Alotaibi, Y., Alrefaei, A., Ilyas, M. (2022). Security Risks in Internet of Things (IoT): A Brief Survey. *Proceedings of the 26th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2022, Vol. I,* pp. 6-10. https://doi.org/10.54808/WMSCI2022.01.6

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. https://doi.org/10.54808/IMCIC2023.01.51

Alrefaei, A.; Ilyas, M. "Ensemble Deep Learning Model based on Multi-Class Classification Technique to Detect Cyber Attacks in IoT Environment," *2024 International Conference on Smart Computing, IoT and Machine Learning (SIML)*, Surakarta, Indonesia, 2024, pp. 174-179, doi: 10.1109/SIML61815.2024.10578143.

Alrefaei A, Ilyas M. Using Machine Learning Multiclass Classification Technique to Detect IoT Attacks in Real Time. *Sensors*. 2024; 24(14):4516, 1-19. https://doi.org/10.3390/s24144516