COLLEGE OF ENGINEERING
AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Abdulelah Al Hanif

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

“Optimizing Intrusion Detection in IoT Network Environments through Diverse Detection Techniques”

February 24, 2025, 11:30 a.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.
Dingding Wang, Ph.D.
Shihong Huang, Ph.D.

ABSTRACT OF DISSERTATION
Optimizing Intrusion Detection in IoT Network Environments through Diverse Detection Techniques

The rapid proliferation of Internet of Things (IoT) environments has revolutionized numerous areas by facilitating connectivity, automation, and efficient data transfer. However, the widespread adoption of these devices poses significant security risks. This is primarily due to insufficient security measures within the devices and inherent weaknesses in several communication network protocols, such as the Message Queuing Telemetry Transport (MQTT) protocol. MQTT is recognized for its lightweight and efficient machine-to-machine communication characteristics in IoT environments. However, this flexibility also makes it susceptible to significant security vulnerabilities that can be exploited. It is necessary to counter and identify these risks and protect IoT network systems by developing effective intrusion detection systems (IDS) to detect attacks with high accuracy. This dissertation addresses these challenges through several vital contributions. The first approach concentrates on improving IoT traffic detection efficiency by utilizing a balanced binary MQTT dataset. This involves effective feature engineering to select the most important features and implementing appropriate machine learning methods to enhance security and identify attacks on MQTT traffic. This includes using various evaluation metrics such as accuracy, precision, recall, F1-score, and ROC-AUC, demonstrating excellent performance in every metric. Moreover, another approach focuses on detecting specific attacks, such as DoS and brute force, through feature engineering to select the most important features. It applies supervised machine learning methods, including Random Forest, Decision Trees, k-Nearest Neighbors, and Xtreme Gradient Boosting, combined with ensemble classifiers such as stacking, voting, and bagging. This results in high detection accuracy, demonstrating its effectiveness in securing IoT networks within MQTT traffic. Additionally, the dissertation presents a real-time IDS for IoT attacks using the voting classifier ensemble technique within the spark framework, employing the real-time IoT 2022 dataset for model training and evaluation to classify network traffic as normal or abnormal. The voting classifier achieves exceptionally high accuracy in real-time, with a rapid detection time, underscoring its efficiency in detecting IoT attacks. Through the analysis of these approaches and their outcomes, the dissertation highlights the significance of employing machine learning techniques and demonstrates how advanced algorithms and metrics can enhance the security and detection efficiency of general IoT network traffic and MQTT protocol network traffic.

BIOGRAPHICAL SKETCH
Born in Abha, Saudi Arabia
B.S., King Khalid University, Abha, Asir, Saudi Arabia, 2016

M.S., George Mason University, Fairfax, Virginia, United States, 2021
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2025

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 2022 - 2025

Qualifying Examination Passed: Fall 2022

Published Papers:

Al Hanif, A., & Ilyas, M. (2023). A Brief Survey on the Internet of Things (IoT) Security. Journal of Systemics, Cybernetics and Informatics, 21(2), 74-82 (2023). https://doi.org/10.54808/JSCI.21.02.74

Al Hanif, A., & Ilyas, M. (2024). Effective Feature Engineering Framework for Securing MQTT Protocol in IoT Environments. Sensors 2024, 24(6), 1782, 1-19. https://doi.org/10.3390/s24061782

Al Hanif, A., & Ilyas, M. (2024). Enhance the Detection of DoS and Brute Force Attacks within the MQTT Environment through Feature Engineering and Employing an Ensemble Technique. International Journal of Artificial Intelligence and Applications (IJAIA), Vol.15, No.4, July 2024. https://doi.org/10.48550/arXiv.2408.00480

Al Hanif, A., & Ilyas, M. Real-Time Intrusion Detection in IoT Networks Using a Voting Classifier Ensemble Technique. IEEE Transactions on Machine Learning in Communications and Networking (submitted).