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

Announces the Ph.D. Dissertation Defense of

Omar Neil Gonzales

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

USER BEHAVIOR ANOMALY DETECTION APPROACHES TO MITIGATE INSIDER THREATS

July 1st, 2025 at 11:00 am
Zoom meeting:
https://fau-edu.zoom.us/j/82521371229?pwd=73xHrVbfwd4Szh9eGKdxHD02egnxC9.1 Meeting ID: 825 2137 1229 Passcode: 9dGB6

DEPARTMENT: College of Engineering and Computer Science

ADVISOR: KwangSoo Yang

PH.D. SUPERVISORY COMMITTEE: Kwangsoo Yang, Ph.D., Shihong Huang, Ph.D., Mohammad Ilyas, Ph.D., Imadeldin Mahgoub, Ph.D

ABSTRACT OF DISSERTATION

Insider threats represent a critical challenge in cybersecurity due to their ability to disguise malicious activity within legitimate user behavior. This dissertation proposes novel approaches to enhance insider threat mitigation through user behavior anomaly detection. First, a systematic survey is conducted to evaluate existing countermeasures, categorizing technical and human-centric strategies while identifying their limitations. Building upon these findings, the dissertation introduces two complementary detection frameworks: the Contiguous, Contextual, and Classifying Pipeline (C3P), which uses symbolic pattern mining and contextual modeling to autonomously score and classify sequences, and the Representation–Reconstruction Detection (R2D) framework, which leverages causal self-attention and variational autoencoding to identify anomalies in latent space. Together, these approaches address key challenges of scalability, limited contextual understanding, and data labeling dependency, providing a more adaptive, interpretable, and robust solution for detecting insider threats in complex user action sequences

BIOGRAPHICAL SKETCH

Omar Neil Gonzales was born in Peru. He earned his Bachelor of Science degree in Computer Science from Florida State University and later obtained his Master of Science degree in Computer Science from Florida Atlantic University.

Omar has proudly served in the United States Navy for 16 years as an Information Systems Technician, gaining extensive experience in secure communications, network infrastructure, and cybersecurity operations.

During his doctoral studies at Florida Atlantic University, Omar focused his research on cybersecurity with an emphasis on user behavior anomaly detection to mitigate insider threats. His dissertation introduced advanced frameworks for Contextual Sequence-Based User Behavior Anomaly Detection (CS-UBAD), including the Contiguous, Contextual, and Classifying Pipeline (C3P) and the Representation–Reconstruction Detection (R2D) framework, to improve anomaly detection accuracy and reduce false positives.

Omar has contributed to academic publications in the areas of cybersecurity and user behavior analytics, and has presented his research at conferences on security and applied machine learning. He plans to continue advancing the field of cybersecurity through research and professional contributions in both academic and operational environments.

FLORIDA ATLANTIC UNIVERSITY

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

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 3 years

Qualifying Examination Passed: Yes

Published Papers:

- **Contextual Sequence-Based User Behavior Anomaly Detection. 19 February 2025. IEEE Access. DOI: 10.1109/ACCESS.2025.3543500.**
- **Towards More Effective Insider Threat Countermeasures: A Survey of Approaches for Addressing Challenges and Limitations. 17 June 2024. DOI: 10.1109/SysCon61195.2024.10553441.**