FAMU-FSU College of Engineering

Machine Learning-Based Intrusion Detection in Smart Power Grids with Cyber-Physical Feature Fusion

CENTER FOR ADVANCED POWER SYSTEMS FSU

INTRODUCTION

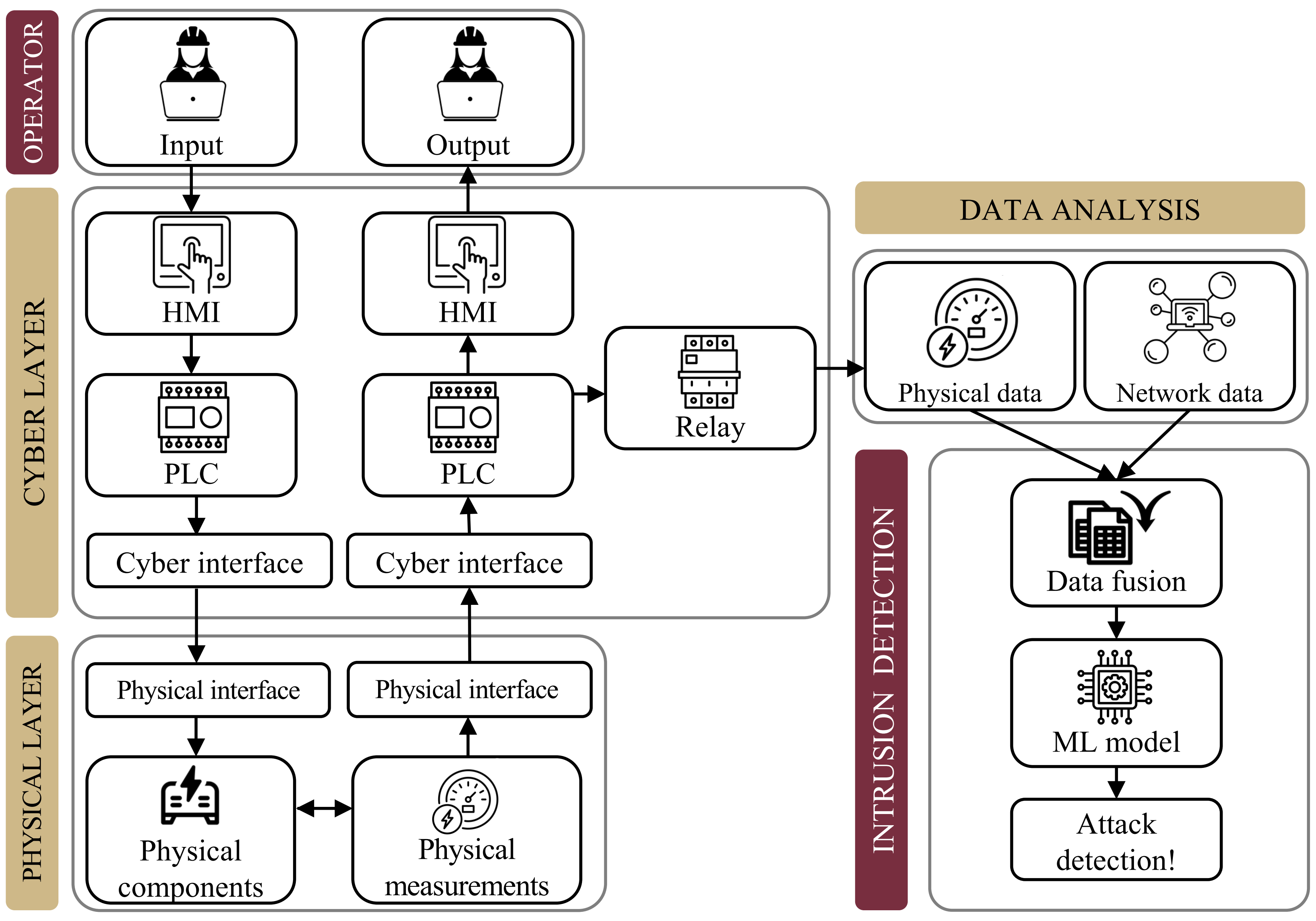
Cyber-physical systems (CPSs) are systems where physical components (physical layer) are managed by computer programs (cyber layer). Smart power grids are examples of CPSs where data communications take place among multiple components, which introduces vulnerability to attacks and malicious behavior. To detect such behavior, machine learning (ML) intrusion detection systems (IDSs) that are trained on cyber or physical data collected from the power grid components are proposed.

MOTIVATION

Existing IDSs neglect the fact that a smart grid is an integrated cyber-physical system, so they solely consider either physical or cyber features. They are also tested against basic cyber threats. Our work overcomes these limitations by proposing a graph neural network (GNN)-based IDS that fuses cyber and physical features while being robust against complex cyber threats.

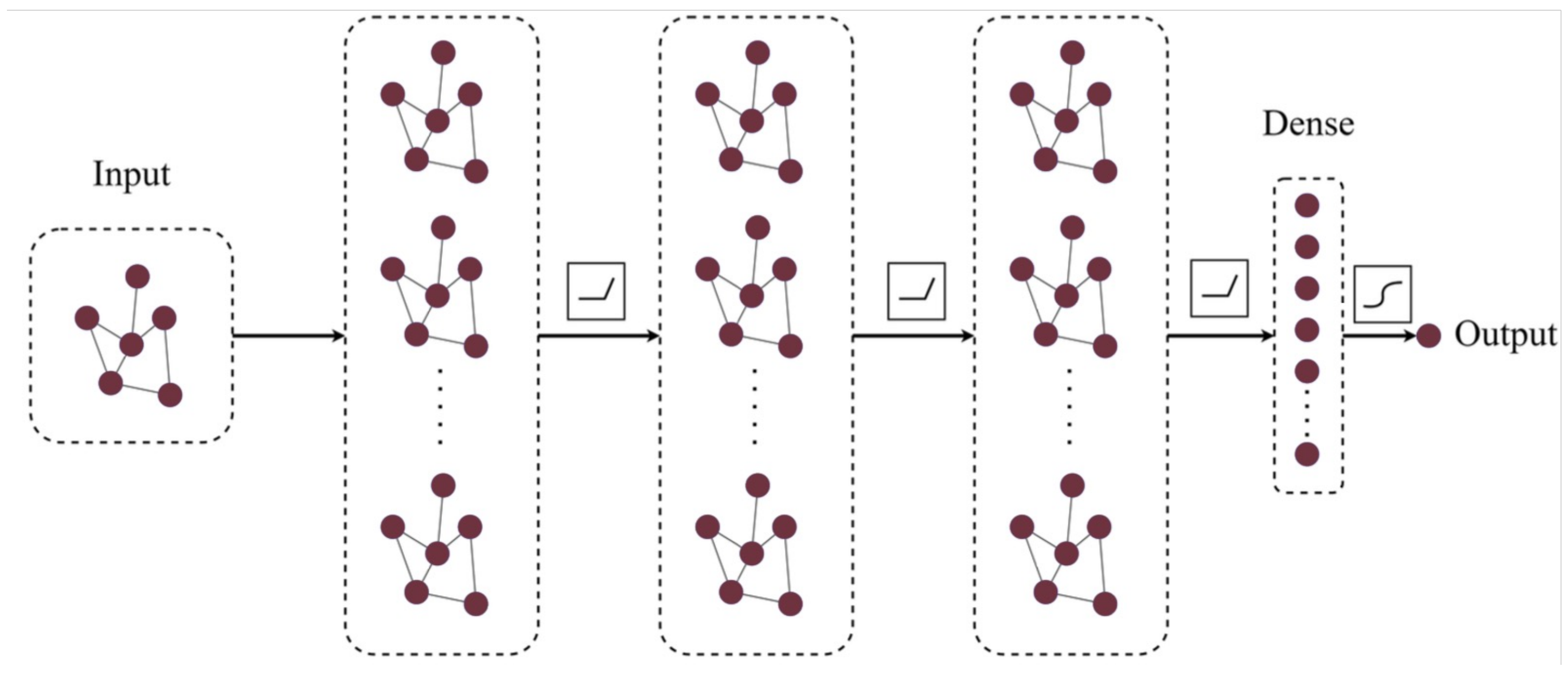
CYBER-PHYSICAL SYSTEM TESTBED

The physical layer is based on real-time simulations. The cyber layer hosts the human-machine interfaces (HMIs) and programmable logic controllers (PLCs) as shown below.



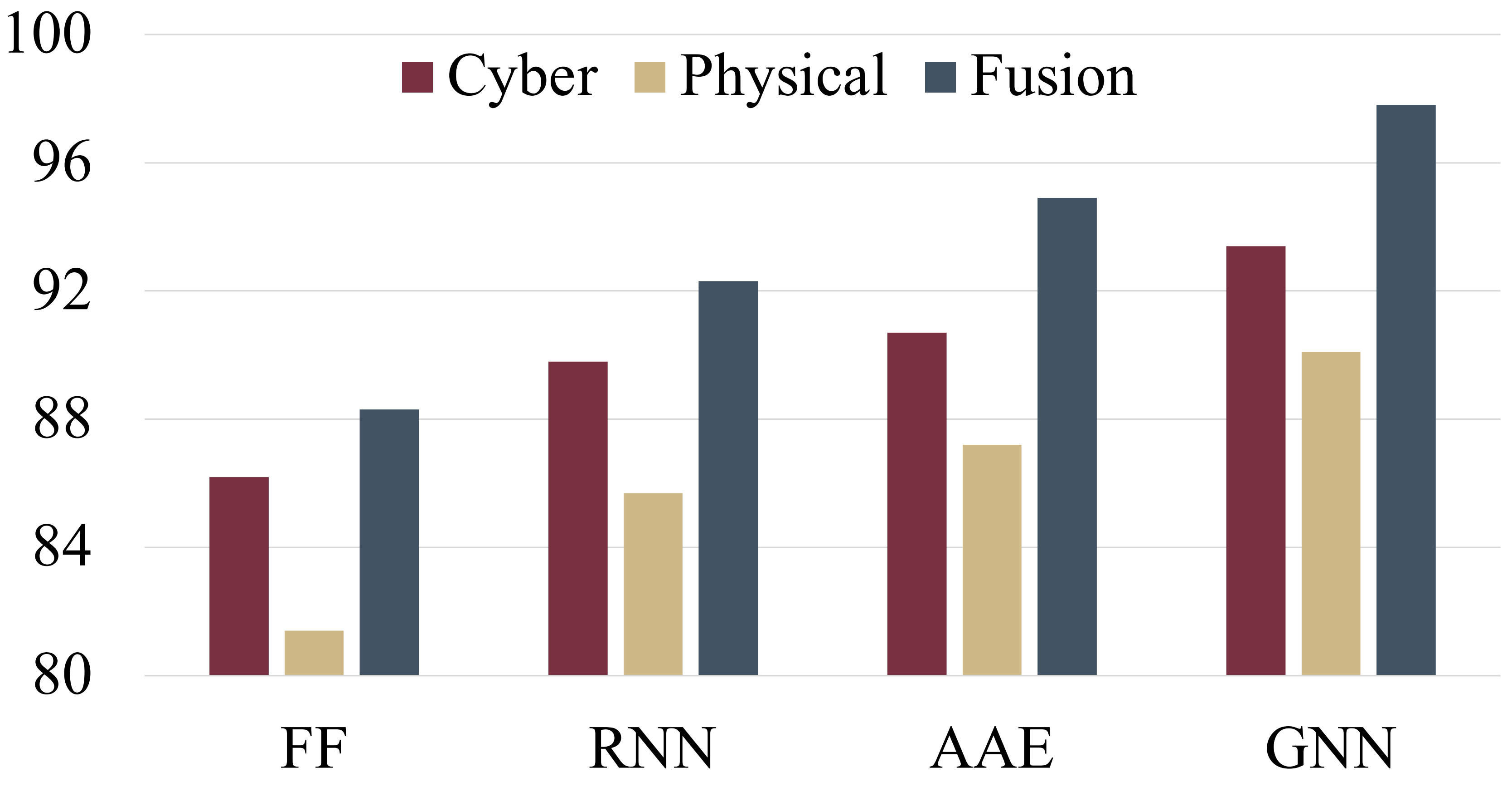
PROPOSED MODEL

We model the cyber-physical system as a connected undirected weighted graph, where nodes represent heterogeneous physical (power substations) and cyber (routers) components. Intra-edges represent the transmission lines connecting the power substation nodes in the physical layer. In the cyber layer, they represent the communication links among routers. Inter-edges are based on the coupling between the physical and cyber nodes. In the physical layer, weights are based on the line admittance values. The graphs are then used as inputs to the GNN-based IDS as shown in the figure below.



RESULTS

The proposed GNN model offers superior detection performance against complex false data injection attacks compared to existing feedforward (FF), recurrent neural network (RNN), and attentive autoencoder (AAE) models by 7 – 10% as shown below.



Abdulrahman Takiddin, Ph.D. | Assistant Professor | a.takiddin@eng.famu.fsu.edu
Department of Electrical and Computer Engineering | FAMU-FSU College of Engineering