A Comparative Analysis of Quantum-Enhanced Feedforward and Graph Attention Networks for Advanced Network Intrusion Detection and Classification

Tom Steinman
School of Science and Engineering
University of Missouri-Kansas City
Kansas City, MO, 64110
Email: tasn78@gmail.com

Selam Mitike
Baskin School of Engineering
University of California, Santa Cruz
Santa Cruz, CA, 95064
Email: selammitike8@gmail.com

***Abstract*—This study investigates the efficacy of Graph Attention Networks (GAT) and Feedforward Neural Networks (FNN) in detecting and tracing the origin of network intrusions. While GAT models are designed to leverage relational information in static graph structures, they may not always be optimal for datasets that do not inherently exhibit strong graph-based relationships. Our research compares the performance of GAT and FNN on binary and multi-class datasets containing various types of network attacks, with FNN serving as a baseline for comparison. Results indicate that FNN models outperform GAT, achieving higher accuracy in both binary and multi-class classification tasks due to their ability to handle non-relational, tabular data more effectively. Additionally, we introduce GAT-QNN and FNN-QNN models by integrating quantum-inspired layers, further enhancing performance. We analyze the models' predictions, demonstrating that while GAT offers advantages in specific scenarios, FNN's simplicity and efficiency make it more effective in the context of these intrusion detection tasks. These findings highlight the importance of selecting appropriate model architectures based on the nature of the data and suggest that FNN models are better suited for real-time intrusion detection when dealing with tabular datasets. Furthermore, our study explores the explainability features within both datasets, particularly highlighting the correlation between features and most important features provided by the CIC-IDS2017 dataset in classifying an attack. These findings suggest that FNN models, with their higher accuracy and robust explainability, may be better suited for real-time intrusion detection and classification tasks compared to GAT models.**

I. Introduction

Graph Neural Networks (GNNs) have emerged as powerful tools in the network security domain, offering significant advantages in representing and analyzing relational data inherent in network structures. Among these, Graph Attention Networks (GAT) utilize attention mechanisms to focus on the most relevant parts of the graph, thereby enhancing the detection of anomalies. GAT models have shown promise in various applications, including social network analysis, recommendation systems, and, importantly, network intrusion detection. However, GATs are primarily designed for static graphs, which limits their ability to capture the dynamic patterns essential for understanding evolving threats in a network environment. In contrast, Feedforward Neural Networks (FNNs), while traditionally less complex in structure, have proven to be highly effective in various machine learning tasks, including binary and multi-class classification. FNNs process input data in a straightforward, layer-by-layer manner, which can be particularly advantageous in scenarios where temporal dynamics are less critical, or when the dataset is well-structured, as in many intrusion detection tasks. Furthermore, recent advancements have explored the integration of quantum-inspired layers into neural networks. These layers leverage principles such as quantum parallelism and entanglement, potentially enhancing the computational power and learning capabilities of traditional models. In this study, we investigate the efficacy of combining these advanced techniques by evaluating Feedforward Neural Networks (FNN) and Graph Attention Networks (GAT), both with and without quantum-inspired layers, on binary and multi-class intrusion detection tasks. By rigorously comparing these models using datasets such as the Smart Home Intrusion Detection dataset and the CICIDS2017 dataset, we demonstrate that FNNs consistently outperform GAT models in terms of accuracy and robustness. The FNN binary model achieved an accuracy of 99.8%, and the multi-class classification model reached an accuracy of over 99.99%, underscoring the model's superior performance. This study underscores the importance of model selection based on the specific characteristics of the dataset and the task at hand, advancing the state-of-the-art in network security analytics.

II. Problem Statements

In modern network security, detecting intrusions is no longer sufficient; it is equally crucial to accurately classify the type of intrusion and understand its underlying patterns to mitigate potential damage and prevent future breaches. Network environments, such as smart homes and enterprise networks, involve complex interactions between numerous devices, creating a dynamic landscape where traditional intrusion detection systems (IDS) often fail to provide comprehensive protection. These systems may lack the precision needed to classify intrusions effectively and fail to provide insights into the specific characteristics of different attack types. Feedforward Neural Networks (FNNs) and Graph Attention Networks (GATs) offer robust frameworks for improving intrusion detection. FNNs, with their straightforward, layer-based structure, excel at processing well-structured data and have demonstrated high accuracy in both binary and multi-class intrusion detection tasks. Meanwhile, GATs utilize attention mechanisms to analyze the relationships within network traffic, focusing on the most relevant communication links between devices, which can help identify and understand patterns indicative of security breaches. The objective of this study is to evaluate and compare the performance of FNNs and GATs in detecting and classifying network intrusions. By focusing on the effectiveness of these models in various intrusion detection scenarios, this research seeks to advance the capabilities of network security systems, providing a more accurate and detailed understanding of intrusion dynamics. Specifically, this study aims to demonstrate how FNNs can outperform GATs in terms of detection accuracy and classification precision, ultimately enhancing the overall security of network environments.

III. Related Work

Neural network architectures have been used to address multiple real-world problems with high success. Their extension to graph-structured data has recently begun to be explored, leading to the development of graph neural networks (GNNs) that have achieved state-of-the-art performance in multiple domains. In the context of highly imbalanced application domains, such as network intrusion detection, GNNs have been utilized to model the network topology. However, the class imbalance problem still affects their performance.

Multiple approaches have been proposed to tackle these challenges, including Graph Attention Networks (GAT), Enhanced Residual Graph Attention Networks (E-ResGAT), and Temporal Graph Networks (TGN). The concept of Graph Attention Networks (GATs) was introduced by Petar Veličković [1]. GATs represent a significant advancement in the field of graph neural networks, addressing several limitations of earlier methods based on graph convolutions. GATs leverage masked self-attentional layers, allowing nodes to attend to their neighbors' features with varying importance. This dynamic weighting mechanism enables the model to assign different levels of significance to different nodes within a neighborhood, enhancing its ability to capture complex patterns in the data. Unlike previous methods that require costly matrix operations or upfront knowledge of the graph structure, GATs eliminate these requirements, making them more efficient and scalable for both inductive and transductive learning problems. GAT models have demonstrated or matched state-of-the-art performance across several established graph benchmarks, including the Cora, Citeseer, and Pubmed citation network datasets, as well as a protein-protein interaction dataset, underscoring their versatility and robustness.

Recent work has proposed Enhanced Residual Graph Attention Networks (E-ResGAT) [2], which build on top of the established GAT algorithms. E-ResGAT integrates residual learning into the GNNs to leverage the available graph information, adding residual connections as a strategy to address high class imbalance. This approach aims to retain the original information and improve the performance of minority classes. Extensive experiments on recent intrusion detection datasets have shown that embedding residuals in graph-based algorithms presents a strong advantage when learning under imbalanced domains, particularly in predicting minority classes.

In a comparative analysis with deep learning models like DNN, LSTM, and CNN, the paper "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017" [3] highlights the effectiveness of these models on the CIC-IDS2017 dataset, achieving accuracy rates of 94.61% with DNN, 97.67% with LSTM, and 98.61% with CNN. While these results demonstrate strong performance, our research with the GAT-QNN model further improves upon these benchmarks. Specifically, our GAT-QNN model achieved an accuracy of 98.7% on the CIC-IDS2017 dataset, surpassing even the best-performing CNN model reported in the comparative study. The added advantage of our approach lies in the explainability provided by the GAT's attention mechanism and the enhanced feature interaction captured by the quantum-inspired layer. This combination not only delivers higher accuracy but also offers deeper insights into the decision-making process, making it a robust solution for network intrusion detection.

Building upon the success of GNNs, traditional neural network models such as Feedforward Neural Networks (FNNs) have also been adapted and enhanced to address challenges in network intrusion detection. FNNs, known for their straightforward architecture and ability to model complex non-linear relationships, have been widely applied across various domains, including cybersecurity[4]. Their simplicity and efficiency make them a viable option for tasks requiring high throughput and real-time processing.

Recent advancements have seen the integration of quantum-inspired techniques into various neural networks[6][7], leading to the development of the FNN-QNN model. By incorporating a quantum-inspired layer, the FNN-QNN model leverages the principles of quantum superposition, allowing it to capture more intricate patterns within the data. This enhancement has proven particularly effective in domains characterized by high-dimensional feature spaces, such as network intrusion detection[4].

Literature suggests that these quantum-inspired layers can potentially improve the performance of traditional FNNs, making them competitive with more sophisticated GNN-based models like GAT. The integration of quantum-inspired layers in both the GAT and FNN architectures points to a growing interest in leveraging quantum computing concepts to enhance classical neural networks. This approach is gaining attention for its potential to address the challenges posed by high-dimensional feature spaces and imbalanced datasets, which are common in network intrusion detection scenarios. As research in this area progresses, quantum-enhanced neural networks may offer new avenues for improving the robustness and accuracy of intrusion detection systems, highlighting a promising direction for future exploration in this field.

IV. Methodology

In our research, we began by implementing and testing the Graph Attention Network (GAT) model using the Cora dataset, a well-established benchmark introduced in the paper by Petar Veličković et al. The Cora dataset consists of 2,708 nodes and is commonly used for binary classification tasks. This initial testing phase was crucial for ensuring that the GAT model functioned as expected. After confirming the model's reliability with the Cora dataset, we adapted it for use with our specific datasets, focusing on intrusion detection in smart home networks and the Canadian CIC-IDS2017 dataset.

Our first dataset was the Smart Home Network Intrusion Detection dataset, which comprises 148,517 nodes. Initially, we applied standard preprocessing techniques, including one-hot encoding for non-numerical features. This preprocessing increased the feature dimensionality from 23 to 104, which led to significant overfitting and resulted in low accuracy. To address this, we implemented several feature engineering techniques and model adjustments in the GAT model:

- We applied PCA to reduce the dimensionality of the feature space from 104 to a more manageable number, which helped mitigate overfitting and improved the model's accuracy.
- To further combat overfitting, we increased the dropout rate by 0.08. This adjustment helped prevent the model from becoming too reliant on specific features during training.

In addition to adjusting the dropout rate, we employed iterative training as a regularization technique. Iterative training involves gradually increasing the amount of data used for training in increments, allowing the model to adjust and generalize better as more data becomes available. Specifically, we trained the model incrementally by adding 10% of the data at each step. This method not only helped to prevent overfitting but also led to a smoother learning process, bringing the model's accuracy closer to that achieved with the Cora dataset. This approach was particularly effective in improving the performance of the GAT model on the Smart Home Network Intrusion Detection dataset.

Furthermore, we implemented an early stopping method as an additional regularization technique. Early stopping monitors the model's performance on the validation set and halts training when no further improvement is observed over a specified number of epochs. This prevents the model from overfitting to the training data and ensures that the final model configuration is the one that generalizes best to unseen data. The integration of early stopping was crucial in maintaining a balance between model complexity and generalization, particularly when working with our datasets, which have varying levels of feature dimensionality and complexity.

The CIC-IDS2017 dataset, containing 2,830,743 nodes and 79 features, presented different challenges. Initially, we trained the model by loading all data into a single batch, which resulted in an accuracy of only 87.1%. To optimize the training process and improve performance, we implemented the following adjustments. We selected only the most important features from the 79 available, focusing on those that had the greatest impact on the model's performance. Instead of loading all data into one batch, we split the data into multiple smaller batches. We also used data loaders for training, validation, and testing subsets with appropriate batch sizes. This change not only made the training process more efficient but also increased the model's accuracy to 94.8%.

GAT Model Architecture

The architecture of the GAT model consists of two primary layers that leverage attention mechanisms to process and aggregate information from node features. The input to the GAT model includes two key components. Node features and edge index. Node features represent the attributes or properties associated with each node, which are crucial for computing attention scores and aggregating information. Edge index defines the connections between nodes, indicating their neighborhood relationships in the graph, which guides the attention mechanism.

The first layer of the GAT model includes 8 attention heads, allowing the model to learn different aspects of node interactions simultaneously. This multi-head attention mechanism provides a richer representation of the graph's structure. The second layer, in contrast, has a single attention head, which consolidates the information from the previous layer's multiple heads into a more focused output, making the final decision on the specific classification. The output layer consists of two components: a softmax function, which normalizes the output into probabilities for each class, and the predicted class, which is the final classification result based on the highest probability.

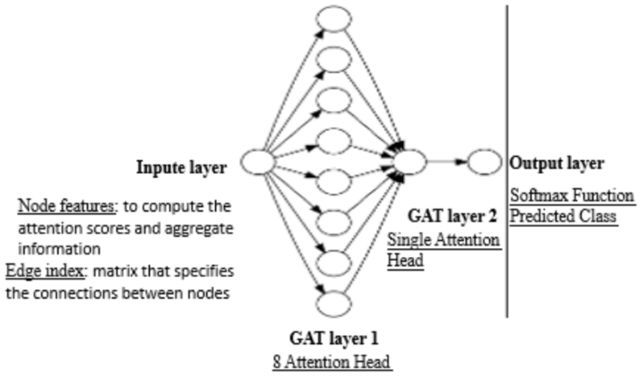
Inpute layer
Node features: to compute the attention scores and aggregate information
Edge index: matrix that specifies the connections between nodes
GAT layer 1
8 Attention Head
GAT layer 2
Single Attention Head
Output layer
Softmax Function
Predicted Class

Fig. 1. GAT model architecture designed for binary classification tasks.

Quantum-Inspired Layer Integration

In addition to the adjustments made to the GAT model, we explored integrating a quantum-inspired layer into the architecture. Quantum computing principles, particularly the principle of superposition, have the potential to capture complex patterns and correlations in data that classical methods might miss. The quantum layer in this model operates with a linear transformation and sigmoid activation:

- Linear Transformation: This is mathematically represented where W is a weight matrix and b is a bias vector. This transformation reshapes and combines the features in a way that highlights the most relevant patterns. $\mathbf{y} = \mathbf{W}\mathbf{x} + \mathbf{b}$
- Sigmoid Activation: Following the linear transformation, a sigmoid activation function is applied. This function ensures that the output values are squashed between 0 and 1, introducing non-linearity into the model and allowing it to handle complex relationships within the data. $\sigma(x) = \frac{1}{1+e^{-x}}$

By integrating this quantum-inspired layer, we were able to enhance the model's ability to capture more intricate patterns. This enhancement led to improved performance, increasing the accuracy for the Smart Home dataset to 87.3% and for the CIC-IDS2017 dataset to 98.7%.

In the context of integrating the quantum-inspired layer into the GAT model, we employed a grid search strategy to optimize the hyperparameters, particularly the dropout rate within the Quantum Neural Network (QNN) inspired layer's setup. Grid search is an exhaustive search method that systematically evaluates a predefined set of hyperparameters to identify the best configuration for the model. In our study, we focused on tuning the dropout rate, a critical hyperparameter in preventing overfitting, alongside other parameters in the GAT model. By applying grid search, we were able to systematically explore various combinations of these hyperparameters, assessing their impact on key performance metrics such as accuracy, precision, F1 score, and AUC for the classification tasks. This careful selection of hyperparameters was instrumental in achieving the optimal balance between model complexity and predictive performance, ensuring that the quantum-enhanced GAT model was finely tuned for the specific challenges presented by our datasets.

Feedforward Neural Network (FNN) Model

As the Smart Home Network Intrusion Detection dataset model follows the same architecture as the FNN binary detection model for the CIC-IDS2017 dataset, the focus will be placed on the models leading to the most accurate classification model.

Data Preprocessing and Feature Engineering

The dataset for the FNN model, sourced from CICIDS2017, was meticulously prepared through the following steps:

- **Data Concatenation and Cleaning:** CSV files from various network traffic scenarios were concatenated into a single DataFrame. Non-numeric columns such as *Flow ID*, *Source IP*, and *Timestamp* were removed, and rows with infinite or NaN values were dropped to maintain data integrity.
- **Categorical Encoding:** Categorical variables were converted into numerical representations through one-hot encoding, enabling seamless processing by the FNN model.
- **Label Encoding:** Labels were extracted and encoded into numeric values, facilitating multi-class classification.
- **Feature Scaling:** A *StandardScaler* was used to normalize the features, ensuring equal contribution from all input features during model training.
- **Batch Size:** A batch size of 64 was used for all FNN models.
- **Epochs:** Training and testing loop of 35 epochs was used for all FNN models.

Model Architecture

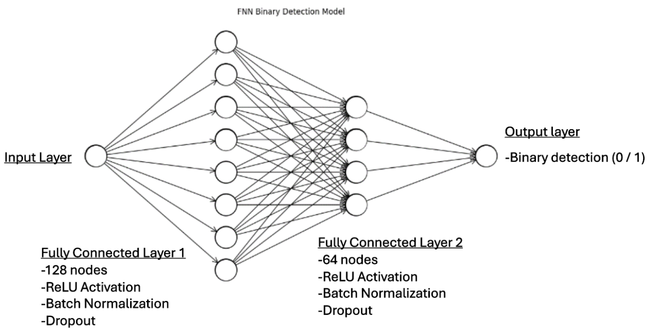

Fig. 2. FNN model architecture designed for binary classification tasks.

The FNN model, built on a traditional multi-layer perceptron (MLP) structure, includes:

- **Input Layer:** This layer receives a feature vector where each element corresponds to a specific attribute. The layer passes the input unchanged to the subsequent layers.
- **Hidden Layers:**
  - **First Hidden Layer:** Contains 128 neurons with ReLU activation, batch normalization for stability, and dropout (0.5) to prevent overfitting.

  - **Second Hidden Layer:** Comprises 64 neurons with similar batch normalization, dropout, and ReLU activation.
- **Output Layer:** Outputs raw logits for binary classification, with a sigmoid activation function to produce probability scores.

Training and Evaluation

The model was trained using cross-entropy loss and the Adam optimizer, supported by a learning rate scheduler (*ReduceLROnPlateau*). Performance metrics such as accuracy, precision, recall, and F1-score were employed, and confusion matrices were generated for detailed class-wise analysis.

Feedforward Neural Network with Quantum Neural Network (FNN-QNN)

Motivation and Quantum Layer Integration

To enhance the classical FNN with quantum computing principles, the FNN-QNN model integrates a quantum-inspired layer between the hidden layers and the output layer. This integration leverages quantum concepts such as superposition to capture complex data patterns that classical methods might miss.

Quantum-Inspired Layer Integration:

- **Quantum-Inspired Transformation:** This layer mimics quantum superposition by performing linear transformations and allowing the exploration of multiple states simultaneously. This enables the model to capture intricate relationships within the data.
- **Sigmoid Activation:** Following the quantum-inspired transformation, a sigmoid function bounds the output between 0 and 1, ensuring non-linearity and enhancing the model's decision boundaries.

Performance Improvements:

The inclusion of the quantum-inspired layer led to notable improvements in accuracy for both the Smart Home Network Intrusion Detection dataset and the CIC-IDS2017 dataset, demonstrating the potential of quantum-inspired techniques in advancing neural network capabilities.

Multi-Class Classification Models

Feedforward Neural Network (FNN)

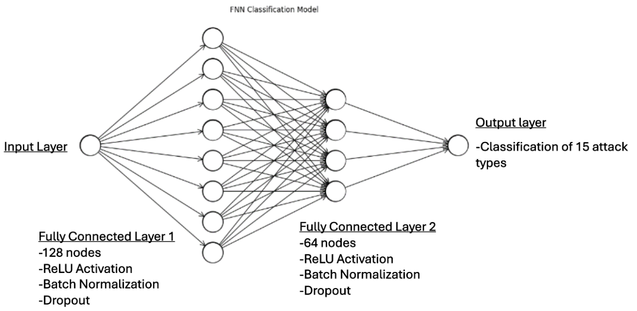

Fig. 3. FNN and FNN-QNN architectures for handling high-dimensional, multi-class classification tasks in the CIC-IDS2017 dataset.

Data Preprocessing and Feature Engineering

The dataset for the multi-class classification FNN model, sourced from CICIDS2017, underwent a similar preprocessing pipeline as the binary classification model, with the primary difference being:

- **Label Encoding:** Labels were encoded into numeric values representing different attack types and normal traffic, suitable for multi-class classification.

Model Architecture

The FNN model, designed for multi-class classification, includes:

- **Input Layer:** This layer receives the standardized feature vector from the dataset.
- **Hidden Layers:**
  - **First Hidden Layer:** Contains 128 neurons with ReLU activation, batch normalization for stability, and dropout (0.5) to prevent overfitting.
  - **Second Hidden Layer:** Comprises 64 neurons with similar batch normalization, dropout, and ReLU activation.
- **Output Layer:** Outputs raw logits for each class, which are used to compute the cross-entropy loss.

Training and Evaluation

The model was trained using cross-entropy loss and the Adam optimizer, with a learning rate scheduler (*ReduceLROnPlateau*) to adapt learning rates based on validation performance. Performance metrics such as accuracy, precision, recall, and F1-score were employed to evaluate the model.

Feedforward Neural Network with Quantum Neural Network (FNN-QNN)

Motivation and Quantum Layer Integration

The FNN-QNN model enhances the traditional FNN by incorporating a quantum-inspired layer. This integration leverages quantum computing concepts to capture complex patterns in the data that may not be fully captured by classical methods.

Quantum-Inspired Layer Integration:

- **Quantum-Inspired Transformation:** This layer performs transformations that allow the model to explore more complex feature interactions. It captures intricate relationships within the data, critical for accurate multi-class classification.
- **ReLU Activation:** Following the quantum-inspired transformation, ReLU activation is applied to introduce non-linearity and improve the model's ability to learn complex patterns.

Performance Improvements

The inclusion of the quantum-inspired layer in the FNN-QNN model resulted in improved classification accuracy on the CICIDS2017 dataset, further validating the efficacy of quantum-inspired techniques in neural network architectures.

Multi-Task Feedforward Neural Network (MT-FNN)

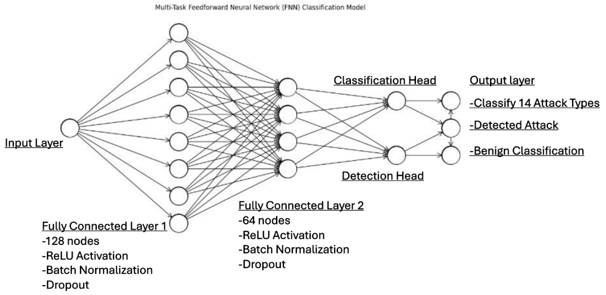

Fig. 4. Architecture of the Multi-Task Feedforward Neural Network designed for simultaneous detection and classification of network traffic.

Motivation

The MT-FNN model was designed to address multiple related tasks—network intrusion detection and classification—within a unified architecture. By sharing common representations across tasks, the model can generalize better and reduce computational overhead. As a majority of the misclassified attacks in the previous models were of the benign class, incorporating binary detection into the classification model was the next step in improving the classification accuracy.

Data Preprocessing

Similar to the FNN and FNN-QNN models, the MT-FNN model undergoes rigorous preprocessing, including data concatenation, cleaning, categorical encoding, and feature scaling.

Model Architecture

The MT-FNN consists of:

- **Shared Hidden Layers:**
  - **First Hidden Layer:** 128 neurons with batch normalization, ReLU activation, and dropout.
  - **Second Hidden Layer:** 64 neurons with similar operations, serving as a shared representation for subsequent tasks.
- **Task-Specific Layers:**
  - **Detection Head:** A single neuron for binary classification, utilizing a sigmoid activation function.
  - **Classification Head:** Multiple neurons for multi-class classification, producing raw logits processed by cross-entropy loss.

Training Process

The model is trained using a combined loss function, integrating both binary cross-entropy and multi-class cross-entropy losses. The Adam optimizer with weight decay regularizes the training, and a learning rate scheduler adjusts the learning rate based on validation performance.

Model Evaluation and Visualization

The MT-FNN's performance is evaluated using metrics specific to both detection and classification tasks, including accuracy, precision, F1 score and ROC AUC. Visualizations, including confusion matrices and plots of key metrics over epochs, provide insights into the model's learning behavior and effectiveness.

V. Result

In our research, we initially enhanced the Graph Attention Network (GAT) model with a quantum-inspired layer (GAT-QNN) to leverage its potential benefits in network intrusion detection. This enhancement aimed to improve the model's ability to learn complex relationships within the data. The performance of both the standard GAT and the GAT-QNN models was evaluated using two distinct datasets: CIC-IDS2017 and the Smart Home Network Intrusion Detection dataset. The evaluation focused on key metrics such as accuracy, precision, F1-score, and Area Under the Curve (AUC) to assess the effectiveness of each model in detecting and classifying network intrusions.

A. *Smart Home Network Intrusion Detection Dataset*

TABLE I
Comparison of AI Models on the Smart Home Network Intrusion Detection Dataset

Model	Accuracy (%)	Precision (%)	F1 Score (%)	ROC AUC (%)
GAT	86.7	93.6	94.3	96.4
GAT-QNN	87.3	90.2	91.5	92.2
FNN	96.58	99.22	96.32	99.49
FNN-QNN	98.65	99.92	98.59	99.93

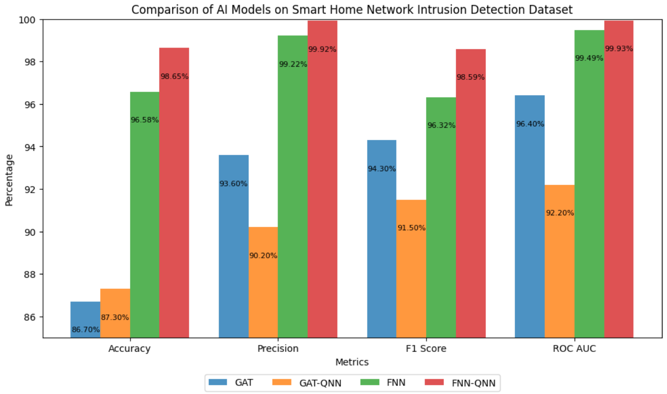

Fig. 5. Comparison of AI Models on the Smart Home Intrusion Detection Dataset

Smart Home Network Intrusion Detection Dataset: In contrast to the CIC-IDS2017 results, the Smart Home Network Intrusion Detection dataset presented different challenges for the models. Here, the addition of the quantum-inspired layer led to a more modest improvement in accuracy, with the GAT-QNN model achieving 87.3% compared to 86.7% for the standard GAT model. However, this improvement in accuracy was accompanied by a reduction in precision and F1-score, with the GAT-QNN model recording 90.2% and 91.5%, respectively, compared to the GAT model's 93.6% and 94.3%.

Moreover, the AUC also decreased from 96.4% for the GAT model to 92.2% for the GAT-QNN model, indicating a reduced ability to distinguish between classes in this dataset. These results suggest that while the quantum-inspired layer provides benefits in terms of accuracy, it may introduce complexities that require careful calibration, particularly in datasets with temporal dynamics and class imbalances like the Smart Home dataset.

B. CIC-IDS2017 Dataset

TABLE II
COMPARISON OF AI MODELS ON THE CIC-IDS2017 DATASET

Model	Accuracy (%)	Precision (%)	F1 Score (%)	ROC AUC (%)
GAT	94.8	95.5	94.9	99.4
GAT-QNN	98.7	98.7	98.7	99.2
FNN	98.07	99.75	98.78	99.79
FNN-QNN	98.31	99.16	98.94	99.84

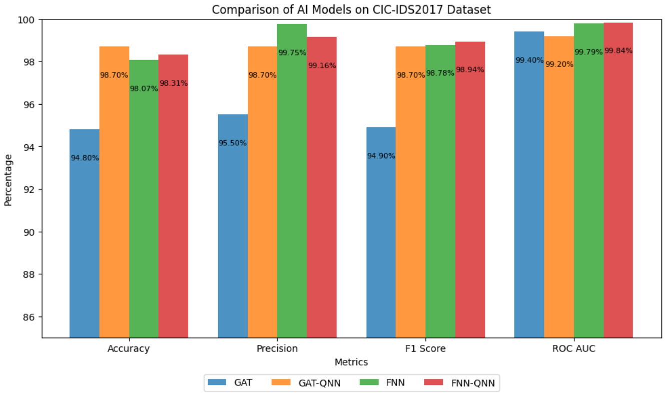

Fig. 6. Comparison of AI Models on the CIC-IDS2017 Dataset

CIC-IDS2017 Dataset: The results for the CIC-IDS2017 dataset demonstrate a clear improvement when the quantum-inspired layer is integrated into the GAT model. The GAT-QNN model achieved an impressive accuracy of 98.7%, surpassing the 94.8% accuracy recorded by the standard GAT model. Precision and F1-score both saw significant gains, with the GAT-QNN model reaching 98.7% for both metrics, compared to 95.5% and 94.9%, respectively, for the GAT model.

Interestingly, while the AUC for the GAT-QNN model was slightly lower at 99.2% compared to the GAT model's 99.4%, the overall performance metrics indicate that the quantum-enhanced model is more effective in this context. The improvement in accuracy, precision, and F1-score suggests that the GAT-QNN model is better equipped to handle the complexity of the CIC-IDS2017 dataset, which features a high-dimensional space and diverse intrusion patterns.

These results underscore the potential of the quantum-inspired layer in enhancing the GAT model's performance in datasets with high complexity and dimensionality. The improved metrics across the board suggest that the GAT-QNN model can effectively capture intricate patterns that may be less accessible to the standard GAT model.

The comparative analysis between the two models across both datasets reveals several important insights:

- GAT-QNN Superiority in Complex, High-Dimensional Data: The GAT-QNN model shows substantial improvements in the CIC-IDS2017 dataset, indicating its potential for handling high-dimensional data and complex patterns. The enhancements in accuracy, precision, and F1-score underscore the utility of the quantum-inspired layer in such contexts. This suggests that the quantum-enhanced GAT model is well-suited for environments where the data is varied and intricate, such as large-scale network intrusion detection tasks.
- Challenges with Temporal Dynamics and Class Imbalance: On the other hand, the Smart Home dataset results highlight the challenges posed by temporal dynamics and class imbalance. The decrease in precision, F1-score, and AUC for the GAT-QNN model suggests that the benefits of the quantum-inspired layer are not uniformly applicable across all datasets and may require additional adjustments for optimal performance. Specifically, in scenarios where data is more temporally dependent or where there is a significant class imbalance, the integration of quantum-inspired layers might necessitate more sophisticated tuning or even different architectural adjustments.
- Dataset-Specific Performance Considerations: The results from both datasets indicate that while the quantum-inspired enhancement generally improves accuracy, its impact on other metrics such as precision, F1-score, and AUC can vary significantly depending on the dataset's characteristics. This highlights the importance of tailoring model enhancements to the specific challenges presented by different types of data, rather than assuming a one-size-fits-all improvement.
- Implications for Future Work: The varying performance of the GAT-QNN model across these datasets suggests several avenues for future research. For instance, further investigation into how quantum-inspired layers interact with different types of data could yield insights that lead to more consistent improvements across a broader range of scenarios. Additionally, exploring alternative enhancements or combinations of techniques may help address the limitations observed in the Smart Home dataset, potentially leading to models that are both highly accurate and robust across diverse applications.

While the GAT-QNN model demonstrated some improvement in accuracy over the standard GAT model, particularly in datasets with high dimensionality, its performance was noticeably hindered in the Smart Home Network Intrusion Detection dataset. This underperformance can be attributed to the GAT model's reliance on attention mechanisms, which are effective in focusing on relevant parts of the graph but are not inherently designed to capture temporal dependencies. In contrast, the Feedforward Neural Network (FNN), which does not depend on graph-based structures, was able to better utilize the temporal features inherent in the dataset, leading to superior performance in terms of precision, F1-score, and AUC.

The GAT model struggles to incorporate the sequential nature of the data into its decision-making process, which limits its ability to accurately classify instances that rely on temporal information. The temporal dynamics present in the Smart Home dataset, coupled with class imbalance, posed significant challenges for the GAT model, resulting in reduced effectiveness despite the slight improvement in accuracy with the quantum-inspired layer. This comparison highlights the limitations of GAT-based models in scenarios where temporal features play a crucial role, suggesting that models like FNNs may be more suitable for such contexts.

CIC-IDS2017 Classification Models

TABLE III
COMPARISON OF FNN CLASSIFICATION MODELS ON THE CIC-IDS2017 DATASET

Model	**Accuracy (%)**	**Precision (%)**	**F1 Score (%)**	**ROC AUC (%)**
FNN	96.01	96.02	95.49	99.49
FNN-QNN	98.42	98.39	98.38	99.86
Multi-Task FNN	99.999+	99.999+	99.999+	99.999+

Feedforward Neural Network (FNN) and FNN-QNN Model Performance:

The performance of the Feedforward Neural Network (FNN) and its quantum-inspired variant (FNN-QNN) on the CIC-IDS2017 dataset highlights the efficacy of traditional neural network architectures for handling high-dimensional, multi-class classification tasks in cybersecurity. The FNN model achieved results with an accuracy of 96.01%, demonstrating its capability to process diverse network traffic features and classify them into predefined classes with high precision and F1-scores of 96.02% and 95.49%, respectively.

The introduction of a quantum-inspired layer in the FNN-QNN model further enhanced the performance, resulting in a marginal increase in accuracy to 98.42% and improvements in F1-score and ROC AUC. These enhancements suggest that the quantum-inspired layer contributes to a more nuanced understanding of the complex relationships within the data, allowing the model to make more precise classifications.

Discussion on Quantum-Inspired Enhancements:

The integration of quantum-inspired layers in the FNN-QNN model underscores the potential benefits of such techniques in the context of high-dimensional data. The improvements observed in accuracy and ROC AUC, albeit slight, indicate that quantum-inspired layers can enhance the model's ability to capture subtle patterns and interactions that might be overlooked by classical neural networks. This suggests that while traditional FNN architectures are effective, the addition of quantum-inspired components can lead to more refined and potentially more powerful models, particularly in scenarios that demand high precision and robustness.

Multi-Task Feedforward Neural Network (FNN) Model for Combined Detection and Classification:

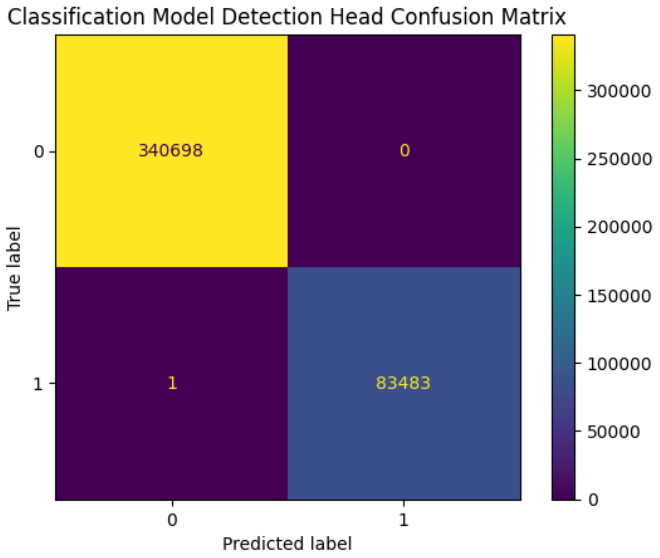

Fig. 7. Multi-Task FNN Detection Confusion Matrix for CIC-IDS2017 Dataset

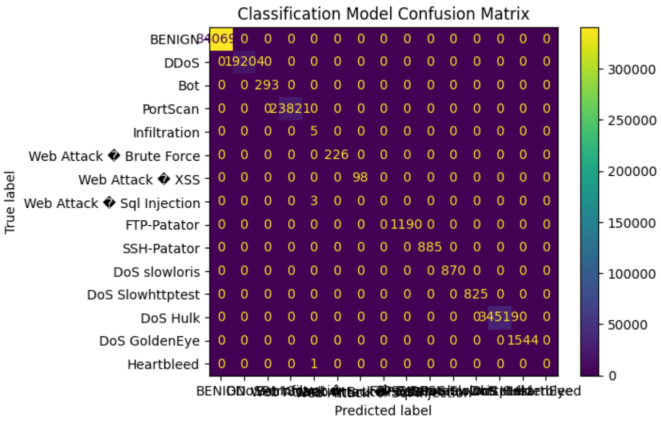

Fig. 8. Multi-Task FNN Confusion Matrix for CIC-IDS2017 Dataset

The Multi-Task FNN model represents a significant advancement in the simultaneous execution of network intrusion detection and classification tasks. By leveraging a shared architecture for feature extraction, followed by distinct heads for detection and classification, the model efficiently learns to perform both tasks from a unified set of features. This approach not only improves computational efficiency but also enhances the model's overall performance, as evidenced by over .9999 scores in accuracy, precision, F1 score and ROC accuracy. These metrics were obtained without the removal of attack categories with a low concentration of data from the dataset[8][9].

The shared learning framework of the Multi-Task FNN model allows for the efficient utilization of common features across both tasks, leading to improved generalization and more accurate detection and classification outcomes. The model's ability to maintain high performance in both tasks suggests that multi-task learning is a viable strategy for enhancing the capabilities of neural networks in cybersecurity applications.

Implications for Multi-Task Learning:

The success of the Multi-Task FNN model in handling both detection and classification tasks on the CIC-IDS2017 dataset highlights the broader applicability of multi-task learning in complex, real-world scenarios. By training a single model to perform multiple related tasks, this approach not only streamlines the learning process but also reduces the need for multiple models, thereby conserving computational resources. Furthermore, the model's strong performance across various metrics, including accuracy, precision, and F1-score, indicates that multi-task learning can lead to models that are both highly efficient and effective in addressing the multifaceted challenges of network intrusion detection[10][11][3].

Explainability in Optimizing Classification with the CIC-IDS2017 Dataset:

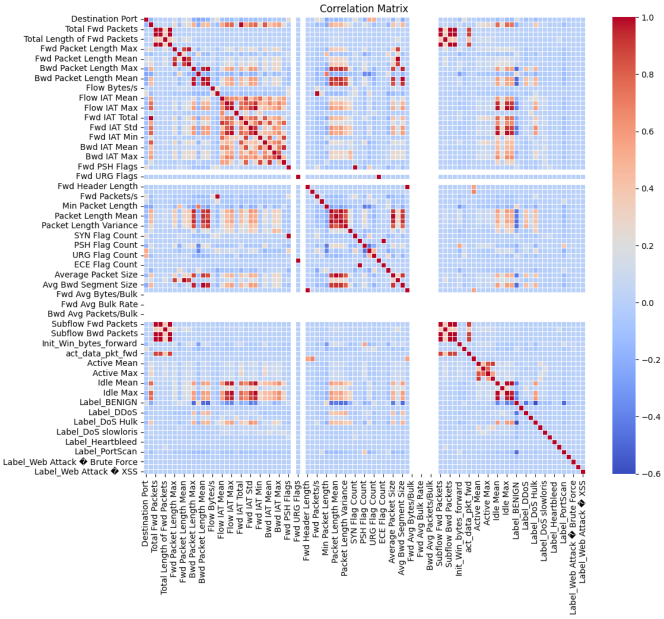

Fig. 9. CIC-IDS2017 Correlation Matrix

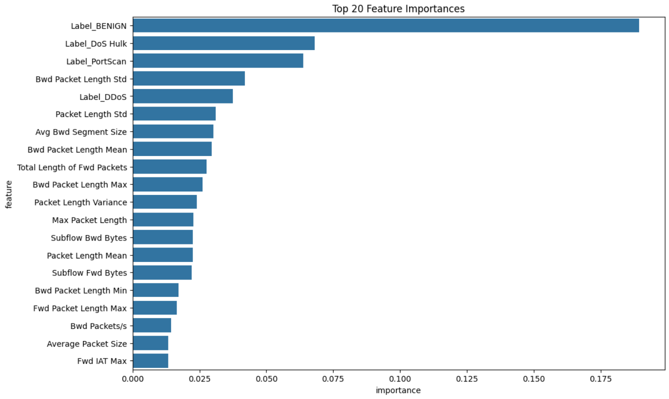

Fig. 10. CIC-IDS2017 Dataset Top 20 Features

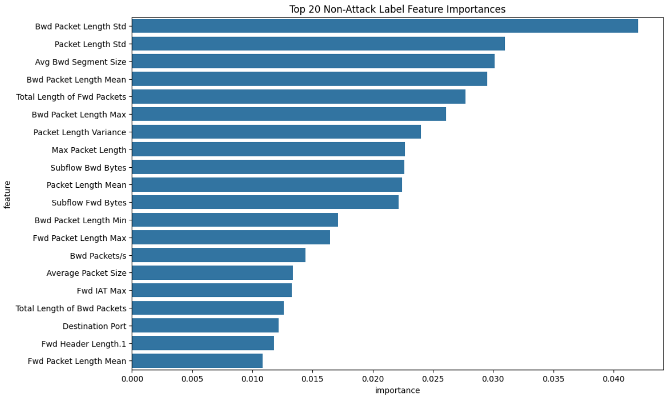

Fig. 11. Multi-Task FNN Confusion Matrix for CIC-IDS2017 Dataset

The analysis of the CIC-IDS2017 dataset through the correlation matrix and feature importance graphs has provided significant insights into the critical features that influence network intrusion detection[12]. The correlation matrix, in figure 9, reveals complex interdependencies among various network traffic features, indicating the presence of both strong positive and negative correlations. This understanding of feature interactions is crucial for enhancing model accuracy and reducing redundancy in feature selection.

The top 20 feature importance graph underscores the significance of backward (Bwd) and forward (Fwd) packet lengths, as well as segment sizes, in accurately identifying network intrusions. Features such as Bwd Packet Length Std, Packet Length Std, and Avg Bwd Segment Size emerged as the most influential, highlighting their critical role in the model's decision-making process. Additionally, the feature importance analysis for benign labels emphasizes the distinction between normal and attack traffic, with the 'Label_BENIGN', 'Label_DoS Hulk', and 'Label_PortScan' features having the highest importance. These findings suggest that focusing on packet length and flow-based metrics can significantly improve the detection accuracy of network intrusion detection systems.

Overall, these insights reinforce the need for a targeted approach in feature selection, particularly emphasizing packet-based metrics to enhance the detection of both attack and benign traffic within network environments. The outcomes of this study provide a robust foundation for future work in optimizing feature selection and model architectures to further advance network intrusion detection capabilities.

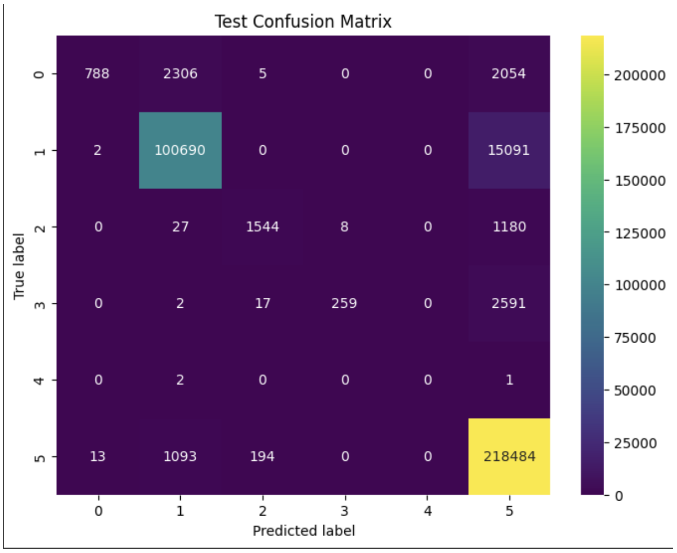

Fig. 12. GAT Confusion Matrix for CIC-IDS2017 Dataset

The confusion matrix for the GAT model applied to the CIC-IDS2017 dataset, as shown in Fig. 12, provides valuable insights into the model's performance and its ability to classify network intrusions across multiple categories. The GAT model shows strong performance in identifying the majority class (Class 1), with a large number of true positives correctly classified. However, there are significant misclassifications observed, particularly with instances from Class 5 being misclassified as Class 0 and Class 1. This suggests that while the GAT model effectively captures the dominant patterns within the data, it struggles with distinguishing between classes that share similar feature spaces or exhibit subtle differences. The GAT model's confusion matrix also reflects the challenges associated with class imbalance, as evidenced by the lower recall for minority classes. This indicates that the GAT model may have a bias towards more prevalent classes, leading to underperformance in accurately detecting less frequent intrusion types. This imbalance affects the model's overall F1-score and may reduce its reliability in real-world scenarios where detecting rare but critical intrusions is crucial. In comparison, the Multi-Task FNN model exhibits a more consistent and balanced performance, making it a more reliable choice for intrusion detection tasks where the ability to accurately classify both common and rare intrusions is critical.

While the quantum-inspired layers provided significant improvements in model performance, particularly in the CIC-IDS2017 dataset, these enhancements come with certain trade-offs. The introduction of quantum-inspired layers increases computational overhead, as these layers require more complex calculations that can strain system resources, particularly when scaling to larger datasets or deploying in real-time environments. Additionally, the need for specialized hardware to fully leverage the potential of quantum-inspired techniques poses a practical challenge for widespread adoption. This complexity may limit the applicability of such models in resource-constrained settings or where rapid deployment is critical. A more nuanced approach may involve balancing the benefits of quantum-inspired layers with the practical considerations of computational efficiency and scalability, ensuring that the model enhancements are both effective and feasible for real-world applications.

VI. Conclusion

The comparative analysis of the GAT, GAT-QNN, FNN, FNN-QNN, and Multi-Task FNN models provides valuable insights into the benefits of integrating quantum-inspired layers and adopting multi-task learning strategies in neural network architectures. While the quantum-inspired enhancements offer marginal improvements in certain metrics, the Multi-Task FNN model demonstrates a more significant leap in performance by effectively combining detection and classification tasks. However, the findings of this study are somewhat limited by the narrow focus on specific datasets. Future research should explore the applicability of these models across a broader range of datasets, including those with different network topologies, traffic patterns, and dynamic data. This would provide a clearer understanding of the models' potential in various real-world scenarios.

Moreover, while the quantum-inspired layers show potential, their integration introduces complexities such as increased computational overhead and the need for specialized hardware. These challenges highlight the importance of balancing the benefits of advanced techniques with practical considerations, particularly in large-scale or resource-constrained environments.

For future research, exploring more sophisticated quantum-inspired techniques and developing advanced multi-task learning frameworks could further enhance the capabilities of neural networks in cybersecurity. Additionally, addressing the limitations identified in this study such as challenges of scalability will be crucial for the broader application of these models in network security and beyond.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant Number CNS-2349236. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. We would like to thank Dr. Yugyung Lee and Dr. Dianxiang Xu for their invaluable guidance, support, and insights throughout this research project.

References

[1] P. Veli, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio, "Graph attention networks," *arXiv preprint arXiv:1710.10903*, 2017.

[2] L. Chang and P. Branco, "Embedding residuals in graph-based solutions: The e-ressage and e-resgat algorithms. a case study in intrusion detection," *Applied Intelligence*, 2024.

[3] J. Jose and D. V. Jose, "Deep learning algorithms for intrusion detection systems in internet of things using cic-ids 2017 dataset," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 1, pp. 1134–1141, 2023.

[4] S. Siva Shankar, B. T. Hung, P. Chakrabarti, T. Chakrabarti, and G. Parasa, "A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system," *Education and Information Technologies*, vol. 29, no. 4, pp. 3859–3883, 2024.

[5] R. Atefinia and M. Ahmadi, "Network intrusion detection using multi-architectural modular deep neural network," *The Journal of Supercomputing*, vol. 77, no. 4, pp. 3571–3593, 2021.

[6] M. Raparthi, "Quantum-inspired neural networks for advanced ai applications-a scholarly review of quantum computing techniques in neural network design," *Journal of Computational Intelligence and Robotics*, vol. 2, no. 2, pp. 1–8, 2022.

[7] Q. T. Nguyen, L. Schatzki, P. Braccia, M. Ragone, P. J. Coles, F. Sauvage, M. Larocca, and M. Cerezo, "Theory for equivariant quantum neural networks," *PRX Quantum*, vol. 5, no. 2, p. 020328, 2024.

[8] H. Friji, A. Olivereau, and M. Sarkiss, "Efficient network representation for gnn-based intrusion detection," in *Applied Cryptography and Network Security*, M. Tibouchi and X. Wang, Eds. Cham: Springer Nature Switzerland, 2023, pp. 532–554.

[9] D. Pujol-Perich, J. Suarez-Varela, A. Cabellos-Aparicio, and P. Barlet-Ros, "Unveiling the potential of graph neural networks for robust intrusion detection," *SIGMETRICS Perform. Eval. Rev.*, vol. 49, no. 4, p. 111–117, jun 2022. [Online]. Available: https://doi.org/10.1145/3543146.3543171

[10] X. Hu, W. Gao, G. Cheng, R. Li, Y. Zhou, and H. Wu, "Toward early and accurate network intrusion detection using graph embedding," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5817–5831, 2023.

[11] V. Hnamte and J. Hussain, "Dependable intrusion detection system using deep convolutional neural network: A novel framework and performance evaluation approach," *Telematics and Informatics Reports*, vol. 11, p. 100077, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772503023000373

[12] I. M. Sayem, M. I. Sayed, S. Saha, and A. Haque, "Enids: A deep learning-based ensemble framework for network intrusion detection systems," *IEEE Transactions on Network and Service Management*, 2024.

[13] A. Kumar and D. Pandey, "Enhancing intrusion detection with ml and deep learning: A survey of cicids 2017 and cse-cic-ids2018 datasets," in *AIP Conference Proceedings*, vol. 3168, no. 1. AIP Publishing, 2024.

[14] O. Elnakib, E. Shaaban, M. Mahmoud, and K. Emara, "Eidm: deep learning model for iot intrusion detection systems," *The Journal of Supercomputing*, vol. 79, no. 12, pp. 13 241–13 261, 2023.

[15] A. Henry, S. Gautam, S. Khanna, K. Rabie, T. Shongwe, P. Bhattacharya, B. Sharma, and S. Chowdhury, "Composition of hybrid deep learning model and feature optimization for intrusion detection system," *Sensors*, vol. 23, no. 2, p. 890, 2023.