Network Intrusion Detection using Hybrid Artificial Neural Networks and Variational Quantum Classifier

David Q. Liu, Ph.D.
Associate Professor
Department of Computer Science
Purdue University Fort Wayne
Fort Wayne, Indiana 46815
liud@pfw.edu

Praveen Venkatachalam
Department of Computer Science
Purdue University Fort Wayne
Fort Wayne, Indiana 46815
venkp01@pfw.edu

Furqan Khan
Department of Computer Science
Purdue University Fort Wayne
Fort Wayne, Indiana 46815
khanfa01@pfw.edu

ABSTRACT

The exponential growth of internet reliance for everyday activities, has opened the window for cyber-attacks more deadly. It is estimated that approx. 6.3 trillion intrusion attacks happened in 2022 alone. This stress the importance of network intrusion detection systems (NIDS) significance for protecting the systems. In this paper we have implemented a hybrid artificial neural network with 1 layer of CNN for feature extraction and an LSTM RNN model for sequential data analysis and 3-layer DNN for classification and error correction. Also, VQC (Variational Quantum classifier) is implemented display the potential of using quantum computers as standalone systems to detect network intrusion for large classical datacenters. The desired network features and topologies are extracted from the KDDCup 99 dataset in combination with various data transformation technique. For effective classification of network intrusions and zero-day attack predictions.

1. INTRODUCTION

In the today's world as we are highly relying on computers and Internet, building secure networks is among the challenges we face. The number of threats being faced over the internet is rising exponentially over the years.[1] The Internet is facing different attacks that puts the data and privacy at risk. To mitigate the impact of these attacks, researchers have proposed numerous techniques, however, as the nature of attacks is constantly evolving, with attackers devising new methods to breach systems, a multitude of challenges arise in effectively safeguarding against such threats. [2]

In order to prevent loss of information, intrusion detection systems (IDS) were developed to IDS is a mechanism that monitors the network traffic to detect any malicious attacks and take preventive measures against intrusions. The Intrusion detection systems are classified into two types: Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection System (HIDS). Network Intrusion Detection System (NIDS) works by monitoring network traffic at crucial network points and analyzing it for suspicious activities, such as attempts to exploit vulnerabilities or gain unauthorized access to a network. HIDS on the other hand monitors system activities in form of various log files running on local host computer to detect attacks. NIDS checks each packet contents network traffic flow. [3]

Machine Learning has been growing at a rapid rate and also making an impact in the field of cybersecurity. ML models can learn to make decision based on the available data, making it an asset to monitor mutating IT environments. Enhancing NIDS with supervised ML models can be challenging. However, by creating a training dataset where the samples are labeled as benign or malignant, it is possible to develop a fully autonomous ML based Network Intrusion Detection System.[4]

Although Machine Learning and Deep Learning has been advancing rapidly in the world of cybersecurity, it faces computational overload issues due to enormous amount of data and computational power requirement. These issues can be addressed using quantum deep learning. Quantum computing utilizes the principles of quantum mechanics such as superposition and entanglement to increase the computational efficiency and reduce power consumption.[5]

Quantum computing is a potential solution for problems faced by classical computing in terms of computational complexity. Quantum Machine Learning applications have shown to improve the capacity and efficiency over classical ML methods [6]. Quantum Machine Learning is the interplay of machine learning and quantum computing which seeks to understand the advantages of quantum devices in developing new algorithms. Quantum neural networks (QNN) are heavily explored in Quantum machine learning. QNNs have emerged as a new class of promising quantum algorithms which are inspired by Artificial Neural Networks (ANNs) and also resemble in architectural structure to ANNs. Convolutional Neural Networks (CNN) are a type of deep learning algorithm used for processing data with grid-like structures, particularly images and videos. They are ideal for tasks such as object recognition, detection, and segmentation, and have become increasingly popular for their ability to learn complex patterns in data [7].

Long Short-Term Memory (LSTM) based Recurrent Neural Networks (RNNs) have shown to achieve remarkable accuracy on cognitive intelligence applications. It is useful for tabular data because it can handle variable length sequence and capture long term dependencies. [8]

Deep Neural Networks (DNN) are a family of machine learning models that are capable of handling a wide range of tasks, such as classification, regression, and pattern recognition [9]. VQC, on the other hand, is an emerging field of research that utilizes quantum circuits to perform computations and optimization tasks for classification problems. It has the potential to provide faster and more efficient classification results compared to classical machine learning algorithms, particularly for large datasets [11].

2. CONCEPT

Neural networks are composed of neurons, which mimic the input-output structure of biological neurons. The number of hidden layers in a neural network determines its depth and ability to extract intricate patterns from data, with training beginning by calculating the input sum of the weighted parameters and bias given by:

$$z = \sum_{i=1}^{n} wixi + b$$

Neural networks use a non-linear activation function to map inputs to outputs, and weights are trained using the backpropagation algorithm and gradient descent methods. The cost function, measured by the mean squared error, is used to iteratively update the weights until the model accurately predicts the desired output which is defined as:

$$C(w) = \frac{1}{n} \sum_{i=1}^{n} \left(y'^{(i)} - y^{i}\right) \quad ^{2}$$

Convolutional Neural Networks (CNNs) are a type of deep neural network commonly used for image classification and recognition. Data parallelism and model parallelism are common techniques for training CNNs, with data parallelism being more commonly used. Other distributed protocols include domain and pipeline parallelism, as well as hybrid approaches. In a study on training CNNs, it was proposed to split convolutional and fully-connected layers and apply data and model parallelism, respectively. However, in the quantum setting, the focus is on the differences between data and model distribution.[7]

In the realm of deep learning, the LSTM based RNN algorithm has revolutionized the way we process sequential data. The LSTM model's modules can solve the RNNs long term reliance issues. The fundamental principle behind this algorithm is the cascade LSTM layers that enable the network to process sequential data in a time-stretched manner. At any given iteration t, the RNN model learns input data from the previous iterations, which enhances its ability to analyze time-series data more effectively. The LSTM layer is the core of the RNN model, consisting of LSTM units that enable the network to remember information over long periods of time. The inputs to the LSTM layer include the input data (Xt−1), hidden data (Ht−1), and internal cell state (Ct−1). These inputs are fed through a series of gate structures that allow the network to decide when to accept input information and update the cell state.

The equations governing the LSTM layer are as follows:

$$ft = \sigma\ (Wf\ [Xt\text{-}1, Ht\text{-}1] + bf)$$

$$it = \sigma\ (Wi\ [Xt\text{-}1, Ht\text{-}1] + bi)$$

$$Ct = ft \odot Ct\text{-}1 + it \odot g\ (Wc\ [Xt\text{-}1, Ht\text{-}1] + bc)$$

$$ot = \sigma\ (Wo\ [Xt\text{-}1, Ht\text{-}1] + bo)$$

$$Ht = ot \odot h(Ct)$$

Where ft, it, and ot are the forget, input, and output gates, respectively. σ is the sigmoid activation function, g is the hyperbolic tangent function, and ⊙ is the element-wise multiplication operator. Wf, Wi, Wc, and Wo are the weight matrices, and bf, bi, bc, and bo are the bias terms.[8]

Deep Neural Network (DNN) is a type of machine learning model that relies on deep learning methodologies. This technology has gained significant interest over the years as it has the ability to learn and analyze large amounts of data. DNN is an extension of Artificial Neural Networks (ANN), which is a variation of DNN. Essentially, DNN is a multilayered ANN that exists between input and output layers. These layers are designed to analyze and interpret the data, enabling the network to make predictions based on the information that it has learned. The applications of DNN are vast and varied, ranging from natural language processing to image recognition, and the potential for innovation in this field is virtually limitless. Rectified Linear Unit (ReLu) is an activation function commonly used in neural networks that returns the input value if it is positive, and zero otherwise. The function is required to increase the sensitivity of the activation input in order to avoid fast saturation.[9]

The SoftMax function is commonly used in machine learning as an activation function to convert a vector of real numbers into a probability distribution. For the final layer, we apply the SoftMax activation function. It assigns probabilities to each possible class of the output, ensuring that the sum of probabilities across all classes equals to 1. [10]
The class with the highest probability is the type of flow analyzed.

$$\sigma\ (xi) = \exp\ (x_i)\ \exp\ (x_1) + \exp\ (x_2) + \text{...........................} + \exp\ (x_n)$$

Where: $0 < i < n$, n: the number of output neurons.

Variational quantum classification (VQC) is a quantum machine learning algorithm used for data classification by optimizing parameters with quantum circuits. It can potentially offer faster and more efficient results than classical machine learning for large datasets. VQC is one of the methods with possible quantum advantage in using quantum-enhanced features that are hard to compute by classical methods. Its performance depends on the mapping of classical features into a quantum-enhanced feature space [11].

For a binary classification problem, with input data vectors $\overrightarrow{x_i}$and binary output labels $y_i = \{0,1\}$; for each input data vector, we build a parameterized quantum circuit that outputs the quantum state:

$$|\boldsymbol{\varphi}(\overrightarrow{x_i};\vec{\boldsymbol{\theta}}) = \boldsymbol{U}_{\boldsymbol{w}(\vec{\boldsymbol{\theta}})}\boldsymbol{U}_{\boldsymbol{\phi}(\vec{\boldsymbol{x}}_i)}|\boldsymbol{\theta}$$

Where $\boldsymbol{U}_{\boldsymbol{w}(\vec{\boldsymbol{\theta}})}$ corresponds to the variational circuit unitary and $\boldsymbol{U}_{\boldsymbol{\phi}(\vec{\boldsymbol{x}}_i)}$corresponds to the data encoding circuit unitary.

Image transformers are algorithms that perform transformations on image data, such as dimensionality reduction or feature extraction, to prepare it for analysis or machine learning tasks. These transformations can help improve the efficiency and accuracy of image-based models.

t-SNE: a nonlinear dimensionality reduction technique for visualizing high-dimensional data

UMAP: another nonlinear dimensionality reduction technique for visualizing high-dimensional data

PCA: a linear dimensionality reduction technique for finding the principal components of the data

kPCA(rbf): kernel PCA with radial basis function kernel

kPCA(cosine): kernel PCA with cosine kernel

kPCA(polynomial): kernel PCA with polynomial kernel

PCA (sigmoid): kernel PCA with sigmoid kernel.

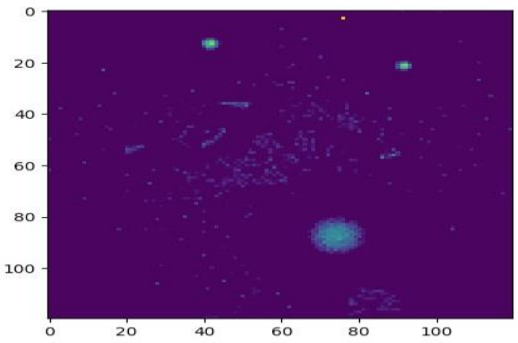


Fig1: dimensionality reducing using UMAP.

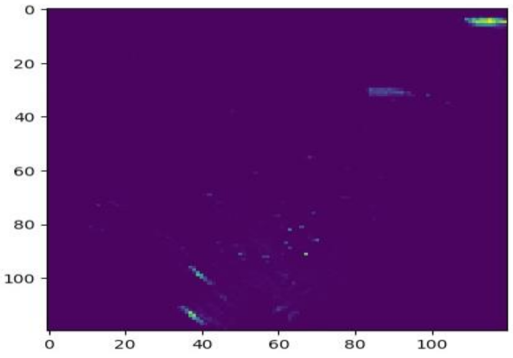
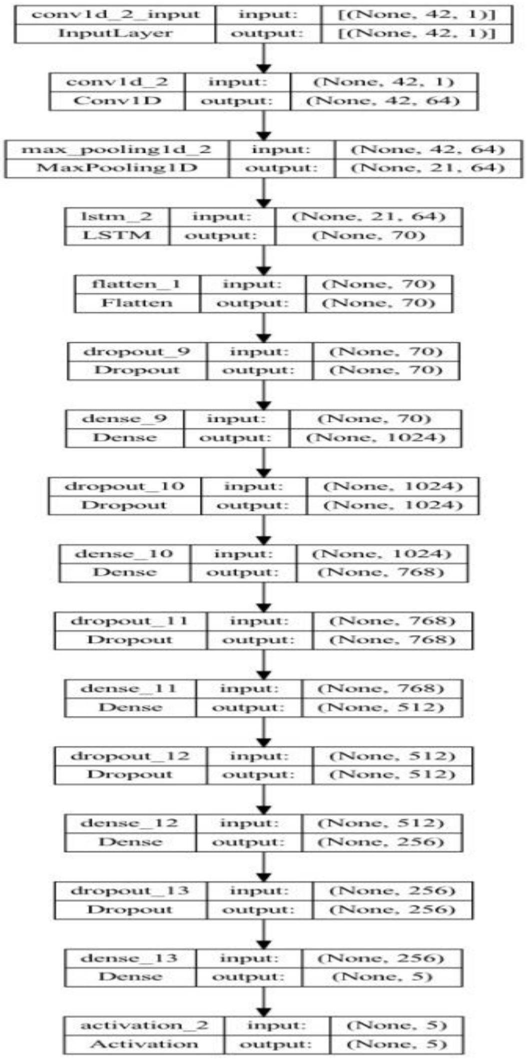


Fig2: dimensionality reducing using kpca-rbf.

A hybrid artificial neural network model has been developed for performing a classification task on time series data with 42-time steps and a single feature. The model combines one layer of Convolutional Neural Network (CNN) for local feature extraction, a Long Short-Term Memory Recurrent Neural Network (LSTM RNN) for analyzing sequential data and a three-layer Deep Neural Network (DNN) for classification and error correction. To explore the potential of using quantum computers as standalone systems for detecting network intrusion in large classical data centers, a Variational Quantum Classifier (VQC) is also implemented.

We use NMF (Non-negative Matrix Factorization) to transform the data into 6 features. Then, it creates a feature map with 6 dimensions and 2 repetitions, and a Variational Form circuit with 6 qubits, 2 repetitions, and 'ry' and 'rz' gates. Finally, an ad-hoc circuit is created by composing the feature map and the Variational Form circuit. This ad-hoc circuit can be used as a quantum classifier for the input data. StandardScaler has been used to preprocess the input data before performing NMF to achieve better results.



conv1d_2_input	input:	[(None, 42, 1)]
InputLayer	output:	[(None, 42, 1)]
conv1d_2	input:	(None, 42, 1)
Conv1D	output:	(None, 42, 64)
max_pooling1d_2	input:	(None, 42, 64)
MaxPooling1D	output:	(None, 21, 64)
lstm_2	input:	(None, 21, 64)
LSTM	output:	(None, 70)
flatten_1	input:	(None, 70)
Flatten	output:	(None, 70)
dropout_9	input:	(None, 70)
Dropout	output:	(None, 70)
dense_9	input:	(None, 70)
Dense	output:	(None, 1024)
dropout_10	input:	(None, 1024)
Dropout	output:	(None, 1024)
dense_10	input:	(None, 1024)
Dense	output:	(None, 768)
dropout_11	input:	(None, 768)
Dropout	output:	(None, 768)
dense_11	input:	(None, 768)
Dense	output:	(None, 512)
dropout_12	input:	(None, 512)
Dropout	output:	(None, 512)
dense_12	input:	(None, 512)
Dense	output:	(None, 256)
dropout_13	input:	(None, 256)
Dropout	output:	(None, 256)
dense_13	input:	(None, 256)
Dense	output:	(None, 5)
activation_2	input:	(None, 5)
Activation	output:	(None, 5)

Fig3: Model Architecture

Fig 3. The model architecture includes a Convolution1D layer with 64 filters of size 3 to extract local features, a MaxPooling1D layer with pool size 2 to reduce dimensionality, an LSTM layer with lstm_output_size set to 70 for processing the output as a sequence and capturing longer-term dependencies in the data. A Flatten layer converts the output of the LSTM layer from a 3D tensor to a 2D tensor. The flattened output is then passed through four Dense layers with ReLu activation function and dropout regularization, each having 1024, 768, 512, and 256 units respectively. Finally, a Dense layer with 5 units and SoftMax activation function produces a probability distribution over the five possible classes. Dropout regularization is used to prevent overfitting. With VQC we receive an accuracy of 60%.

Hybrid Neural Network (HNN), a type of neural network architecture that combines both neural network models and traditional mathematical models to improve performance and accuracy. We have also used HNN where we include Conv1D and LSTM layers along with Dense layers and apply batch normalization and dropout to prevent overfitting. The model is compiled using categorical cross-entropy loss and Adam optimizer with a specific learning rate. We see an accuracy of 79.4%.

4. RESULTS

We run the model for VQC and HNN and plotted the results for both the models. We receive an accuracy of 60% for VQC, whereas the accuracy with HNN has been 79.4%. The classification results are shown below:

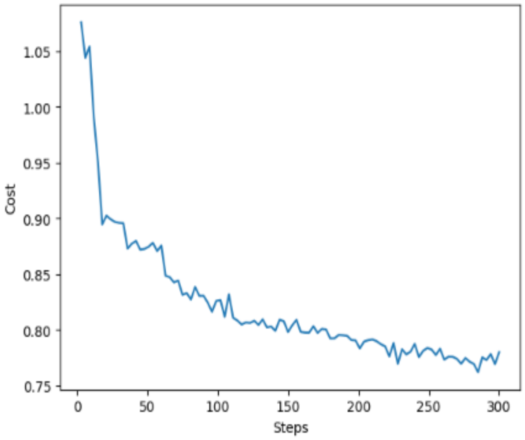


Fig4: VQC Plot for Steps vs the Cost.

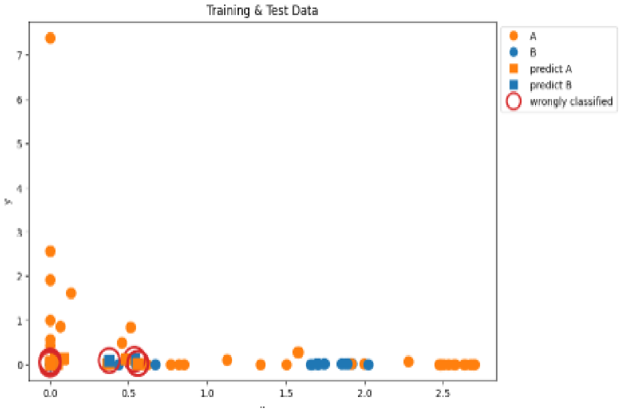


Fig5: VQC Classification Training Model

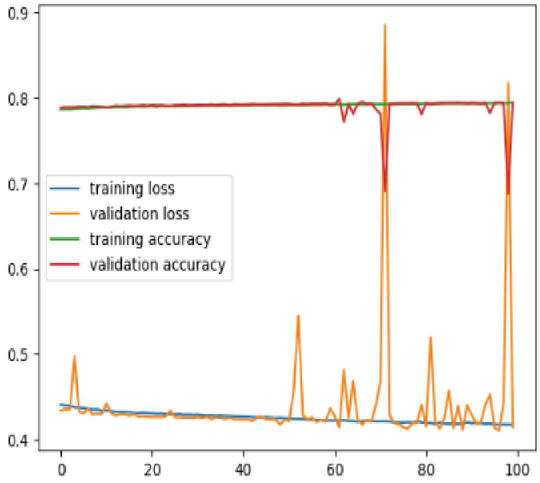


Fig6: HNN Accuracy

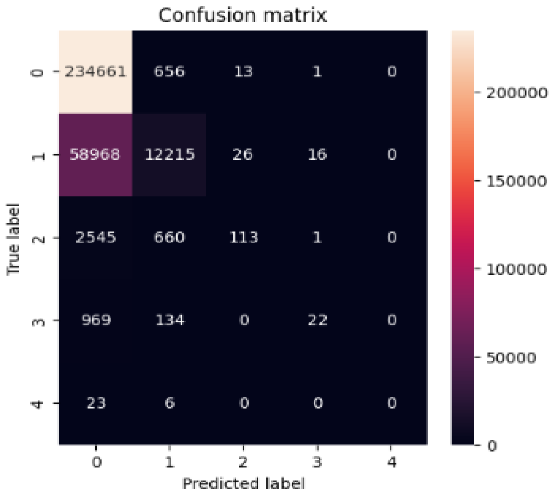


Fig7: HNN Confusion Matrix

CONCLUSION AND FUTURE WORK

Even though the accuracy of VQC is 60% it must be noted that the dataset used was just 100 stratified samples from the NIDS dataset, with a greater number of qubits it can be said that the standalone mode for the NIDS systems using the quantum computers will be much efficient and faster in predicting network intrusions and zero-day attacks. The Hybrid neural network model is very useful in terms of feature extraction and multiclass classification but there is more that must be done. In future models like VTNNs or a hybrid of classical and quantum machine learning algorithms can be tested for better network security.

REFERENCES

[1] Intrusion Detection System in Software – Defined Networks Using Machine Learning and Deep Learning Techniques – A Comprehensive Survey.

[2] DCNNBiLSTM: An Efficient Hybrid Deep Learning – Based Intrusion Detection System.

[3] Deep Learning Approach for Intelligent Intrusion Detection System.

[4] The Cross- Evaluation of Machine Learning – Based Network Intrusion Detection Systems.

[5] Quantum distributed deep learning architectures: Models, discussions, and applications.

[6] Quantum Machine Learning for Network Intrusion Detection Systems, a Systematic Literature Review.

[7] An Invitation to Distributed Quantum Neural Networks.

[8] A Fast and Power Efficient Architecture to Parallelize LSTM based RNN for Cognitive Intelligence Applications

[9] A Feature Selection Based DNN for Intrusion Detection System

[10] Intrusion detection system for SDN network using deep learning approach

[11] Efficient Discrete Feature Encoding for Variational Quantum Classifier

Github link of the project code:
https://github.com/praveen-venkatachalam/NIDS-HNN-VQC