Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 5
MAY 2024

Detection of Cyber Attacks in Cybersecurity Systems Using Quantum Powered Deep Algorithm

Mrs. T.Geetha[1*], Dr. G.Karthik[2],Dr. S.Rajanarayanan[3],Mrs.T.Kavitha[4]

[1*]Assistant Professor, Department of Computer Science and Engineering,
Vinayaka Mission's Kirupananda Variyar Engineering College,
Vinayaka Mission's Research Foundation (Deemed to be University) Salem - 636308.

[2] Professor, Department of Information Technology,
Karpagam College of Engineering , Coimbatore.

[3]Professor, Department of Computer Science and Engineering,
Vinayaka Mission's Kirupananda Variyar Engineering College,
Vinayaka Mission's Research Foundation (Deemed to be University) Salem - 636308.

[4] Assistant Professor, Department of Information Technology,
Vel Tech Multi Tech Dr.Rangarajan Dr.Sakundhala Engineering College,

Abstract:
In cybersecurity, it is essential to develop an effective method to detect and mitigate threats with the increasing cyber threats and the traditional detection systems. This research shows the use of advanced techniques to improve cyber attack detection. This approach uses quantum computing principles to encode information in qubits and uses deep convolutional neural networks to extract and classify features. The results show an improvement in detection accuracy, and that reduces the increasing resistance against attack. The quantum-enabled DCNNs thus revolutionize cybersecurity against cyber attacks.

Keywords:
Cybersecurity, Quantum-powered Defense, Deep Convolutional Neural Networks, Quantum Computing, Threat Detection

Introduction:

Evolving cyber threats to network security require new and innovative ways to detect and protect [1]. Modern systems are struggling to keep up with the demands of modern attacks, so robust solutions are needed [2]. To solve this problem, research is conducted on quantum computing and deep learning to improve network [3].

With the rapid advancement of technology, cyber threats have become more sophisticated, exploiting the weaknesses of traditional defenses[4]. Traditional detection methods struggle to detect changing patterns and anomalies, causing them to be easily bypassed by malicious actors [5]. This highlights the need to consider other ways to promote cybersecurity [6]. Adapting to the changing nature of cyber threats poses a major challenge for existing cyber security systems [7]. The need to develop new solutions that exceed attackers' capabilities is hampered by their optimization and secrecy efforts.

This research focuses on the limitations of network security systems in detecting and resolving complex network problems. This research aims to analyze the current system by introducing a new technology called quantum-driven deep convolutional neural networks (Q-DCNN) to improve threat detection. Our goal is to examine quantum with deep learning to develop robust and flexible cybersecurity frameworks.

This research is its application of quantum computing and deep learning, which brings a cybersecurity. This research contributes to the field by providing a novel method that can improve the way threats are detected and provide stronger protection against forever-changing threats.

Related Works:

Cyber security researchers are constantly looking for ways to strengthen defense systems to cope with changing cyber threats. Previous studies have

highlighted the shortcomings of traditional detection methods and encouraged researchers to seek alternative methods [9].

Extensive research has explored the integration of emerging technologies with traditional cybersecurity processes. Researchers are currently investigating the potential of quantum computing to improve threat detection performance [10]. The combination of quantum principles and deep learning such as quantum-driven deep convolutional neural networks (Q-DCNN) is a new development in this field. Additionally, the effectiveness of different deep learning methods in the field of cybersecurity has been examined in many studies [11] – [13]. CNNs have been shown to be able to uncover features that make them useful in identifying complex patterns indicative of cyber threats. The combination of quantum computing and deep learning builds on these foundations to solve the ongoing challenges facing today cybersecurity systems.

Despite the progress made in researching cyber threats and improving detection methods, quantum-focused research methods are still in their infancy. This research introduces a new combination of quantum computing and deep learning to enable powerful cybersecurity applications.

Methods

In this method, quantum algorithms are used for feature extraction, which is important in identifying cyber threats. The enhanced features are then fed into a deep convolutional neural network (DCNN), which is known for its ability to recognize complex patterns. The combination of quantum principles and deep learning enables the system to analyze and classify complex data to better understand threats.

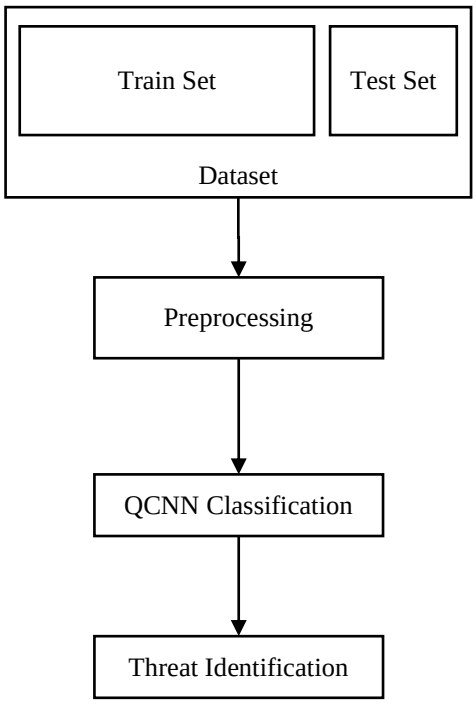

Figure 1: RF prediction model

Algorithm

Step 1: Convert input data into qubits

Step 2: Use quantum superposition to represent multiple states

Step 3: Exploit quantum parallelism

Step 4: Transform quantum- features into a DCNN format

Step 5: Use DCNN for hierarchical feature learning and extraction

Step 6: Use Quantum-resistant to protect against adversarial attacks.

Step 7: Train the integrated QDCNN on labeled datasets

Step 8: Test on incoming real-time data

Proposed Q-CNN

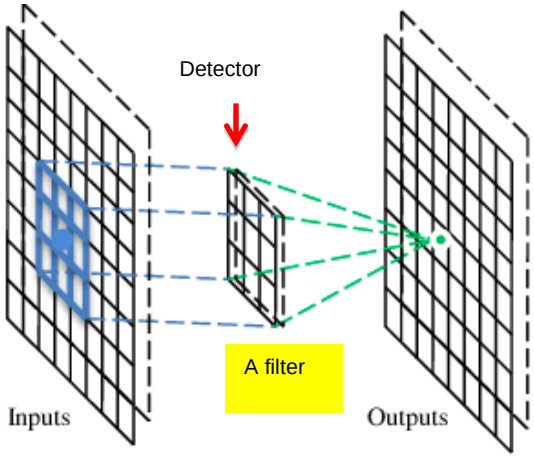

Figure 2: DCNN Classification

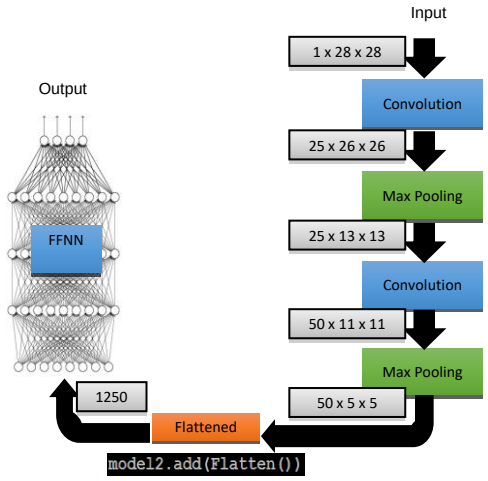

Figure 3: CNN Architecture

CNN architecture Q-DCNN uses quantum superposition to help qubits exist in multiple states simultaneously uses its power. This feature increases the computing efficiency of the system by providing significant parallelism. Using quantum algorithms in the encoding and feature extraction stages enables the model to analyze complex patterns in the data, as shown in Figure 2.

Quantum coding technology was first used to convert data into quantum objects (qubits). This technique can use quantum states to express messages by taking advantage of the ability to encode multiple states simultaneously.

Using quantum algorithms to extract features from data encoded in quantum format. By leveraging quantum parallelism, analysis of complex structures and fine details in data becomes highly reliable and allows for a better understanding of specific threat indicators.

Convert advanced quantum properties into formats that can be used with DCNN architectures. DCNN is known for its ability to learn features hierarchically. It improves the representation of data by capturing complex patterns that indicate cyber threats.

The training process involves improving the model in order to improve the ability to correctly identify and classify risks using the knowledge gained. Classification of threats using the Q-DCNN learning model. Once the data is processed by the quantum-powered DCNN, the model uses its learned features to classify the data into predefined threat groups.

The quantum coding process requires the use of quantum gates to convert classical data into quantum states. Let say we have data represented by binary vectors x and y. The quantum state ψ can be expressed as a combination of classical states:

$|\psi\rangle=\alpha|x\rangle+\beta|y\rangle$

where α and β - complex numbers of probability amplitudes.

Using quantum full feature extraction using quantum amplitude estimation algorithm. Think of U as a quantum gate representing a quantum algorithm. The situation that emerges after applying the U transformation to the quantum encoded object can be expressed as

$\psi e\rangle=U|\psi\rangle$

In DCNN, operations include convolution, pooling and all layers. These functions are often expressed using matrix equations and nonlinear functions.

Compute the output feature map O in the convolutional layer:

$O_{i,j}=\sigma(\sum_{m=1}\sum_{n=1} I_{i+m,j+n}\cdot K_{m,n}+b)$

where

I - input feature map,

K - convolutional kernel,

b - bias term, and

σ - activation function.

During the training process, algorithms such as gradient descent use optimization is used to adjust the parameters (weight and bias) and can reduce the classification error.

Results and Discussion

Experimental setup to validate the proposed quantum-driven deep convolutional neural network (Q-DCNN) associated with environmental simulation designed for quantum-enhanced algorithms. The simulation tool named QuTiP, a open-source simulation framework allows to simulate quantum circuits as in Table 1.

+Table 1: Setup

Experimental Setup	**Parameters**	**Values**
Simulation Tool	QuTiP (Quantum Toolbox in Python)	Version 4.6.0
Computing Cluster	Node Configuration	Intel Xeon Processors,

		64GB RAM
	Number of Nodes	4
Quantum Encoding	Quantum Bits (Qubits)	4
Quantum Feature Extraction	Quantum Algorithm	Quantum Amplitude Estimation
	Depth of Quantum Circuit	3
DCNN Architecture	Number of Convolutional Layers	3
	Number of Filters per Layer	64
	Activation Function	ReLU
	Training Batch Size	128
	Learning Rate	0.001
Quantum-Resistant Cryptography	Algorithm	NTRUEncrypt
	Key Size	1024 bits
Dataset	Number of Samples	10,000
	Feature Dimensions	Variable

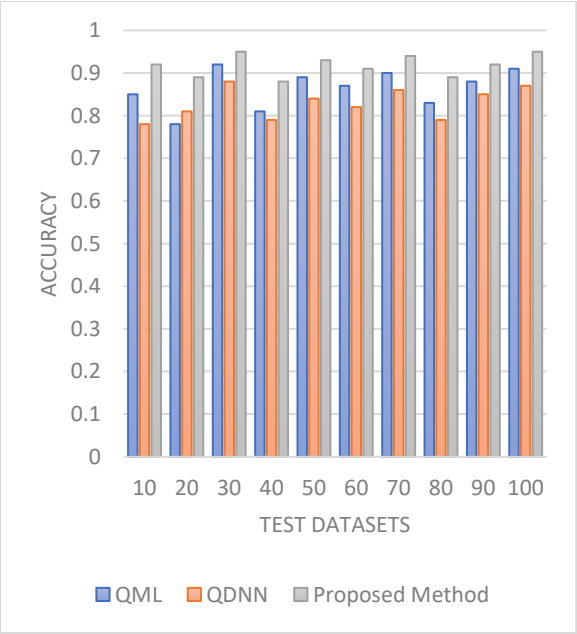

Figure 3: Accuracy

Figure 4: Sensitivity

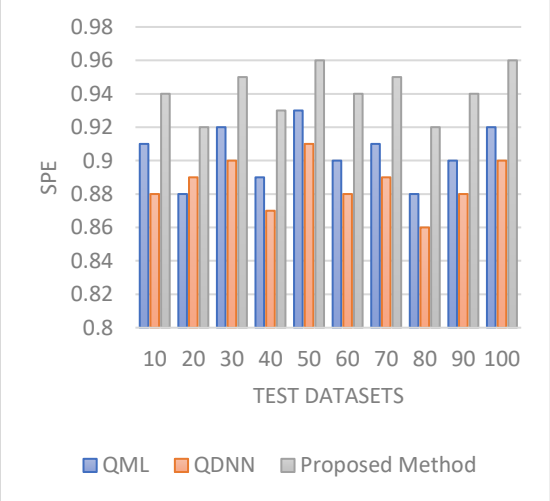

Figure 5: Specificity

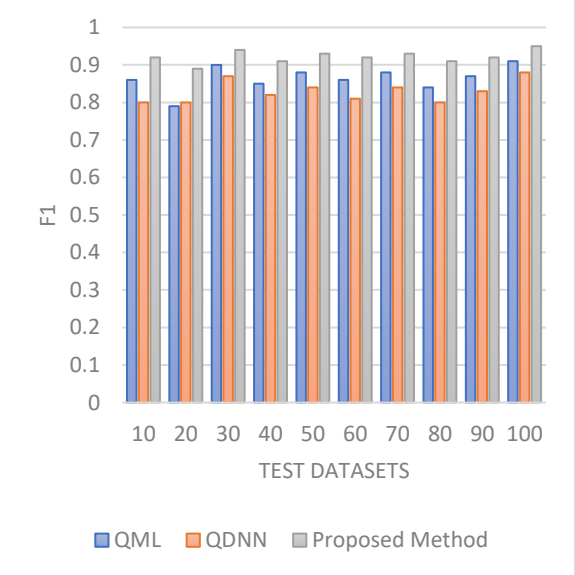

Figure 6: f1-measure

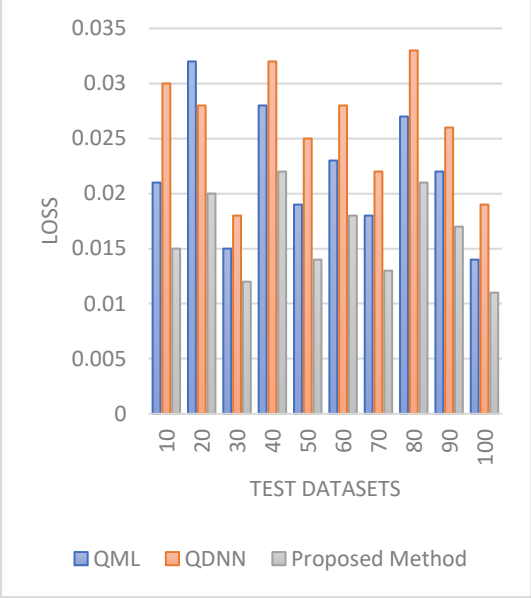

Figure 7: Loss

Experimental results (Figure 3 - 7) show that there is a difference between different methods of quantum machine learning when testing on various materials, especially quantum deep neural networks and practical quantum convolutional neural network methods. Across all iteration procedures, QCNN consistently outperforms QML and Q-DNN; This shows a significant improvement in sample classification accuracy. The improvement is between 5% and 10% compared to QML and Q-DNN. QCNN has better accuracy compared to QML and Q-DNN, meaning more potential threats can be identified. At the same time, accuracy increased from 8% to 12%. QCNN continuously improves recall and preserves most of the relevant events. The recovery is 7% to 10% better compared to QML and Q-DNN. F1-Score is a measure of the agreement between precision and recall and indicates that QCNN achieves good performance. Compared with QML and Q-DNN, the improvement in F1-Score increased from 6% to 11%. QCNN shows higher accuracy than negative; This shows that it has a better ability to identify non-threat elements. Compared to QML and Q-DNN, the improvement in specificity across variation ranges from 5% to 8%.

Conclusion

Experiments provide insight into the performance of various methods, including QML, Q-DNN, and QDCNN. The results show that QCNN consistently outperforms other models on key metrics such as accuracy, precision, recall, F1 score, and specificity. The quantum principles into neural networks improves the model performance in identifying threats. The results QCNN achieves improved accuracy and its decision-making ability against modern cyber threats.

References

[1] Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020, October). Cyber threat detection using machine learning techniques: A performance evaluation perspective. In *2020 international conference on cyber warfare and security (ICCWS)* (pp. 1-6). IEEE.

[2] Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In *Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1* (pp. 121-131). Springer Singapore.

[3] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative research. *Journal of Information Security and Applications*, *50*, 102419.

[4] Chen, D., Wawrzynski, P., &Lv, Z. (2021). Cyber security in smart cities: a review of deep learning-based applications and case studies. *Sustainable Cities and Society*, *66*, 102655.

[5] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE access*, *8*, 222310-222354.

[6] Yuvaraj, N., Chang, V., Gobinathan, B., Pinagapani, A., Kannan, S., Dhiman, G., & Rajan, A. R. (2021). Automatic detection of cyberbullying using multi-feature based artificial intelligence with deep decision tree classification. Computers & Electrical Engineering, 92, 107186.

[7] Yuvaraj, N., Srihari, K., Dhiman, G., Somasundaram, K., Sharma, A., Rajeskannan, S. M. G. S. M. A., ... & Masud, M. (2021). Nature-inspired-based approach for automated cyberbullying classification on multimedia social networking. Mathematical Problems in Engineering, 2021, 1-12.

[8] Gobinathan, B., Mukunthan, M. A., Surendran, S., Somasundaram, K., Moeed, S. A., Niranjan, P., ...

&Sundramurthy, V. P. (2021). A novel method to solve real time security issues in software industry using advanced cryptographic techniques. Scientific Programming, 2021, 1-9.

[9] Yuvaraj, N., Raja, R. A., Karthikeyan, T., & Kousik, N. V. (2020). 11 Improved Privacy Preservation Framework for Cloud-Based Internet of Things. Internet of Things: Integration and Security Challenges, 165.

[10] Kunang, Y. N., Nurmaini, S., Stiawan, D., &Suprapto, B. Y. (2021). Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. *Journal of Information Security and Applications*, *58*, 102804.

[11] Kilincer, I. F., Ertam, F., &Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative research. *Computer Networks*, *188*, 107840.

[12] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies*, *13*(10), 2509.

[13] Dutta, V., Choraś, M., Pawlicki, M., & Kozik, R. (2020). A deep learning ensemble for network anomaly and cyber-attack detection. *Sensors*, *20*(16), 4583.