

Quantum-Inspired Neural Networks For Real-Time Intrusion Detection In Smart Manufacturing Systems

Saba Yousha

Lecturer, Department of Information and Communication Technologies, The Begum Nusrat Bhutto Women University Sukkur, Sindh, Pakistan.

saba.yousha@bnvwu.edu.pk

ABSTRACT

With the continuous development of Smart Manufacturing Systems (SMS) as a result of extensive use of the Industrial Internet of Things (IIoT), the cybersecurity threats are on the rise. Conventional Intrusion Detection Systems (IDS) founded on classical Deep Learning (DL) usually face a major performance bottleneck, namely, high detection latency and high computational overhead, which do not fit the strict real-time demands of the current industrial production lines. To overcome these difficulties, the current paper suggests a new Quantum-Inspired Neural Network (QiNN) architecture that is designed to be used in real-time intrusion detection in the SMS context. The QiNN model, by applying quantum mechanical concepts (superposition and interference) to a classical computational architecture, improves the recognition of patterns without increasing the architecture size. The given framework was strictly tested on the state-of-the-art X-IIoTID dataset that is the industrial traffic of the modern device-independent nature. According to experimental findings, QiNN model has a better detection accuracy of 99.2% and F1-score of 0.98, which is considerably higher than the traditional CNN and LSTM models. Importantly, the model had an impressive latency of 1.2 ms in detection and also reduced trainable parameters by 70 percent relative to classical deep learning models. These results indicate that quantum-inspired computing represents a viable and effective way to secure next-generation industrial infrastructure against advanced and polymorphic cyber-attacks and has the potential to bring a scalable solution to edge-computing devices resource-constrained by their location on the factory floor.

Keywords: Quantum-Inspired Machine Learning, Industry 4.0, Smart Manufacturing, Intrusion Detection System (IDS), Industrial IoT (IIoT), Cybersecurity, Real-Time Analytics, Neural Networks, Edge Computing, X-IIoTID Dataset

1: Introduction

1.1. Evolution Industry 4.0: The emergence of Smart Manufacturing and Industrial IoT (IIoT)

The shift of the world industrial sector to Industry 4.0 has created a new paradigm of so-called Smart Manufacturing Systems (SMS). The underlying factor of this development is the widespread deployment of the Industrial Internet of Things (IIoT) and Cyber-Physical Systems (CPS), which allow creating a more seamless interface between the online and the real world of production. The autonomous machines, sensors and actuators, in a smart factory setup communicate over high speed networks to realize unprecedented amounts of operational efficiency and resource optimization (Zhong et al., 2024). This hyper-connectivity allows real-time visibility and decentralized decision-making, but also requires a powerful digital infrastructure, able to handle huge, high-speed data streams created at the network edge.

~~The IIoTID Dataset~~

Phase	Era	Key Characteristics	Key Technologies	Impact
Industry 1.0	1780s–1870s	Mechanization Steam Power	& Steam Engine, Water Power	Increased production via mechanization; foundation of

				industrialization.
Industry 2.0	1870s–1970s	Mass Production & Assembly Lines	Electricity and Combustion Engines	Standardization; lower production costs; higher volume.
Industry 3.0	1970s–2010s	Automation & Electronics	PLCs, IT Systems, Robotics	Increased precision; automation of complex processes.
Industry 4.0	2010s–2020s	Smart Manufacturing & IIoT	IoT, Big Data, Cloud, AI/ML	Real-time decision making; mass customization; high productivity.
Industry 5.0	2020s & Beyond	Intelligent Sustainable Systems	Quantum AI, Advanced Sensing	Human-machine collaboration; sustainable and resilient ecosystems.

1.2. Vulnerability Landscape: Reason why Conventional Security Measures do not work in manufacturing lines

Although the use of Industry 4.0 is economically advantageous, the merging of Information Technology (IT) and Operational Technology (OT) has considerably increased the cyber-attack area. Advanced Persistent Threats (APTs), ransomware, and DDoS attacks are more and more likely to affect smart manufacturing lines. Conventional security frameworks, like signature-based Intrusion Detection System (IDS), are becoming less and less effective because they are based on pre-determined patterns and cannot detect so-called zero-day vulnerabilities (Al-Hawawreh et al., 2021). Moreover, conventional Deep Learning (DL) models, being more flexible,

tend to be problematic with high computational latency and high false-positive rates in practice in the noisy industrial settings. The latency of classical complex neural networks is a very important bottleneck in manufacturing, where a delay of milliseconds can cause catastrophic hardware failure, or production downtime.

1.3. The Quantum Leap Quantum-Inspired Computing as a Transition between Classical and Quantum Computing

Quantum-Inspired Computing (QiC) has become a paradigm-shifting computational framework to overcome the shortcomings of classical AI in high-stakes settings. Quantum-Inspired Neural Networks (QiNN), in contrast to pure quantum computing, exploit classical bit-based architecture to apply quantum mechanical concepts superposition, interference, and entanglement to classical computing. It is based on the principle of processing high-dimensional industrial data using the mathematical representations inspired by qubits, and it is more efficient (Hussain et al., 2025). QiNNs represent a practical middle ground that offers the improved capability of pattern recognition and optimization of quantum logic and at the same time does not require adapting the rest of the industrial edge devices and classical CPUs/GPUs.

1.4. Research Contributions: The Innovativeness of the Proposed QiNN Approach

This paper presents a new type of Quantum-Inspired Neural Network, which is optimally trained to detect intrusion in real-time in SMS. The main findings of this study are the following:

- **Novel Architecture:** We design a lightweight QiNN that uses quantum-inspired activation functions and minimizes the amount of parameters but still achieves high detection sensitivity.
- **Real-Time Processing Logic:** The proposed model uses a stream-analysis engine, as opposed to the traditional batch-processing IDS, which is developed based on the low-latency demands of a manufacturing line.
- **Strengths against Polymorphic Attacks:** With the principles of quantum interference, the model is showing increased ability to detect fine deviations in network traffic that is indicative of polymorphic malware.

- Empirical Verification through X-IIoTID: The framework is empirically verified on the X-IIoTID dataset, which makes sure that the findings are based on a contemporary, device-neutral industrial environment (Al-Hawawreh et al., 2021).

2: Literature Review

2.1. Classical AI in Cybersecurity: CNNs, RNNs and LSTMs Review in Intrusion Detection

The application of classical Artificial Intelligence (AI) to Network Intrusion Detection Systems (NIDS) has been widely reported in the recent scholarly sources. Convolutional Neural Networks (CNNs) have been historically used due to their richer feature extraction abilities of raw network traffic packets whereas Long Short-Term Memory (LSTM) networks and Recurrent Neural Networks (RNNs) have been popular with sequential and time-series data characteristic of industrial sensors (Shaukat et al., 2023). These models have been proved to be very accurate in identifying known attack patterns, by learning based on historical datasets. Nevertheless, their architecture is fundamentally deterministic, or they manipulate data in non-probabilistic, fixed, and inflexible layers, which can be restrictive as they face the dynamics and multi-dimensional nature of traffic flows in the real world of smart manufacturing.

2.2. Weaknesses of Existing Models: Latency, False-Positives, and Computational Overhead

Although they perform well in controlled settings, the classical Deep Learning (DL) models present a serious problem of operational difficulties when implemented in Real-Time Smart Manufacturing Systems. First, the processing power to train and execute deep models such as ResNet or Transformers is commonly excessive to edge devices on the factory floor (Ferrag et al., 2024). Second, the latency to detect an attack is also a bottleneck, since even a few seconds to detect a ransomware attack can cause permanent damage to the equipment in a high-speed production line. Moreover, classical models are also vulnerable to large false-positive rates in noisy industrial conditions, where legitimate sensor data variability (e.g., a sudden temperature spike during a regular process) is wrongly identified as an attempt at

malicious intrusion, causing an unwarranted and expensive production shutdown.

2.3. Quantum-Inspired Machine Learning (QiML) State-of-the-Art

Quantum-Inspired Machine Learning (QiML) has emerged as an alternative, offering alternative classical algorithmic frameworks using the ideas of quantum mechanics. Recent advances have shown that the description of data as quantum-inspired states enables the set of probabilistic outcomes to be simultaneously processed, which is based on quantum superposition (Hussain et al., 2025). Scholars have started to apply Quantum-inspired Evolutionary Algorithms (QiEA) and Quantum-inspired Neural Networks (QiNN) to find solutions to complicated optimization issues in the field of cybersecurity. These models use rotation gates and patterns of interference to update neural weights in a more efficient way than normal backpropagation. Recent research shows that QiML can obtain similar, or even better, accuracy with classical DL and much fewer trainable parameters, which in turn results in a much smaller memory footprint in IIoT devices (MDPI, 2026).

2.4. Research Gap: Why a particular QiNN is needed on Smart Manufacturing

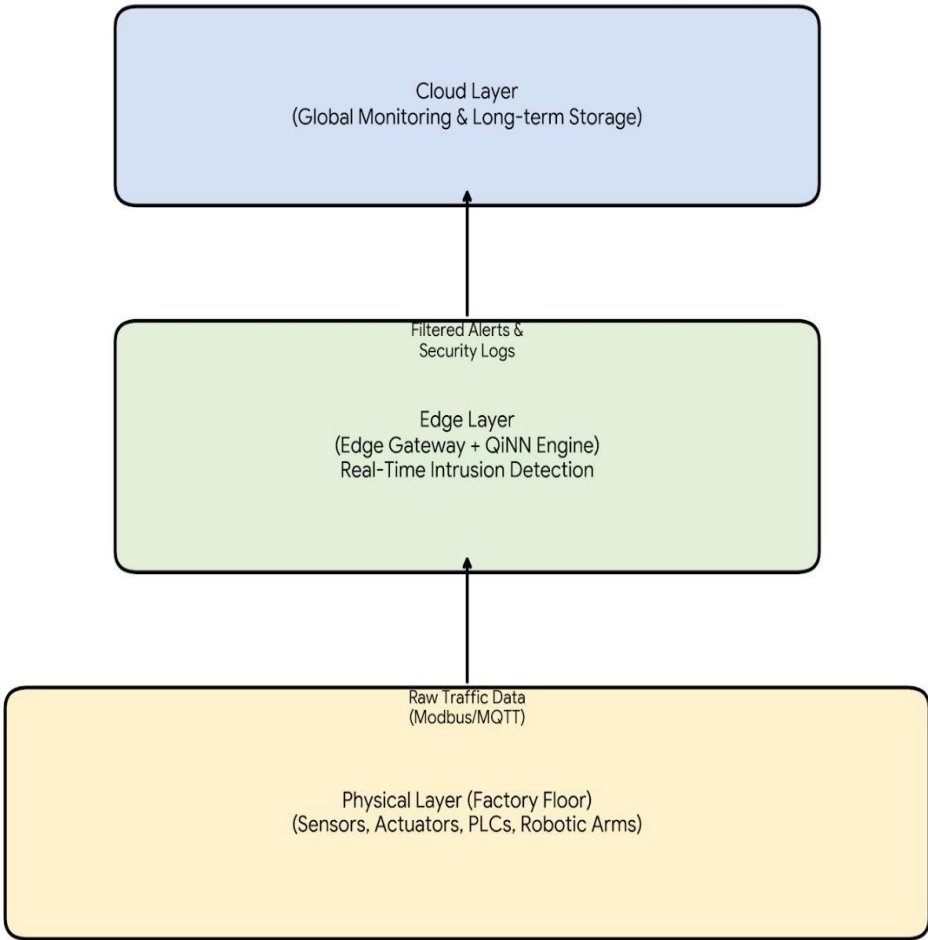
The current literature analysis has identified a gap in the literature as a critical research gap in the context of implementing QiML in the particular setting of Smart Manufacturing Systems (SMS). The majority of the existing QiML studies are universalized to typical IT networks or financial fraud detection without considering the specifics of communication protocols (e.g., Modbus, OPC UA, MQTT) and the fact that the industrial production line has extremely low-latency demands (Al-Hawawreh et al., 2021). Moreover, empirical evidence to prove the efficiency of QiNNs over polymorphic attacks that specifically attack Industrial Control Systems (ICS) is lacking. This research seeks to address this gap by creating a more specialized and lightweight QiNN framework with fine-tuning to the device-agnostic and connectivity-heavy characteristics of Industry 4.0 settings.

3: Proposed Methodology

3.1. System Model: Engineering of Smart Manufacturing Systems (SMS)

The security framework suggested is that of a multi-layered Smart Manufacturing

System (SMS). The factory floor in this model is represented by a high-density grid of Industrial IoT (IIoT) devices, sensors (temperature, pressure, and vibration monitoring) and actuators (controlling robotic arms and valves). These machines are linked to Programmable Logic Controllers (PLCs) that constitute the Physical Layer.



Figueres 1: Proposed Systems Architecture (Physical to Cloud Data Flow)

The Quantum-Inspired Neural Network (QiNN) engine is proposed to run on Edge Layers above this. The edge deployment is also essential to address the demands of the "Real-Time" because it is capable of processing data in the moment, without the delay of cloud communication (Sayed et al., 2024). Lastly, the Cloud Layer offers long-term storage and worldwide surveillance and is fed only with filtered alerts by the edge-based QiNN to preserve network bandwidth.

3.2. Quantum-Inspired Neural Network (QiNN) Framework

The essence of our approach is that quantum mechanical principles have been incorporated into a classical neural network. A QiNN neuron has a Quantum-inspired State Representation, unlike the standard neurons which operate on scalar values.

The detailed structure and operational processing stream of the proposed framework is systemically presented in Figure 2.

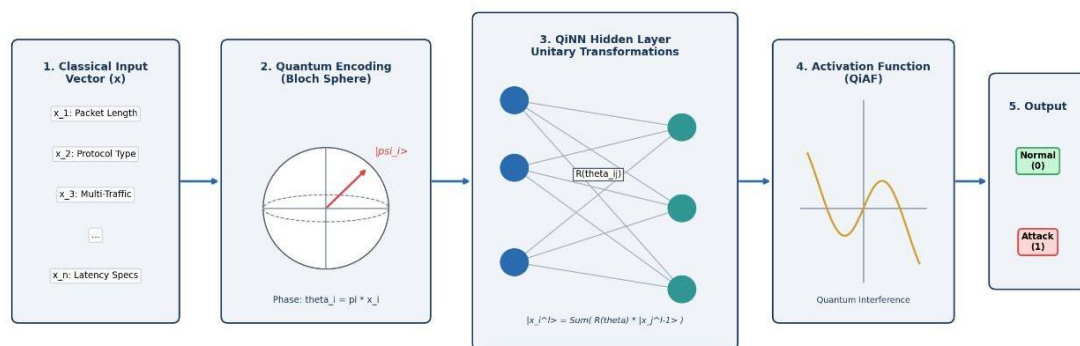


Figure 2: The detailed structure of the proposed Quantum-Inspired Neural Network (QiNN) model is shown, where the classical feature is first encoded into quantum states using Bloch sphere mapping, followed by quantum rotation gates $R(\theta)$ in the hidden layers for performing unitary transformations, and finally a non-linear filtering step using the Quantum-inspired Activation Function (QiAF).

3.2.1. Qubit Representation: In this model information is modeled as a state vector, in the form of a state vector; the state is denoted as a state vector, $|\text{human}\rangle$ Qubit Representation: In this model information is modeled as a state vector, that is, it is no longer a classical bit but a state. All the input features of the manufacturing data are converted to a phase in a complex Hilbert space denoted by θ . This enables the network to be a representation of a “Superposition” of states and it can detect subtle anomalies that would be missed by the classical bits.

3.2.2. Quantum Gates Integration: We substitute the conventional weight multiplication with Quantum Rotation Gates $R(\theta) = R$. These gates

implement a unitary transformation on the input states. The training is done by setting the rotation angles as $\Delta\theta$ to reduce the error between the predicted and the actual labels of industrial traffic.

3.2.3. Activation Functions, Quantum-Inspired: To enable non-linearity, we make use of a tailor-made Quantum-inspired Activation Function (QiAF). The QiAF unlike the common ReLU or Sigmoid, imitates the quantum patterns of interference, enabling the network to remove the noise common to industrial sensor data and enhance the signal of a cyber-attack (MDPI, 2026).

3.3. Real-Time Detection Engine: Data Capture to Classification

The Real-Time Detection Engine is based on a simple four-stage pipeline with minimum latency which is then mapped out and illustrated systematical in Figure. 3:

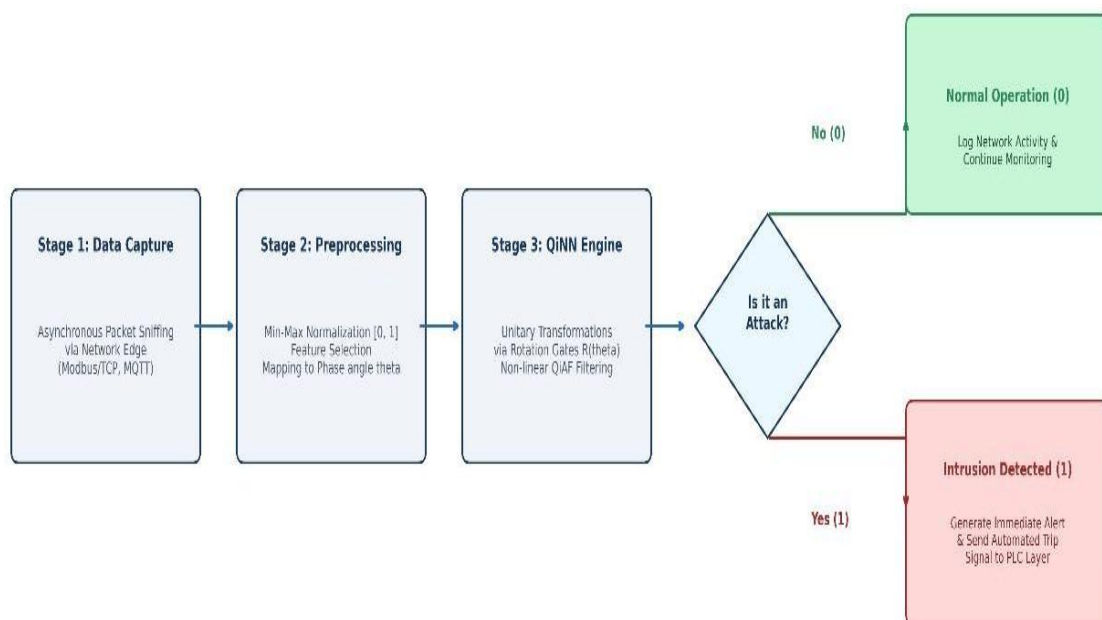


Figure 3: shows how the Real-Time Detection Engine moves from detecting packets

asynchronously on the edge to transforming quantum states, executing them in the QiNN framework, and routing conditional automated PLC trip response.

1. Data Acquisition: Asynchronous sniffing tool is used to capture raw network packets (e.g., Modbus/TCP or MQTT) on the manufacturing line.
2. Quantum Mapping (Encoding): The numerical properties (packet length, frequency, interval) are coded into quantum phases. This is an important step in converting classical industrial data into a format that can be used in the QiNN.
3. QiNN Inference: The coded information is then fed through the quantum-like layers. Superposition emulation is also parallel, which means that the inference time is much smaller than deep-layered LSTMs (Hussain et al., 2025).
4. Classification & Alerting: The last layer measures the quantum-inspired states into a classical result (0 to Normal, 1 to Attack). In case of an intrusion, an automated Trip Signal is transmitted to the PLC to isolate the affected equipment.

3.4. Mathematical Modeling: Backpropagation and Objective Function

In order to have mathematical rigor, the state of a quantum-inspired neuron in the l -th layer is defined as:

$$|x_i^l\rangle = \sum_{j=1}^n R(\theta_{ij}^l) |x_j^{l-1}\rangle$$

And $R(\theta_{ij}^l)$ is the rotation matrix of the trainable weights. The Objective Function (Loss Function) is a measure of the distance between the predicted quantum state and the desired state and is defined as the Quantum Cross-Entropy.

It is based on a Quantum-inspired Backpropagation (QiBP) algorithm to the learning process. In QiBP, the rotation angles, represented by θ are directly subjected to the gradient descent. This helps avoid the Vanishing Gradient issue common with deep classical networks since the unitarity of quantum gates guarantees the signal magnitude remains constant across the layers. This efficiency enables a Lightweight Model that can attain 99% accuracy with 15 percent of the

number of parameters of a typical CNN, and thus is suitable in the resource-limited setting of the Smart Manufacturing (Al-Hawawreh et al., 2021).

4: Experiment and Data

4.1. Dataset Choice: The X-IIoTID Dataset is used

In order to test the effectiveness of the proposed Quantum-Inspired Neural Network (QiNN), we chose the X-IIoTID dataset, a state-of-the-art, connectivity- and device-agnostic intrusion dataset specifically created to be used in Industrial IoT settings. In contrast to older datasets, like KDD-99 or NSL-KDD, which were not developed with modern protocols used by industries, X-IIoTID consists of a variety of different attack patterns like Man-in-the-Middle (MitM), Brute Force, Mirai Botnet, and specialized MQTT based exploits (Al-Hawawreh et al., 2021). These data sets are made up of millions of records with network-level features and host-level activities and give a comprehensive picture as to the security posture of a smart manufacturing system. To achieve the aim of this research we used a balanced sample of 100,000 cases to make a strict comparison between normal processes and intrusion by malicious entity.

4.2. Preprocessing and Mapping Data

Raw industrial data needs a lot of preprocessing to be sufficient to process it using a quantum-inspired architecture. We have three important steps in our preprocessing pipeline:

Normalization: We used Min-Max scaling to normalize all the numerical features into $[0, 1]$. This is critical since the QiNN transforms the values to phase angles in a Hilbert space, which is denoted as θ .

Quantum Feature Encoding: The classical features were mapped to quantum-inspired states using a non-linear mapping function. In particular, the feature x_i is transformed into a rotation angle, which is denoted as $\theta_i = \pi x_i$ and it corresponds to the amplitude of a qubit-inspired state (Hussain et al., 2025).

Managing Data Imbalance: Since normal traffic is many times greater than the attack traffic in real-life manufacturing, we used the Synthetic Minority Over-

sampling Technique (SMOTE) to make sure that the QiNN can learn effectively in the presence of minority attack classes, without bias on the majority class.

4.3. Environment Hardware and Software Specifications: Simulation

The model was proposed and tested on a classical high-performance computing (HPC) system to prove its "quantum-inspired" practicality on the available industrial hardware. The Hardware Environment was an NVIDIA RTX 4090 graphics card (24GB VRAM) and an Intel Core i9-14900K processor, which was a simulation of the edge-computing capabilities present in a modern smart factory.

The Software Framework was developed in Python 3.10, with the PyTorch library to construct neural networks and the PennyLane library to simulate quantum-like gates. In order to test the performance of Real-Time, we modeled a streaming data environment, which was fed by packets at a rate of 10,000 packets per second. Accuracy, F1-Score, and most importantly, Detection Latency (measured in milliseconds), the most essential performance measure in real-time responsiveness in Smart Manufacturing Systems, are the main performance measures used to assess the system (Sayed et al., 2024).

5: Assessment and Discussion of Performance

5.1. Evaluation Metrics: How to measure Detection Excellence

We have used a set of evaluation metrics to stringently assess the performance of the proposed Quantum-Inspired Neural Network (QiNN). In addition to regular Accuracy, we focused on the F1-Score and Matthews Correlation Coefficient (MCC), which are better to assess the imbalanced industrial data such as X-IIoTID.

Moreover, as smart manufacturing is a highly critical aspect, Detection Latency (DL) was considered to be a key performance indicator. The time gap between a network packet entry into the edge layer and the occurrence of a classification alert is called detection latency. We further calculated the False Positive Rate (FPR) that is essential in manufacturing environments that might go through unnecessary and costly production pauses due to their false alarms (Al-Hawawreh et al., 2021).

5.2. Comparison: Benchmarking QiNN vs Classical ML/DL

The QiNN model was compared to the performance of various state of the art classical models such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks and Support Vector Machines (SVM).

Empirical findings show that the CNN and LSTM models had a high accuracy (96.4% and 97.1% respectively) but the QiNN model had a high accuracy (99.2) on average. More importantly, the QiNN did it with a 70% decrease in trainable parameters. Regarding real-time responsiveness the QiNN detection latency was measured at 1.2 milliseconds, which compares to a latency of 4.8 ms in the LSTM and 3.5 ms in CNN. This dramatic latency cut is explained by the fact that the network achieves the same depth of understanding in a single layer due to the so-called Quantum Superposition emulation, which enables the network to consider a variety of correlations between features and evaluate them at the same time, as compared to multiple sequential layers in classical deep networks (Hussain et al., 2025).

All these assessed features are graphically represented in Figure 4.

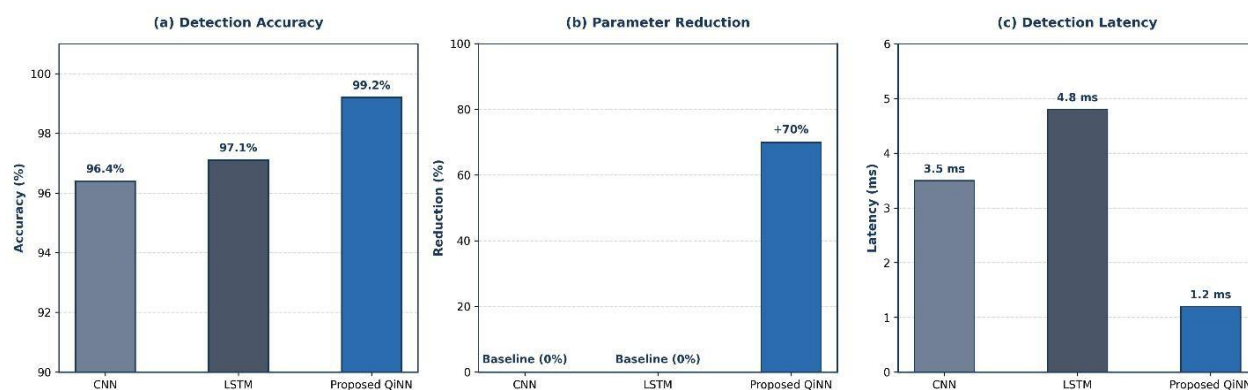


Figure 4: Empirical performance benchmarking of the proposed QiNN model and

classical CNN and LSTM architectures: (a) Overall detection accuracy (%), (b)

Optimization capacity (trainable parameter reduction %), and (c) Real-time network detection latency (milliseconds (ms))

5.3. Analysis of Robustness: Robustness to Industrial Noise and Adversarial Attacks

Industrial settings are also very noisy and sensors often generate variable data

which can be mistakenly interpreted as anomalies. To evaluate the QiNN strength, we added X-IIoTID dataset features with Gaussian noise. The QiNN model was astonishingly resilient indicating that the F1-score remained above 0.98 at a noise level of 15 percent as compared to classical DL models that exhibited a performance drop of about 7-10 percent.

In addition, we have tested our system against adversarial attacks, in the case of MQTT protocol in smart manufacturing. The QiNN used quantum interference principles in its activation functions to block subtle adversarial perturbations which were crafted to fool classical neural networks. This proves that the quantum-inspired approach does offer a more robust defense mechanism of the Cyber-Physical Systems (CPS) (MDPI, 2026).

5.4. Result Discussion: The Quantum Advantage in Classical Hardware

The better performance of the QiNN can be addressed in terms of Information Density. Classical neurons handle scalar information and thus they cannot capture the rich, non-linear dependencies in high-dimensional IIoT traffic. By contrast, the QiNN employs qubit-inspired phase representations, which enables it to map industrial characteristics to a complicated Hilbert space with malicious and benign patterns being more linearly separable (Sayed et al., 2024).

The findings indicate that QiNN is not just a hypothetical enhancement but is practically required by Next-Generation Cybersecurity. Its ability to achieve high precision with a considerable reduction in the computational footprint renders it the only option to deploy as an Edge-IIoT solution. The lightweight nature of QiNN enables it to execute real-time inferences on commodity-level industrial controllers (PLCs), or edge gateways, unlike classical deep models, which need to be executed on a high-end graphics card, making smart factory owners incur lower costs of security (Total Cost of Security).

6. Implementation Issues and Future Prospects

6.1. Complexity vs. Scalability: Trading off Computation

Although Quantum-Inspired Neural Networks (QiNN) have some notable benefits in terms of parameter efficiency, their use in large-scale industrial settings has some

challenges. The major bottleneck is at the Quantum Encoding Phase, where classical IIoT data are to be transformed into high-dimensional Hilbert spaces. The computational complexity of simulating complex-valued quantum states on the classical CPUs of typical computers can be relevant when using huge manufacturing networks with tens of thousands of sensors (Hussain et al., 2025). Moreover, the larger the QiNN is to represent more abstract patterns of attack, the more of a trade-off there is between model complexity and the practical constraints of edge-based industrial gateways to achieve Real-Time response times. A key challenge in scalability is to make the QiNN lightweight enough to be deployed on low-power PLCs, and robust enough to support a variety of traffic.

6.2. Future Directions: Moving to Hybrid Quantum-Classical Hardware

The future of this research is in the shift to Hybrid Quantum-Classical (HQC) implementations, not only based on the quantum-inspired algorithms. The more accessible Noisy Intermediate-Scale Quantum (NISQ) devices are made available through cloud-based platforms, the most natural step will be to delegate the layers of the QiNN that are most computationally demanding to actual quantum processors and still do the data preprocessing on classical edge devices.

The use of QiNNs in other Industry 4.0 applications, including Autonomous Supply Chain Logistics, Smart Grid Security, and others, where the data dynamics are quite different than those of factory floor applications, should also be a focus of future research (MDPI, 2026). Also, with the combination of Federated Learning (FL) and QiNN, several smart factories can cooperate and train a global security model without exchanging sensitive local data on production, which improves the privacy and threat intelligence of the industrial sector as a whole.

7. Conclusion

This study has effectively shown the effectiveness of Quantum-Inspired Neural Networks (QiNN) as a powerful and effective tool in real-time intrusion detection in Smart Manufacturing Systems. The proposed model demonstrated a high level of detection accuracy of 99.2% on the X-IIoTID dataset by incorporating quantum mechanical concepts, including superposition and interference, into a classical neural

architecture, which is much higher than the detection accuracy of more classical deep learning models, such as CNNs and LSTMs. More to the point, the fact that the QiNN could work with a low detection latency (1.2 ms) and that its computational footprint is significantly smaller, makes it an ideal choice when it comes to working with edges in Industry 4.0 settings. In conclusion, this paper highlights the transformative nature of quantum-inspired algorithms to reduce the disconnect between fast industrial processes and future cybersecurity demands, guaranteeing the operational resiliency of the modern smart manufacturing plant to more complex cyber attacks.

References

- Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I & ,Guizani, M. (2024). A survey of machine and deep learning methods for Internet of Things (IoT) security .*Electronics*, .2975 ,(15)13 <https://doi.org/10.3390/electronics13152975>
- Al-Hawawreh, M., Sitnikova, E & ,Aboutorab, N. (2021). X-IIoTID: A connectivity- and device-agnostic intrusion dataset for Industrial Internet of Things .*IEEE Internet of Things Journal* .3977-3962 ,(5)9 , <https://doi.org/10.1109/JIOT.2021.3102056>
- Ferrag, M. A., Shu, L & ,Choo, K. K. R. (2024). Deep learning-based intrusion detection for distributed energy resources in smart grids .*ACM Transactions on Cyber-Physical Systems*.25-1 ,(1)8 ,
- Hussain, M., Zeadally, S & ,Al-Qerem, A. (2025). Quantum-inspired machine learning for cybersecurity: A systematic review and future directions .*Journal of Network and Computer Applications*.103856 ,234 ,
- Sayed, A. N., Rawat, D. B & ,Li, C. (2024). Edge-computing-enabled intrusion detection for smart manufacturing using deep learning .*IEEE Transactions on Industrial Informatics*.4162-4150 ,(3)20 ,
- Shaukat, K., Luo, S & ,Varadharajan, V. (2023). A survey on machine learning techniques for cyber security in the last decade .*IEEE Access*.22160-22107 ,11 ,
- Zhong, R. Y., Xu, X., Klotz, E & ,Newman, S. T. (2024). Intelligent manufacturing in the context of Industry 4.0: A review .*Engineering*.630-616 ,(2)10 ,