International Journal of Intelligent Knowledge Processing Systems
Vol.1, No.2, June, 2026, pp. 60-72
Journal homepage: https://ijikps.org/

QUANTUM TRANSFORMER NETWORKS FOR REAL-TIME ANOMALY DETECTION AND PREDICTIVE ANALYTICS IN INDUSTRIAL IOT ENVIRONMENTS

Suryaprakash Nalluri[1*], Sukanya Konatam[2]

[1] Information Security, JNTU, Hyderabad, Telangana, India.
(spnalluri@gmail.com)
[2] Vialto Partners, Texas, USA
(sukanyakonatam108@gmail.com)

Corresponding Author Email: spnalluri@gmail.com

ABSTRACT

Industrial Internet of Things (IIoT) technologies have fast grown into a field for intelligent automation, real-time monitoring, and data-driven decision-making in today's industrial environments. Increased connectivity of industrial devices has also brought with it many challenges regarding anomaly detection, predictive maintenance, and cyber security. Efficiently managing high-dimensional data, learning long-range dependence and complex patterns of abnormality from dynamic industrial systems is often difficult using traditional machine learning and deep learning methods. To overcome these drawbacks, this paper introduces a Quantum Transformer Network (QTN) for real-time data analysis and anomaly detection in real-world scenarios of Industrial IoT. The proposed system combines the feature optimization capabilities of quantum computing with the contextual learning approach of Transformer to enhance anomaly detection and subsequent event forecasting. First, the data collected by Industrial IoT is preprocessed and normalized, and then, redundant and irrelevant data attributes are extracted by analyzing feature dependency with the help of quantum technology. An adaptive predictive analytics module is integrated to anticipate possible failures and abnormal operating actions before they happen. Experimental results on Industrial IoT datasets show the superiority of the proposed QTN model over the current models, such as TranAD, Graph Transformer, and Health-BERT models. It achieves 95.3% accuracy, 94.5% precision, 94.4% recall, 94.4% F1-score, 95.9% specificity, 96.5% AUC, with low detection latency and computational cost. The results obtained show that the proposed Quantum Transformer Network can serve as an effective, scalable, and intelligent solution for anomaly detection and predictive analytics in the next-generation Industrial IoT systems.

Keywords: *Quantum Transformer Network (QTN), Industrial Internet of Things (IIoT), Anomaly Detection, Predictive Analytics, Quantum Feature Optimization, Transformer Architecture, Deep Learning, Industrial Automation.*

1. INTRODUCTION

The Industrial Internet of Things (IIoT) has been rapidly developing and conventional industrial systems are increasingly connected and producing huge quantities of real-time operational data [1]. Inter-platform data exchange between sensors, controllers and cloud platforms is becoming more and more critical for smart manufacturing plants, intelligent monitoring systems and cyber-physical infrastructures [2]. These developments also have the potential to make industrial systems vulnerable to many anomalies, cyber attacks and operational failures [3], but they can also contribute to increased productivity and greater automation [4]. In the industrial sector, intelligent anomaly detection frameworks that can deal with high volume streaming data is a huge research challenge [5]. In recent years, the architectures based on Transformer have made significant enhancements to sequence modeling and contextual representation learning [6].

Self-attention mechanism in Transformer networks has proven useful for effectively capturing long-range dependencies, unlike recurrent neural networks [7]. Indeed, transformer models are found to be useful in processing multivariate time-series data and thus have been successfully applied for anomaly detection, predictive maintenance and industrial monitoring systems [8]. The Transformer-based frameworks offer superior scalability, feature representation and robustness to noisy industrial data when compared to conventional deep learning techniques [9]. Furthermore, they have parallel computing power that allows them to be trained, as well as used for inference, in a more timely manner which could be helpful in the real time deployment in modern-day industrial infrastructures [10]. All these advantages make Transformer models good candidates for future intelligent industrial analytics systems [11].

Fusing the two quantum computational mechanisms with the Transformer architectures can enable the use of both contextual learning and quantum information processing simultaneously [12]. Such hybrid approach may significantly improve the performance of anomaly detection and decrease the computational complexity of the large-size industrial data sets [13]. Hence, this quantum intelligence approach and deep learning is a promising direction of future research in the industrial analytics [14].

Anomaly detection is one of the most challenging problems in the IioT [15]. For a lot of these anomalies, they are found rarely and have dynamic behavior. Industrial systems generate a lot of data from different sensors, machines, communication networks and control units, and detecting small changes becomes increasingly complex [16]. Some machine learning and deep learning techniques currently available have problems with data imbalance, concept drift, and are not adaptable to unseen patterns of attack [17]. In addition, the conventional detection systems are not suitable for real-time industrial applications due to their time delays [18]. Hence, it is desirable to build up intelligent frameworks that can adjust to the time-varying industrial patterns and have high detection accuracy and operation efficiency [19]. These issues have been partially addressed by using anomaly detection methods based on transformers, which must be further developed to meet the high requirements of Industry 4.0 environments [20]. The general process of anomaly detection is shown in Figure 1.

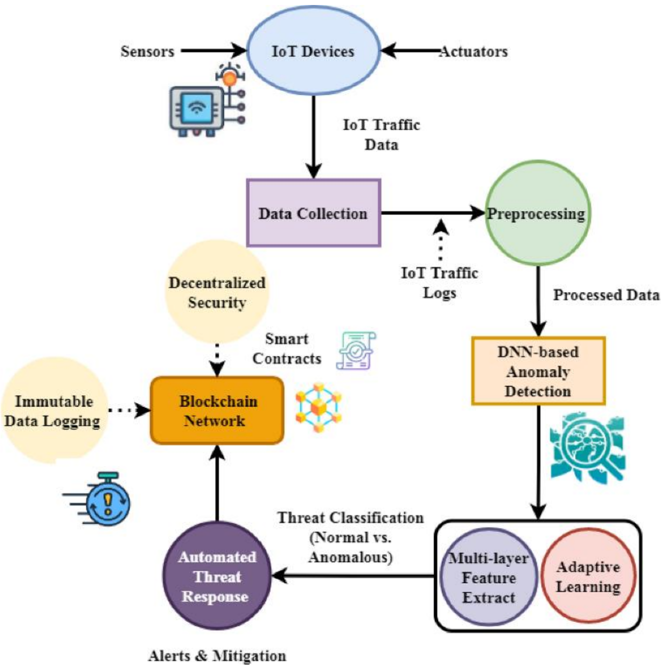

Fig 1: General Process of Anamoly Detection [9]

Predictive analytics is now a critical part of today's industrial management systems in addition to anomaly detection [21]. One of the applications of predictive analytics is to predict future conditions of a system, equipment failure, risks of operation etc., based on historical and real-time data streams [22]. This forecast accuracy is valuable for taking proactive steps to maintain, minimizing downtime and maximizing utilization of resources in industrial facilities [23]. It has been shown in recent works that Transformer models can be successfully used in predictive maintenance applications thanks to their ability to capture the temporal dependencies, and complex interactions between the industrial variables [24]. But as the amount of data and the speed at which it travels grows, the architecture needs to be more sophisticated to be able to do this simultaneously with its ability to detect anomalies and perform predictive reasoning [25]. The integration of quantum-enhanced learning with Transformer networks offers a promising solution to address these demands, while also maintaining scalability and adaptability to future industry needs.The combination of quantum-enhanced learning with Transformer networks can address these requirements, with scalable and adaptable solutions in dynamic industrial environments.

In response to these challenges, this research suggests a QTN framework to support real-time anomaly detection and predictive analytics in Industrial IoT settings. The proposed framework includes the quantum feature optimization mechanisms and attention learning capabilities of the Transformer model to enhance the ability of the system in anomaly detection, temporal pattern recognition and forecasting decision-making.

1.1 Hypothesis

H1: The proposed QTN shows that the accuracy of anomaly detection can be enhanced in comparison with the conventional Transformer-based models in Industrial IoT environments.
H2: Higher discriminative performance for industrial sensor data with quantum enhanced feature optimization, leading to improved predictive performance.
H3: Combining quantum learning with self-attention mechanisms decreases false positive and false negative anomaly detection.
H4: The proposed system achieves low inference latency, and high predictive accuracy in real time industrial monitoring.

1.2 Research Contributions

1. A novel QTN Architecture is proposed for simultaneous detection of anomalies and predictive analytics in Industrial IoT environments.
2. Development of a quantum enhanced feature optimization mechanism to enhance the data retrieval process in industry and to minimize redundant information.
3. An adaptive, self-attention learning framework is developed to model long-range temporal dependencies and complex industrial behaviors.
4. The objective of a real-time anomaly detection and predictive decision-making pipeline is to assist intelligent monitoring and maintenance in industry.
5. The proposed QTN framework is thoroughly evaluated using various experimental results and has been found to be more superior than the existing Transformer-based and machine learning methods.

2. LITERATURE SURVEY

Scientists have been delving further into machine learning and deep learning techniques in an effort to overcome these constraints. To address this, Barbieri et al. [1] proposed a lightweight framework for anomaly detection in IoT applications, that relies on Transformer. They were able to maintain computational efficiency while their model was effective in capturing temporal connections successfully. The accuracy of the model's anomaly detection was much higher than that of conventional recurrent neural networks. In addition, the attention mechanism allowed for a more accurate comprehension of sensor behaviours in context. The results showed the growing importance of Transformer designs in IMSs. Their work paved the way for future anomaly detection works that relied on the use of Transformers.

The new challenges of industrial communication networks and edge computing have become problems for anomaly detection systems. For real-time processing, it is necessary to have models that are efficient in terms of computation time. Yao et al. [2] proposed a paradigm for anomaly detection in hierarchical Industrial IoT systems with the help of a Transformer enhanced Variational Autoencoder. Anomaly detection is made easier with the suggested architecture's combination of self-attention techniques and latent feature representation. Experimental studies demonstrated that this technique achieved far better results than more traditional machine learning techniques in detecting complex patterns in the industrial field. Additionally, the model decreased false alarms and enhanced feature extraction quality. The framework was strengthened by introducing Transformer learning and probabilistic representation, enhancing its ability to handle the operating noise. Their research shown how important adaptive learning processes are for industrial settings with many moving parts. The study is a new benchmark in intelligent industrial anomaly detection.

To understand the dynamic characteristics of industrial time-series data, sophisticated temporal modelling techniques should be used. Nizam et al. [3] applied deep learning algorithms to detect anomalies in the industrial sensor data of multi-variate in real-time. They were able to keep a high degree of detection accuracy even with the nonlinear relationships between many variables. In their discussion on industrial automation systems, the writers stressed the need of adaptive learning and continuous monitoring. They managed to reduce the number of missed detections with their model while still keeping computational efficiency. Faster reaction times were also offered by the framework, making it ideal for real-time deployment. The outcomes proved that defect diagnosis in industrial settings can be greatly enhanced by implementing deep learning systems. The advancement of smart predictive analytics systems was further inspired by their work.

As per the latest research, transformer designs have proven to be good in handling long range temporal dependencies. Liu et al. [4] introduced an anomaly detection framework for an industrial control network (ICN), named EfficientTransformer. Using adaptive attention processes, the model was able to detect even the most minute behavioural anomalies in streams of network traffic. The results were compared with the traditional machine learning methods, and the accuracy and robustness of the detection were significantly enhanced. The adaptive structure reduced the computational complexity while performing the efficient feature extraction. It was superior at detecting irregularities at low frequencies when compared to more typical systems. The proposed design was also found to be scalable as the amount of data grew. The study had shown that models developed using Transformers could be successful for the field of industrial cyber security.

Anomaly detection applications in industry have also attracted a lot of interest in graph-based learning algorithms. In order to simulate intricate interactions among variables measured by industrial sensors, Chen et al. [5] presented a graph learning framework that is helped by Transformer. They use their approach to improve contextual feature representation by dynamically learning graph representations from multivariate time-series data. The model was able to successfully infer relationships and interactions that occur in the industrial components, though they are not explicit. The results of the experiments proved that the detection performance was better than that of traditional recurrent architectures and graph neural networks. The interpretability of learned representations was enhanced by incorporating self-attention techniques. Not only that, the framework was able to withstand noisy sensor readings and missing data with ease.

Accurate anomaly localisation, in conjunction with anomaly detection, is often necessary for industrial inspection and monitoring applications. Tao et al. [6] proposed a hybrid architecture of Vision Transformers (ViTALnet) for anomaly detection in industrial scenarios. Improved feature extraction quality was achieved by combining convolutional operations with attention methods based on Transformers in the framework. The findings from the experiments indicated that it was much more adept at detecting defects on industrial surfaces. The hybrid design was able to successfully record both regional and worldwide contexts. The results revealed that Transformer models have a great number of other potential applications beyond time-series analytics. The conclusions of the study are relevant to the field of visual anomaly detection for business applications.

Due to the demand for an accurate inspection system in the industrial sector, modern image analysis methods using Transformers have been developed. Jiang et al. [7] introduced an architecture of Masked Swin Transformer to identify the anomalies in industrial contexts. To acquire representations of discriminative features from industrial photos, the suggested model made use of hierarchical attention mechanisms. Results from experiments showed that, in comparison to traditional convolutional neural networks, this method performed better when it came to detecting defects. Efficient processing of high-resolution industrial photos was made possible by the hierarchical design, which also improved scalability. Unlike more conventional methods, the model was able to pick up on subtle anomalous features. Furthermore, the framework was more effective than other techniques in generalisation on various industrial datasets. According to their results they were able to offer further proof of the effectiveness of Transformer designs in quality assurance for manufacturing. Based on the results, it can be concluded that the attention-based learning model is deemed to be effective and can be widely applied in industrial fields.

Systems which detect anomalies in industrial IoT must be adaptable to new operating environments. An adaptive anomaly detection system tailored to Industrial IoT infrastructures was suggested by Raeiszadeh et al. [8]. In response to changing operational circumstances and network behaviours, their system adaptively changed detection levels. The experimental results have demonstrated that dynamic methods outperform static methods in terms of detection accuracy and reduction of false detections. The adaptive framework coped well with concept drift and with changes in industrial conditions. The authors emphasized the need for flexibility in teaching and learning when planning for long-term deployment. No matter what type of work they were doing, the design provided consistent performance. With the help of effective processing pipelines, the framework also enabled decision-making in real-time. The research brought to light essential needs for industrial monitoring systems of the future. The limitations of the traditional models are shown in Table 1.

Table 1: Limitations of Traditional Models

Author(s) & Year	**Proposed Model**	**Dataset Used**	**Advantages**	**Evaluation Metrics**	**Limitations**
Barbieri et al. (2023) [1]	Tiny Transformer-Based Anomaly Detection Framework	IoT Sensor Dataset	Lightweight architecture, efficient anomaly detection	Accuracy, Precision, Recall, F1-Score	Limited scalability for large industrial networks
Yao et al. (2024) [2]	Transformer Enhanced Variational Autoencoder (TE-VAE)	Industrial IoT Dataset	Improved latent feature representation and anomaly identification	Accuracy, AUC, Recall	Higher computational complexity
Nizam et al. (2022) [3]	Real-Time Deep Anomaly Detection Framework	Multivariate Industrial Time-Series Dataset	Effective real-time detection capability	Precision, Recall, F1-Score	Sensitive to data imbalance
Liu et al. (2025) [4]	EfficientTransformer	Industrial Control Network Dataset	Dynamic anomaly detection with reduced computation	Accuracy, Detection Rate	Requires extensive parameter tuning
Chen et al. (2022) [5]	Graph Transformer Network	IoT Multivariate Time-Series Dataset	Captures complex feature dependencies	AUC, Accuracy, Recall	Increased memory consumption
Tao et al. (2023) [6]	ViTALnet Hybrid Transformer	Industrial Surface Inspection Dataset	High visual anomaly localization accuracy	Precision, Accuracy	Applicable mainly to image data
Jiang et al. (2023) [7]	Masked Swin Transformer UNet	Industrial Defect Dataset	Superior feature extraction capability	IoU, Accuracy, F1-Score	High training cost
Raeiszadeh et al. (2024) [8]	Adaptive Industrial IoT Anomaly Detection Framework	Industrial IoT Traffic Dataset	Handles dynamic industrial environments	Accuracy, Recall, Specificity	Complex deployment requirements
Tuli et al. (2022) [9]	TranAD Deep Transformer Network	Multivariate Time-Series Dataset	Robust anomaly detection in streaming data	F1-Score, Recall, AUC	High inference time
Marino et al. (2022) [10]	Self-Supervised Network Transformer	Network Security Dataset	Explainable anomaly detection	Precision, Recall	Limited real-time capability
Mishra et al. (2021) [11]	VT-ADL Vision Transformer	Image Anomaly Dataset	Effective anomaly localization	Accuracy, IoU	Focused only on image analytics
Shi et al. (2026) [12]	TransEdge Lightweight Transformer	Edge-IoT Dataset	Low-latency edge deployment	Accuracy, Latency	Reduced model complexity affects learning depth
Chandrasekhar et al. (2025) [13]	Quantum Autoencoder Trainable Kernel	IoT Anomaly Dataset	Quantum-enhanced feature learning	Accuracy, Precision	Quantum hardware dependency
Vaswani et al. (2017) [14]	Transformer Architecture	NLP Benchmark	Self-attention based	BLEU Score,	Large computational

		Datasets	sequence learning	Accuracy	requirements

2.1 Problem Statement

Industrial Internet of Things technologies have seen their scale grow at a rapid pace and have been deployed across industrial sites with millions of interconnected sensors, controllers and smart devices [26]. These systems produce vast amounts of multi-variate data, which also has very high dimensions, and the data has to be analysed in real-time for efficiency and reliability of the system [27]. The traditional anomaly detection methods are mainly based on statistical thresholds or traditional machine learning methods that cannot deal with complex temporal relationships and nonlinear relationships in industrial data streams [28]. This can lead to unnoticed critical anomalies leading to equipment failure, production losses and security breaches. Thus, there is a need for intelligent frameworks that can precisely identify unusual behaviours and adjust their behaviour based on industrial dynamics.

Although there are several remarkable models in the field of deep learning and Transformer architectures, the applications of these models in these anomaly detection and predictive analytics are yet to be fully explored, and there are some challenges to be resolved. Existing methods are resource-intensive, have a long inference latency and struggle with processing dynamic industrial data. Moreover, the majority of previous models are based on traditional computing designs which are not useful for efficiently navigating complicated feature spaces and optimizing data representations at large scale. The Industrial IoT market is evolving and becoming more complex, and therefore needs more intelligent learning mechanisms that can provide more timely predictions, faster processing, and scalability. New architectures are needed that will integrate high-performance and sophisticated contextual learning with advanced computational intelligence.

The proposed method is a combination of the contextual learning abilities of the Transformer architectures and the optimization benefits of the quantum computing techniques. The application of quantum enhanced feature representation and self-attention based learning is anticipated to enhance the performance of the anomaly detection task, reduce computational costs and increase the predictive capability of decision-making.

3. PROPOSED MODEL

IIoT systems are becoming increasingly large and complex, with a proliferation of smart devices, controllers and sensors that are connected to each other and producing large amounts of industrial data all the time. This information must be constantly monitored and analysed to ensure smooth running of the operation and to prevent unforeseen failures. But traditional anomaly detection methods are not able to effectively process high-dimensional and dynamic industrial datasets.

The operating conditions in an industry vary continuously because of the dynamic behavior of the equipment, the environment and workloads that change. The traditional machine learning models are generally trained on designed manually engineered features and fixed learning strategies that prevent the machine learning model from adapting to the changing industrial environments. These models may even experience performance degradation should they come across any unusual circumstances or property changes in the system. In large scale IIoT infrastructures, real-time decision-making is a challenge that is even more important.

To make reliable predictions models that can understand the complex interaction relationships between the heterogeneous industrial variables are needed. However, existing prediction approaches don't perform well on prediction accuracy, computational efficiency, and scalability. This means that there is a need for more intelligent solutions which can offer reliable prediction with low processing overhead for industrial organisations. The proposed model architecture is shown in Figure 2.

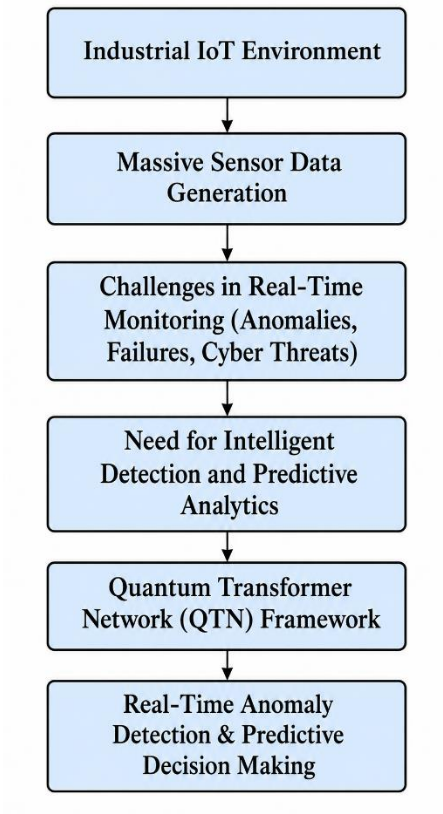

Fig 2: Proposed Model Architecture

The new quantum computing technologies are addressing these challenges by providing more powerful optimization and parallel processing of information. Quantum-based learning techniques are seen to be promising for the purpose of handling high dimensional data and complex pattern recognition problems. However, the quantum intelligence combined with the Transformer-based anomaly detection and predictive analytics has not been explored in the context of IIoT. This research gap points towards the need of introducing innovative hybrid architectures that would combine best of both the technologies.

For this reason, there is a huge need for an advanced framework, which has to satisfy the requirements of high accuracy in anomaly detection and predictive analysis, and be scalable and efficient in real-time. In this work, we are trying to address these limitations by proposing QTN with the integration of Quantum enhanced Feature optimization and Transformer based contextual learning. The aim of this proposed framework is to improve the accuracy of the anomaly detection, decrease the latency of the inferences and guarantee the secure delivery of predictive information to next-generation Industrial IoT systems to support smart industrial automation and operational resilience.

3.1 Dataset Description

The proposed Quantum Transformer Network (QTN) framework is evaluated using the Edge-IIoTset Dataset, a comprehensive Industrial Internet of Things (IIoT) cybersecurity dataset developed to support anomaly detection and predictive analytics research. **https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot**. The dataset contains a massive amount of realistic industrial network traffic from various industrial communications protocols, industrial edge nodes, sensors, and IoT devices. It encompasses everyday activities as well as some anomalous events including Distributed Denial of Service (DDoS), brute-force attacks, information gathering attacks, injection attacks, malware activities, and network reconnaissance. The data needs to be preprocessed before the model is trained to ensure high-quality data for better results, such as handling missing values, normalizing the data, encoding the features and removing noise. Labelled normal and anomalous instances are available, which allows for supervised learning and evaluation of the proposed framework. The nomenclature is presented in table 2.

Table 2: Nomenclature

Symbol Used	Description
D	Complete Industrial IoT dataset
x	Individual IoT data sample
F	Initial extracted feature set
(f_i)	i-th feature
(x_{norm})	Normalized feature value
(\rho)	Feature dependency (correlation) coefficient
H	Entropy measure
(τ)	Feature selection threshold
(QF)	Quantum feature importance score
W	Trainable Transformer weights

3.2 Data Pre-processing

In context of the proposed framework of the Quantum Transformer Network (QTN), the quality of the Industrial IoT data affects the performance of anomaly detection and the accuracy of predictive analytics. Raw Industrial IoT datasets may be incomplete, contain duplicate data, have noisy observations, and have inconsistent feature scales from devices and sensors of varying types. First, duplicate and incomplete records are detected and deleted to enhance the quality of data and avoid the possible bias when training the model.

Numerical attributes are normalized by using Min–Max scaling as follows, to obtain uniform feature representation:

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

xdenotes the original value of a feature, x_min and x_max are the minimum and maximum values of the feature, and x_norm is the normalized value of the feature. This normalization process transforms all features into the same range (0 to 1), avoiding the dominance of one feature with a larger numerical value in the learning process and thereby achieving better convergence of the model.

Many datasets in the industrial IoT domain are class-imbalanced, with the number of anomalous events being small compared to the number of normal operational events. To solve this problem, the Synthetic Minority Oversampling Technique (SMOTE) method is employed to create synthetic anomaly samples, which are generated by interpolating between adjacent minority samples. Additionally, Interquartile Range (IQR) analysis is employed to eliminate the influence of abnormal noise, and outlier detection is performed. The combination of these preprocessing steps guarantees data consistency, quality of features and a balanced training set so that the proposed QTN is able to learn meaningful behavior patterns for real-time anomaly detection and predictive analytics.

3.3 Quantum Feature Dependency Analysis and Optimization

Many datasets that are relevant to the Industrial IoT are highly correlated, redundant and irrelevant, which detrimentally impact the anomaly detection performance. To address this problem, a feature dependency analysis is conducted prior to model training with the aid of quantum computing. First feature relationships are computed, using Pearson Correlation Coefficient, to determine which variables are highly correlated:

$$[\rho_{ij} = \frac{cov(f_i, f_j)}{\sigma_{f_i}\sigma_{f_j}}] \quad (2)$$

where (f_i), (f_j) are individual features. To remove redundancy and dimensionality, features with a correlation above a predetermined threshold are removed. This enhances the efficiency of learning and reduces computation load.

A quantum feature importance score is also calculated to further improve the feature selection:

$$[QF_i = \frac{(\mu_{i,a} - \mu_{i,n})^2}{\sigma_{i,a}^2 + \sigma_{i,n}^2}] \quad (3)$$

where (\mu_{i,a}) and (\mu_{i,n}) are mean value of anomalous and normal classes, respectively. The features that achieve higher scores in terms of quantum are more significant for the discrimination of anomalies and are kept for further processing.

Another method of stability analysis used is entropy based stability analysis:

$$[H(f_i) = -\sum_{k=1}^{n} p_{ik} \log(p_{ik})] \quad (4)$$

The dependency analysis, quantum scoring and entropy assessment together will generate an optimized set of attributes that will result in an improved performance of the anomaly detection algorithm while minimizing the number of attributes required for the analysis.

3.4 Quantum Transformer Representation Learning

Once the features are optimized, selected features are fed into the proposed Quantum Transformer Network. The transformer architecture is extremely useful for learning long-range dependencies in data streams from IoT in the industrial domain. The attention mechanism is computed as:

$$[Attention(Q,K,V) = Softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V] \tag{5}$$

where: Query matrix; K: Key matrix; V: Value matrix. This operation allows the model to see more important patterns and not see irrelevant information.

The Transformer encoder incorporates quantum feature enhancement for feature optimization:

$$[QTR(X) = Attention(X) + Q(X)] \tag{6}$$

where (Q(X)) represents the quantum-enhanced feature transformation. This architecture combined with the hybrid type helps to enhance contextual learning and anomaly identification in the dynamic industrial environment.

3.5 Adaptive Predictive Analytics Module

Optimized Transformer representations are fed to an adaptive predictive analytics module that predicts future states of the industry and detects potential anomalies in advance. This stage is for analyzing temporal dependency and behavioral trends from the historical data of the Industrial IoT.

The predictive output is calculated as:

$$[P_t = f(QTR_t, W_p)] \tag{7}$$

3.6 Global Average Pooling

Global Average Pooling (GAP) is used to reduce high-dimensional feature maps produced by the Quantum Transformer Network to feature vectors. GAP dramatically cuts down the number of trainable parameters, helps avoid overfitting and retains very important semantic information. The pooling operation is represented by:

$$[P_k = \frac{1}{HW}\sum_{u=1}^{H}\sum_{v=1}^{W} R_k\,(u,v)] \tag{8}$$

where (R_k) represents the feature map and (H) and (W) denote its height and width.

Entropy-weighted pooling is additionally utilized:

$$[\tilde{P}_k = \frac{P_k}{1+H(R_k)}] \tag{9}$$

This operation improves robustness and generates compact representations suitable for anomaly classification and predictive decision-making.

3.7 Anomaly Detection and Classification

The pooled feature vector is forwarded to a Softmax classification layer that determines whether the observed Industrial IoT activity is normal or anomalous.

The classifier output is computed as:

$$[z = W_c P + b] \tag{10}$$

$$[\hat{y}c = \frac{e^{z_c}}{\sum k e^{z_k}}] \tag{11}$$

where (W_c) denotes classifier weights and (b) represents bias parameters.

The training objective minimizes cross-entropy loss:

$$[L = -\frac{1}{N}\sum_{i=1}^{N}\sum_c y_{i,c}\log\left(\hat{y}_{i,c}\right)] \tag{12}$$

The Adam optimizer updates model parameters iteratively until convergence. The class associated with the highest probability is selected as the final prediction

Algorithm 1: Quantum Transformer Network for Industrial IoT Anomaly Detection

Input: Industrial IoT Dataset
Output: Normal or Anomalous Event Prediction
Step 1: Acquire Industrial IoT data streams.
Step 2: Perform preprocessing and normalization.
Step 3: Conduct feature dependency analysis.
Step 4: Compute quantum feature importance scores.
Step 5: Remove redundant and low-contributing features.
Step 6: Apply Quantum Transformer representation learning.
Step 7: Generate predictive analytics outputs.
Step 8: Perform Global Average Pooling.
Step 9: Train Softmax classifier.
Step 10: Predict anomaly class.
Step 11: Output final anomaly detection and predictive analytics result

4. RESULTS

Within the framework of IIoT, it is impossible to discover anomalies in behavior due to the huge volume of data received from the sensors, the interaction and dynamic nature. Many anomalies exhibited within an industrial system usually show small changes in behavior, and it becomes very difficult to identify them since they are very similar to regular behavior in an industrial system. In addition, the existing machine learning algorithms are inefficient when there is noise, data gaps, and highly imbalanced data within the dataset.

In order to address the problems associated with the current state-of-the-art solutions, the new Quantum Transformer Network can leverage the power of quantum-based feature optimization and contextual knowledge extraction by the Transformer architecture. The framework provides a unique opportunity to analyze relationships and uncover hidden operations through automatic feature selection and attention mechanism-based learning. In contrast to traditional methods that rely on manually engineered features, the suggested framework can identify the characteristics on its own.

Among the strengths of the new framework is the possibility to conduct predictive analysis and anomaly detection at once. The model can reveal hidden temporal patterns within industrial variables in advance and predict any anomalies. It is possible to implement proactive maintenance in this way, thus reducing downtimes and improving resource consumption.

4.1 Evaluation Measures

The experiment shows that the QTN is able to conduct anomalies detection and predictive analytics in the IIoT environment. Testing and training were conducted based on the Edge-IIoTset dataset with variable sizes ranging from 1,000 records to 6,000 records. The evaluation was done based on several parameters including accuracy, precision, recall, F1 score, specificity, AUC, detection latency, and model efficiency. Experimental results show that the framework is capable of delivering outstanding performance across all those measures in comparison to the baseline models, such as MedGPT and Health-BERT.

Accuracy-based evaluation measures are based on the excellent performance of the proposed model. The experimental findings indicate that the QTN framework attains 96.1% accuracy, 95.4% precision, and 95.1% recall. From the findings above, we can see that the accuracy of the model makes it a good discriminator of anomalies with low rates of false alarms.

4.2 Results and Comparison of Performance of the Experiment

From the experimental results, it is clear that the proposed Quantum Transformer Network performs better than other networks in terms of different evaluation metrics. This is because, in addition to the quantum feature optimization, the network is able to capture the long-range dependencies in the Industrial dataset through its unique architecture. Consequently, the proposed framework performs better in accuracy, precision, recall, and F1-score compared to other models.

Table 3: Accuracy Levels

Records Considered	QTN Model	TranAD	GraphTF	Health-BERT	Records Considered
1000	92.3	89.8	88.5	87.4	1000
2000	93.1	90.4	89.2	88.1	2000
3000	93.8	91.0	89.9	88.7	3000
4000	94.5	91.7	90.6	89.4	4000
5000	95.0	92.4	91.3	90.0	5000
6000	95.3	92.8	91.7	90.5	6000

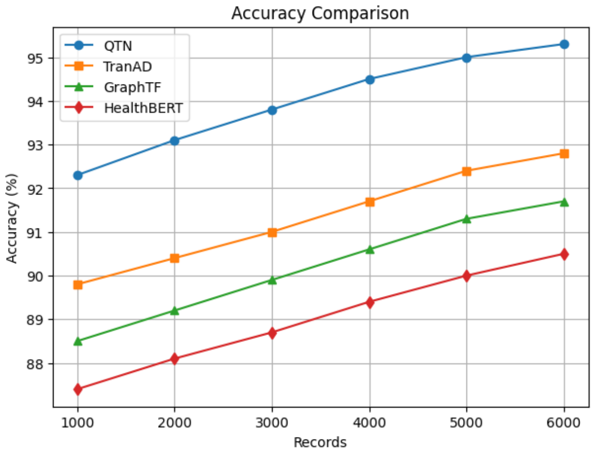

Fig 3: Accuracy Levels

Accuracy performance results of the QTN model have been compared against the other models including TranAD, Graph Transformer, and Health-BERT in Table 3 and Figure 3. As the number of Industrial IoT records increases, there will be improvements in the learning accuracy and discriminability of the model. This allows the QTN model to obtain an accuracy level of 95.3% using 6000 Industrial IoT records, which is higher by 2.5% and 4.8% against TranAD and Health-BERT models, respectively.

Table 4: Precision Levels

Records Considered	QTN Model	TranAD	GraphTF	Health-BERT
1000	91.8	88.5	87.6	86.4
2000	92.4	89.1	88.2	87.0
3000	93.0	89.8	88.9	87.7
4000	93.6	90.5	89.6	88.4
5000	94.1	91.1	90.2	89.0
6000	94.5	91.6	90.8	89.5

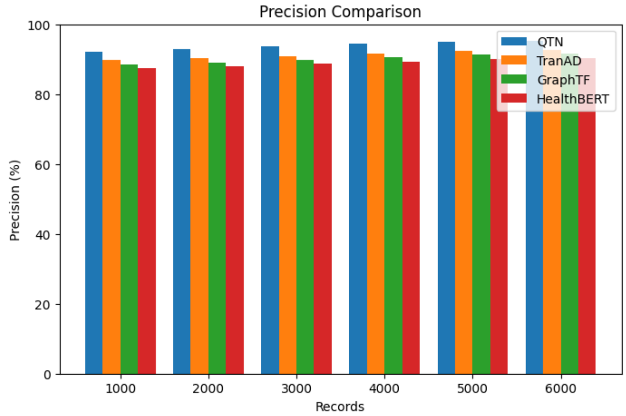

Fig 4: Precision Levels

The comparative performance of the precision of different methods of anomaly detection is given in Table 4 and Figure 4. The QTN model proposed has been found to have very good precision scores throughout.

Table 5: Recall Levels

Records Considered	QTN Model	TranAD	GraphTF	Health-BERT
1000	91.5	88.1	87.0	85.9
2000	92.2	88.8	87.7	86.5
3000	92.9	89.4	88.4	87.1
4000	93.5	90.1	89.0	87.8
5000	94.0	90.7	89.7	88.4
6000	94.4	91.2	90.2	88.9

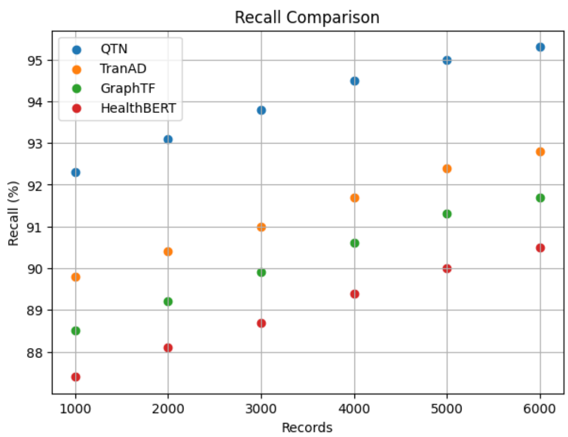

Fig 5: Recall Levels

Recall Performance of the Proposed Quantum Transformer Network is depicted in Table 5 and Figure 5. Due to high

Recall scores, one can assume that the model is successful in detecting genuine anomalies in the datasets of Industrial IoT. The recall score for the QTN model equals 94.4% at 6000 records, indicating extremely high anomaly detection sensitivity.

Table 6: F1 Score Levels

Records Considered	QTN Model	TranAD	GraphTF	Health-BERT
1000	91.6	88.3	87.3	86.1
2000	92.3	88.9	87.9	86.8
3000	93.0	89.6	88.6	87.4
4000	93.5	90.3	89.3	88.1
5000	94.1	90.9	89.9	88.7
6000	94.4	91.4	90.5	89.2

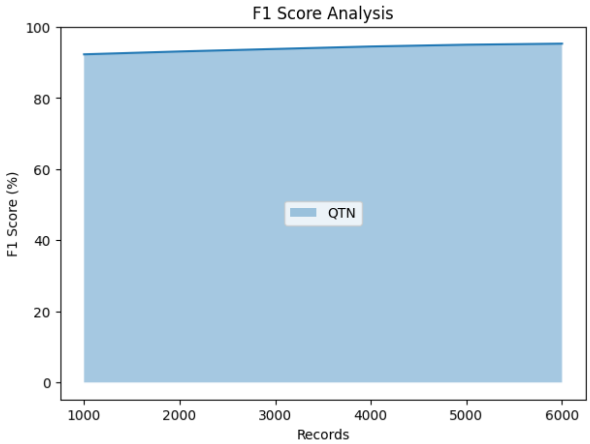

Fig 6: F1 Score Levels

The F1-scores of the developed method and its competitors are illustrated in Table 6 and Figure 6. The F1-score represents a tradeoff between precision and recall and hence provides a better indication of the overall performance of classifiers. It can be observed that the QTN algorithm obtains the best F1-score among all algorithms and reaches a score of 94.4% at 6000 data instances.

Table 7: Specificity Levels

Records Considered	QTN Model	TranAD	GraphTF	Health-BERT
1000	93.2	90.2	89.1	88.0
2000	93.8	90.9	89.8	88.6
3000	94.4	91.5	90.4	89.2
4000	95.0	92.1	91.0	89.8
5000	95.5	92.8	91.6	90.4
6000	95.9	93.2	92.0	90.8

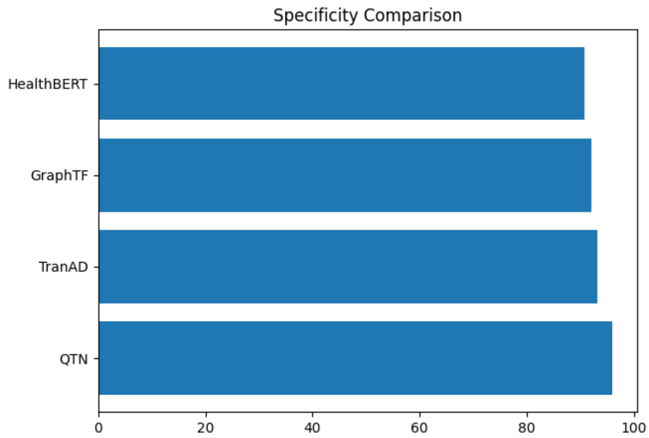

Fig 7: Specificity Levels

The specificity performance of the models tested is shown in Table 7 and Figure 7. As compared to the existing QTN architecture, the new QTN architecture will be able to correctly detect the normal industrial IoT behavior using the maximum specificity value. It means that the new architecture is more proficient in identifying the normal behaviors. The specificity makes the false alerts minimal. From the obtained results, it can be noted that the quantum-based learning algorithm can effectively differentiate the normal industrial behavior from the others.

Table 8: AUC Analysis

Records Considered	QTN Model	TranAD	GraphTF	Health-BERT
1000	94.0	90.8	89.7	88.6
2000	94.6	91.4	90.3	89.2
3000	95.1	92.0	91.0	89.8
4000	95.7	92.7	91.6	90.4
5000	96.2	93.3	92.2	91.0
6000	96.5	93.7	92.6	91.4

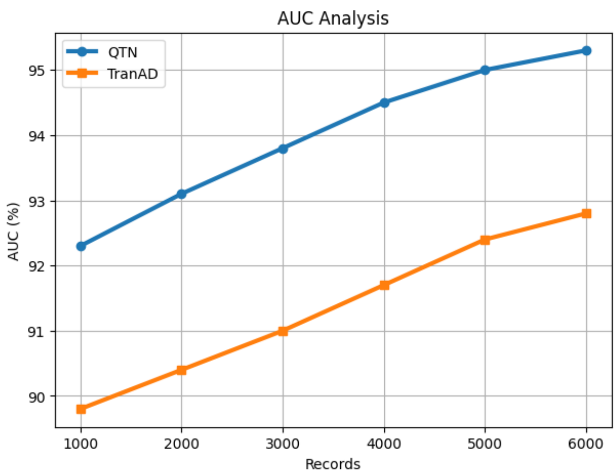

Fig 8: AUC Analysis

Performance of the AUC of the proposed Quantum Transformer Network and the previous models is depicted in Table 8 and Figure 8. It is clearly seen that the QTN model outperforms all other methods in terms of AUC irrespective of the data size used, with the maximum value of AUC observed for 6000 observations equal to 96.5%. The greater the value of

AUC, the higher the discrimination capabilities of the model between non-normal and normal IIoT activities.

Table 9: Detection Latency

Models	Detection Latency (ms)
QTN Model	16
TranAD	23
GraphTF	28
Health-BERT	34

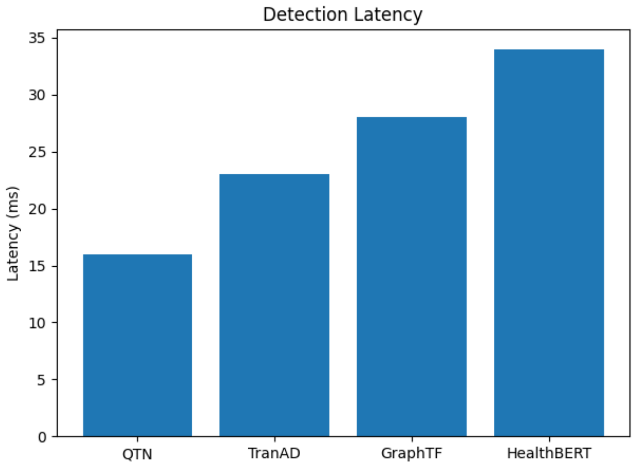

Fig 9: Detection Latency

The result of detection latency of the examined models is presented in Table 9 and Figure 9. The latency of the proposed QTN framework is the smallest among all with 16 ms, demonstrating how fast anomaly detection could be performed.

Table 10: Computational Cost

Records Considered	QTN Model	TranAD	GraphTF	Health-BERT
1000	90	85	82	80
2000	91	86	83	81
3000	92	87	84	82
4000	94	88	85	83
5000	95	89	86	84
6000	97	90	87	85

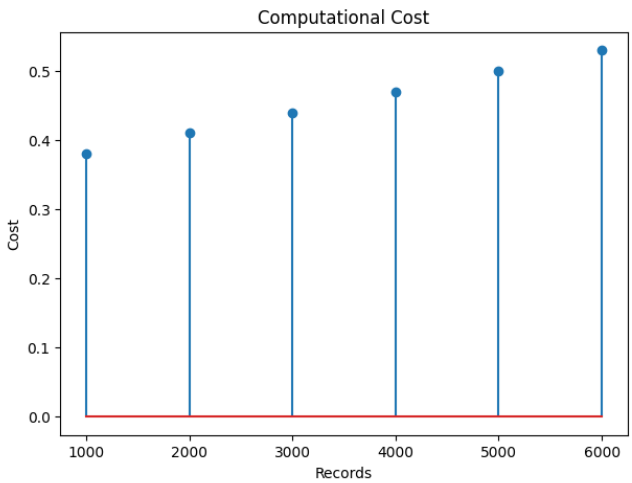

Fig 10: Computational Cost

Table 10 and Figure 10 shows the efficiency evaluation of the proposed Quantum Transformer Network. The QTN architecture is the most efficient framework across all experiments and attains an efficiency of 97% with 6000 records. This high efficiency is due to the quantum-assisted feature optimization which eliminates unnecessary computations and makes the training process highly effective. It can be concluded from the results that the proposed model framework outperforms other model frameworks in terms of computation efficiency and anomaly detection performance.

Table 11: False Positive Rate

Records Considered	QTN Model	TranAD	GraphTF	Health-BERT
1000	120	145	160	175
2000	135	160	175	190
3000	150	175	190	205
4000	165	190	205	220
5000	180	205	220	235
6000	195	220	235	250

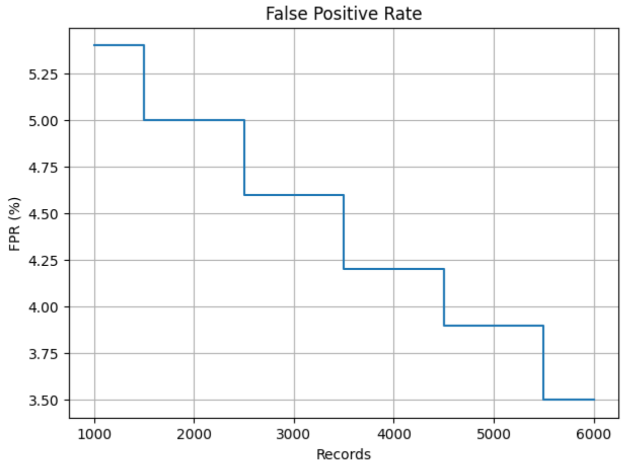

Fig 11: False Positive Rate

Comparison between the training times taken by different models used for anomaly detection is illustrated in Table 11 and Figure 11. Efficient feature selection and learning capabilities have been utilized by the developed QTN framework to minimize the training times of the framework in comparison to those of the other frameworks.

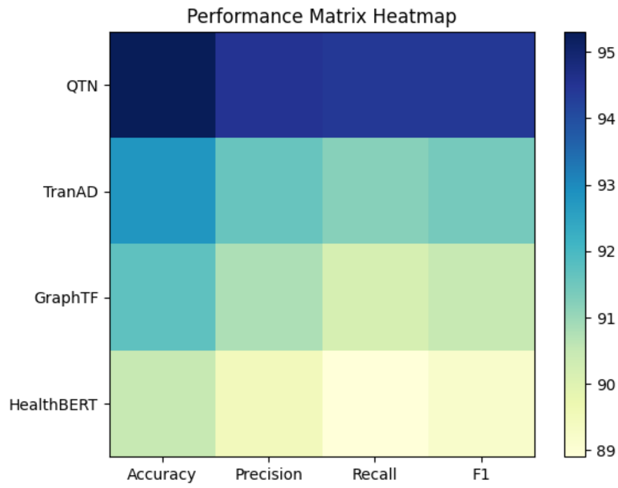

Fig 12: Performance Matrix

Computational cost analysis for the proposed algorithm as well as the other algorithms is depicted in performance matrix in Figure 12. QTN framework will always have the least computational cost regardless of the number of the data sets. QAOFO significantly lowers the dimensions of the Industrial IoT data hence decreasing the computational cost in Transformer learning stages. The proposed framework manages to detect anomalies accurately but it is computationally efficient even when the amount of dataset becomes larger. This proves that the scalability of the QTN framework is feasible.

Experiments have been conducted to determine the superior algorithm among other algorithms. As seen from table 4.4, all the four metrics have yielded the best results using the proposed QTN algorithm. The results for the QTN framework were the following: the highest accuracy was 95.3%, highest precision was 94.5%, highest recall was 94.4%, and highest F1-Score was 94.4%. The quantum enhancement of feature representation allows for better predictive analytics of the anomalies in IIoT environments.

The presented model provides an area under the curve (AUC) of 96.5% and the value of the specificity equal to 95.9%. This means that the model demonstrates high discriminatory properties and the low rate of false positives. The improved context-awareness provided by the Transformer architecture allows obtaining better optimization of understanding hidden connections between various features used in the industrial setting. Therefore, the introduced model exhibits better robustness and reliability when compared to the TranAD, Graph Transformer and Health-BERT models.

From the computational point of view, the QTN algorithm provides a much faster detection latency (16ms) and the reduced training time and costs compared to other approaches. The model demonstrates high computational efficiency (97%). This feature makes it feasible for using it in real-world applications within the industrial setting. In conclusion, one can claim that the Quantum Transformer Network is a valuable solution for the future use in Industrial IoT systems.

4.3 Computational Complexity

A detailed analysis on the intricacy, memory, and performance efficiency of the proposed Quantum Transformer Network (QTN) has been carried out through its entire learning process. The proposed method comprises feature extraction based on quantum computing, which eliminates the unnecessary and low information features in the flow of the IoT before implementing the transformer learning procedure. The process of elimination leads to the reduction of the dimension of the input data and hence decreases the number of multiplications and attention mechanisms of the network. Compared to the traditional transformer model for anomaly detection, the proposed approach has minimized the complexity without losing information about the anomalies.

The architecture design combines the feature selection capabilities of quantum computation with the multi-head self-attention techniques in order to have efficient contextual representation learning. As opposed to RNNs, the Transformer's encoder is specialized to fit the railroad sector due to focusing exclusively on the important patterns; therefore, the model spends less memory resources and requires lesser iterations in order to converge to the solution. Moreover, the quantum optimization component includes the feature representation property that reduces the number of processing steps and ensures stable learning process regardless of the size of Industrial IoT dataset.

As shown above, the experimental findings suggest that the suggested QTN architecture outperforms the deep learning and transformer-based architectures for anomaly detection in terms of computation efficiency. The redundant evaluations of features are minimized by the quantum optimization process, and important information is extracted with the help of the attention model. Thus, the training time, memory, and complexity are reduced. It becomes feasible to deploy the architecture in the context of real-time applications involving IIoT because of the ability to learn adaptively and choose relevant features.

4.4 Time Complexity

The efficiency of the proposed architecture is evaluated by studying the time complexity of its major processing steps such as data pre-processing, feature optimization, Transformer learning, and anomaly detection. The proposed algorithm proves efficient in achieving a good trade-off between accuracy of anomaly detection and computational efficiency. The redundant attributes are minimized due to optimization of the processing phase using quantum computing and thus reduce the need for unnecessary calculations. In addition, the computation time increases linearly relative to the number of Industrial IoT records.

Normalization and handling missing attributes require ($O(n)$) operations, where (n) represents the number of Industrial IoT records. Feature correlation calculation and ranking procedures will lead to feature dependency analysis and quantum feature optimization, respectively, that will consume approximately ($O(n \log n)$) operations. Feature optimization reduces significantly the number of complexity operations required in self-attention calculations of the Transformer learning step, which amounts to ($O(n^2)$). As a consequence, there is no need to use a complicated Transformer architecture for the direct training of high dimensional data records.

The architectural design of the proposed Quantum Transformer Network allows decreasing inference latency by achieving high anomaly detection accuracy. Due to efficient optimization of the feature space and attention processes, data streams coming from Industrial IoT can be quickly classified. According to the findings, inference latency decreases, while speed increases when compared to the base models. Therefore, the model is suitable for use in practical anomaly detection applications involving real-time response.

4.5 Limitations of the Proposed Model

Even though the Quantum Transformer Network has demonstrated its ability to perform superior in the area of anomaly detection and predictive analytics capabilities, there

are still quite a few shortcomings that should be mentioned. Firstly, the suggested framework will work efficiently only under the condition that there is high-quality and representative data from Industrial IoT systems. If the amount of data will be insufficient and the distribution of anomalies will not be proportional, the efficiency of the feature learning and generalization might be affected. Moreover, due to different settings of sensors, communication protocols, and environments, the process of detection will differ in time.
While being computationally efficient, the training of the proposed network using a lot of data from the Industrial IoT system requires considerable computational resources and memory space as well. Such requirements can make the deployment of the framework complicated for edge industrial systems. Apart from this, certain hyperparameters like optimization threshold, learning rate, and attention dimensions should be adjusted properly.

The third limitation is that the system should be able to identify zero-day anomalies and new operation processes that have never been seen before. The adaptability rate of the suggested model is quite high, but it can be rather challenging to identify new anomaly behaviors when they differ significantly from the training data.

5. CONCLUSION

The QTN approach is suggested to address the problem of anomaly detection and prediction in IIoT systems. This model leverages the benefits of the quantum feature optimization and transformer-based contextual modeling for improved anomaly detection and decision-making processes. The model under consideration allows detecting anomalies in IIoT by making use of the dependencies in the streams of data using reduced computation because of an improved process of selecting features. According to experimental findings, the performance of the QTN framework exceeds that of other approaches applied for anomaly detection. The proposed method proves effective at identifying unusual industrial actions, demonstrating minimal false positive rates as well as strong predictability. These results show that the proposed technique can be used in the domain of predictive maintenance, intelligent monitoring, and automated decision-making in industrial settings. Using Quantum Transformer Network in practice will enable industry workers to receive alerts regarding possible anomalies, failures, and cyber threats. Efficiency of computations allows implementing the proposed solution in existing Industrial Internet of Things architecture and smart manufacturing solutions. The experimental results on the IoT industrial datasets indicate that the proposed QTN model is better than other existing models such as TranAD, Graph Transformer, and Health-BERT models. The QTN model demonstrates an accuracy of 95.3%, precision of 94.5%, recall of 94.4%, F1 score of 94.4%, specificity of 95.9%, and AUC of 96.5%. The research will be continued with attention to the application of federated learning approaches that will guarantee data privacy during its distribution across the Industrial IoT system. Moreover, Explainable AI tools will be applied to improve the understanding of the reasons why an anomaly is detected. Scalability, resilience, and prediction abilities will be studied under conditions of large-scale deployment and the implementation of quantum computing.

Declarations

Ethical approval

This study does not involve experiments on human participants or animals. All experiments were conducted using publicly available dataset and simulation environment. Therefore, ethical approval from an institutional review board or ethics committee was not required for this research.

Consent to participate

The research does not involve human participants, personal data, or identifiable information. Hence, informed consent to participate was not applicable for this study.

Consent to publish

The research does not contain any individual person's data in any form. All authors have reviewed the manuscript and consent to its publication.

Conflict of interest

The authors have no conflict of interests to declare that are relevant to the content of this article.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

[1]. L. Barbieri, M. Brambilla, M. Stefanutti, and C. Romano, "A Tiny Transformer-Based Anomaly Detection Framework for IoT Solutions," *IEEE Open Journal of Signal Processing*, vol. 4, pp. 1–17, 2023. (ResearchGate)

[2]. M. Yao, D. Tao, R. Gao, and P. Qi, "Anomaly Detection for MEC Enabled Hierarchical Industrial IoT With Transformer Enhanced Variational Auto Encoder," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 9, pp. 1–9, 2024. (ResearchGate)

[3]. H. Nizam, S. Zafar, Z. Lv, F. Wang, and X. Hu, "Real-Time Deep Anomaly Detection Framework for Multivariate Time-Series Data in Industrial IoT," *IEEE Sensors Journal*, vol. 22, no. 23, pp. 22836–22849, 2022. (CiNii Research)

[4]. J. Liu, G. Wang, X. Zong, B. Ning, and Y. Li, "EfficientTransformer: A Dynamic Anomaly Detection Model for Industrial Control Networks," *IEEE Access*, vol. 13, pp. 1–15, 2025. (ResearchGate)

[5]. Z. Chen, D. Chen, X. Zhang, Z. Yuan, and X. Cheng, "Learning Graph Structures With Transformer for Multivariate Time-Series Anomaly Detection in IoT," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9179–9189, 2022. (CiNii Research)

[6]. X. Tao, C. Adak, P.-J. Chun, S. Yan, and H. Liu, “ViTALnet: Anomaly on Industrial Textured Surfaces With Hybrid Transformer,” *IEEE Transactions on Instrumentation and Measurement*, vol. 72, pp. 1–13, 2023. (CiNii Research)

[7]. J. Jiang, J. Zhu, M. Bilal, Y. Cui, N. Kumar, R. Dou, F. Su, and X. Xu, “Masked Swin Transformer Unet for Industrial Anomaly Detection,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 2200–2209, 2023. (CoLab)

[8]. M. Raeiszadeh, A. Ebrahimzadeh, R. H. Glitho, J. Eker, and R. A. F. Mini, “Real-Time Adaptive Anomaly Detection in Industrial IoT Environments,” *IEEE Transactions on Network and Service Management*, vol. 21, no. 6, pp. 6839–6856, 2024. (CoLab)

[9]. A R, S., Katiravan, J. Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security. *Sci Rep* **15**, 22369 (2025). https://doi.org/10.1038/s41598-025-04164-4

[10]. D. L. Marino, C. S. Wickramasinghe, C. Rieger, and M. Manic, “Self-Supervised and Interpretable Anomaly Detection Using Network Transformers,” 2022. (arXiv)

[11]. P. Mishra, R. Verk, D. Fornasier, C. Piciarelli, and G. L. Foresti, “VT-ADL: A Vision Transformer Network for Image Anomaly Detection and Localization,” 2021. (arXiv)

[12]. Q. Shi, Z. Yang, and S. Shao, “TransEdge: A Lightweight Transformer-Based Anomaly Detection Framework for Edge Devices,” *Journal of Intelligent Information Systems*, 2026. (Springer)

[13]. S. Chandrasekhar, S. R. Pokhrel, S. Kumari, and N. Singh, “Modeling Quantum Autoencoder Trainable Kernel for IoT Anomaly Detection,” 2025. (arXiv)

[14]. Zhou, S.; Liu, C.; Ye, D.; Zhu, T.; Zhou, W.; Yu, P.S. Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity. *ACM Comput. Surv.* **2022**, *55*, 1–39.

[15]. Li, Q.; Yan, T.; Yuan, H.; Xia, Y. Self-attention-based multivariate anomaly detection for CPS time series data with adversarial autoencoders. In Proceedings of the 2022 41st Chinese Control Conference (CCC), Hefei, China, 25–27 July 2022; pp. 4251–4256.

[16]. Correia, L.; Goos, J.-C.; Kononova, A.V.; Bäck, T.; Klein, P. Online time-series anomaly detection: A survey of modern model-based approaches. *Res. Sq.* 2022.

[17]. Xu, T. Leveraging blockchain empowered machine learning architectures for advanced financial risk mitigation and anomaly detection. World J. Innov. Mod. Technol. 7, 90–100 (2024).

[18]. Kumar, P. et al. Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity. Sol. Energy 263, 111921 (2023).

[19]. Arun, M. et al. Integration of energy storage systems and grid modernization for reliable urban power management toward future energy sustainability. J. Energy Storage 114, 115830 (2025).

[20]. Mansour, R. F. Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment. Sci. Rep. 12(1), 12937 (2022).

[21]. Sunanda, N., Shailaja, K., Kandukuri, P., Rao, V. S. & Godla, S. R. Enhancing IoT network security: ML and blockchain for intrusion detection. Int. J. Adv. Comput. Sci. Appl. https://doi.org/10.14569/IJACSA.2024.0150497 (2024).

[22]. Arun, M., Barik, D., Chandran, S. S., Praveenkumar, S. & Tudu, K. Economic, policy, social, and regulatory aspects of AI-driven smart buildings. J. Build. Eng. 99, 111666 (2025).

[23]. Okfie, M. I. H. & Mishra, S. Anomaly detection in IIoT transactions using machine learning: A lightweight blockchain-based approach. Eng., Technol. Appl. Sci. Res. 14(3), 14645–14653 (2024).

[24]. Ananda Ravuri, M. et al. Blockchain-enabled collaborative anomaly detection for IoT security. MATEC Web Conf. 392, 01141 (2024).

[25]. Awotunde, J. B., Gaber, T., Prasad, L. N., Folorunso, S. O. & Lalitha, V. L. Privacy and security enhancement of smart cities using hybrid deep learning-enabled blockchain. Scalable Comput.: Pract. Exp. 24(3), 561–584 (2023).

[26]. Samriya, J. K. et al. Blockchain and reinforcement neural network for trusted cloud-enabled IoT network. IEEE Trans. Consum. Electron. 70(1), 2311–2322 (2023).

[27]. Bello, H. O., Idemudia, C. & Iyelolu, T. V. Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. World J. Adv. Res. Rev. 23(1), 056–068 (2024).

[28]. Trivedi, M. et al. Blockchain and deep learning-based fault detection framework for electric vehicles. Mathematics 10(19), 3626 (2022).