Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

AN EFFECTIVE QUANTUM CONVOLUTIONAL NEURAL NETWORKS BASED PREDICTIVE FRAMEWORK FOR CYBERSECURITY INTRUSION DETECTION AND PREVENTION IN WIRELESS SENSOR NETWORKS

K P Manikandan[1], Gomathi C[2], V.Saraswathi[3], Pavithra Guru[4], S. K. Rajesh Kanna[5], M.Preetha[6]

[1]*Assistant Professor, Department of CSE(cyber security), Madanapalle institute of technology & science , kadiri road, Angallu, Madanapalle , Andhrapradesh 517325.*
[2]*Assistant Professor, Department of AI&DS, Panimalar Engineering College, Chennai (0009-0003-9938-7013).*
[3]*Professor, Department of CSE, Chennai Institute of Technology, Sarathy Nagar, Kundrathur, Chennai (0009-0000-5947-468X).*
[4]*Assitant Professor, Department of ECE , SRMIST Ramapuram (0000-0003-2403-1728).*
[5]*Professor, Department of Mechanical Engineering, Rajalakshmi Institute of Technology, Chennai, India (0000-0003-1013-008X).*
[6]*Professor & Head, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai (0000-0001-8483-9871).*

Email: *manikandankp@mits.ac.in, gomathipec@gmail.com, saraswathiv.cse@citchennai.net, gururvs@gmail.com, skrkanna@gmail.com, smpreetha14@gmail.com*

Wireless Sensor Networks (WSNs) are essential for many uses, such as military surveillance and environmental monitoring. However, their open nature makes them vulnerable to security threats, making Intrusion Detection and Prevention Systems (IDPS) essential for safeguarding WSNs against unauthorized access and malicious activities. This work presented a novel Correlation coefficient min-max Scale Modulation Transformer based Quantum Classical Convolutional Network with Aphid-Ant Optimization (CCMM SMT-QCCN-AAO) for intrusion detection. Initially, the pre-processing function is carried out using (CCMMW) to eliminate the noise features from the input WSN-DS dataset. Then, the intrusion based features were extracted using the Scale Aware Modulation Meet Transformer (SAMMT) for the further detection and classification. After that a novel Aphid-Ant Optimization Algorithm (AAOA) is employed to optimize the hyperparameters of Quantum Classical CNN model for reducing the error rate, computational time, computational complexity and improve the classification accuracy. In addition, WSN-DS classes such as Blackhole, Flooding, Grayhole, Normal, and TDMA are detected and classified using Hybrid Quantum Classical CNN (HQCCNN) for the effective detection From the obtained results, it is observed since the CCMM SMT-QCCN-AAO model performs better than the existing methods by providing improved accuracy of 99.67%, precision of 99.66%, recall of 99.66%, specificity of 99.67% and f1-score of 99.66%.

Keywords: *Intrusion detection, wireless sensor network, Feature extraction, Convolutional layer, pooling layer*

1. INTRODUCTION

These days, the wireless sensor network (WSN) is receiving more attention because of its widespread use in both the military and the civilian sector. These services include area monitoring, smart cities, healthcare, and environmental sensing [1,2]. The provision of such vital services would pique the curiosity of security attackers and necessitate the continuous improvement of security remedies [3,4]. Potential assaults that can negatively impact the services these networks offer can be prevented, detected, and limited by these solutions. With the quick development of internet technology, issues with organised security are becoming more and more unusual every day [5,6]. Intrusion detection system (IDS) researchers have been working nonstop to defend networks against malware and other threats. Based on the items that are detected, an intrusion detection system can be divided into two groups: network-based and host-based. Host-based IDSs monitor the behaviour or condition of the host system service, including any instances of illegal installation or access, as well as the presence of anticipated data in the file system's memory status and system events [7,8].

Host-based intrusion detection systems rely on the event log system. However, HIDS's drawbacks include its low false alarm rate and inability to analyse behaviour tied to the internet. Network-based intrusion detection systems (IDS) identify unauthorized computer system access attempts through network traffic analysis [9,10]. They scan incoming packets for suspicious patterns and may alert administrators or prevent access. To develop an intelligent intrusion detection system that focuses on dynamic expansion and self-adaptive behavior, a more automated approach is needed [11,12].

New invasions and the emergence of large data have led to an evolution in network attacks. These changes are difficult for traditional anomaly detection tools to identify. The main goals of research are to lower training costs and train high-efficiency models. As more sophisticated intrusion detection techniques are developed, applying them to convolution neural network classifiers may increase the accuracy and rate of detection [13-15]. This work proposed a solution for intrusion detection and more accurate in recognizing altered malware, enhancing detection accuracy and preventing potential threats. The key contribution of the proposed study is given as follows:

- Initially, the pre-processing function is carried out using (CCMMW) to eliminates the noise features from the input WSN-DS dataset
- Then, the intrusion based features were extracted using the Scale Aware Modulation Meet Transformer (SAMMT) for the further detection and classification
- After that a novel Aphid-Ant Optimization Algorithm (AAOA) is employed to optimize the parameters of Quantum Classical CNN model for reducing the error rate, computational time, computational complexity and improve the classification accuracy.
- In addition, WSN-DS classes such as Blackhole, Flooding, Grayhole, Normal, and TDMA are detected and classified using Hybrid Quantum Classical CNN (HQCCNN) for the effective detection
- Finally, the performance characteristics recall, error rate, accuracy, precision, specificity, computational time, and f-score) were evaluated and contrasted with those of other models.

2. LITERATURE SURVEY

In 2024, Jhon, A. et al, [16] have introduced a CBWSN_VSEMLA for the creation of a security threats detection system. The CBWSN model employs fuzzy C-Means clustering, whereas the VSEMLA uses a combination of ensemble machine learning techniques for attack detection and Principal Component Analysis (PCA) for feature selection. The

PCA_RandomForest IDS model outperforms the others with 99.999% accuracy, according to the experimental results; the PCA_Bagging IDS model comes in second with 196.78% accuracy, and the PCA_LogitBoost model with 98.88% accuracy. But it takes a long time to compute 231.64 seconds to train the PCA_Random Forest method.

In 2023, Bukhari, S.M, et al. [17] have presented a FL-based SCNN-Bi-LSTM model in Wireless Sensor Networks (WSNs) to improve private and security.Several sensor nodes can train a single global model using the novel FL-based SCNN-Bi-LSTM model without disclosing personal information. Using network pattern analysis, it successfully detects sophisticated cyber attacks. The purpose of the model is to use specialised datasets to identify and classify various kinds of Denial of Service (DoS) attacks. As a result of its improved detection rates and classification accuracy over conventional ADNN models, the FL-SCNN-BiLSTM model reduced the number of false positives and negatives.

In 2024, Gatate, V. et al, [18] have presented a novel DHN-SCA method for intrusion detection in WSN. The Deep Hybrid Network including Spatial and Channel Attention (DHN-SCA) is the name given to it. The DHN combines a local attention module with convolutional neural networks (CNNs) to improve intrusion detection accuracy and efficacy. Element-wise multiplication operations are used by the two sub-modules that comprise the Local Attention Module, Spatial Attention and Channel Attention, to enhance the feature tensor. Metrics including accuracy, precision, recall, and F1 score are used in studies and evaluations on benchmark datasets to study the performance of the DHN.

In 2023, Ravindra, C. et al, [19] have presented a ELM-TSAO method for anomalous detection. Piecewise Aggregate Approximation is used to extract low-dimensional features from the input with high accuracy during pre-processing. The Enhanced Transient Search Arithmetic Optimisation meta-heuristic technique is used to optimise an ELM in the second phase. Dynamic thresholding, which creates threshold rates to distinguish between normal and abnormal sensed information, is used in the last stage to detect anomalous data. The suggested procedure is simulated using the PYTHON platform. When compared to alternative models, the suggested anomaly detection model performs well, with an overall accuracy of 97.4% for the IBRL dataset.

2.1 Problem statement

WSNs are increasingly utilized in critical applications like environmental monitoring and military surveillance, but their deployment faces security challenges due to their distributed nature and limited resources. The challenge lies in cybersecurity intrusion detection and prevention, which must protect networks against threats like unauthorized access, data tampering, and Dos attacks while balancing energy efficiency, processing power, and network scalability. Effective solutions must address sensor node vulnerability, accurate intrusion detection, and preventive measures without affecting network performance or longevity.

3. PROPOSED METHODOLOGY

This section provides a full explanation of a deep learning architecture used in wireless sensor network to optimise intrusion detection by the extraction and classification of Hybrid features. Initially, the pre-processing function is carried out using (CCMMW) to eliminate the noise features from the input WSN-DS dataset. Then, the intrusion based features were extracted using the Scale Aware Modulation Meet Transformer (SAMMT) for the further detection and classification. After that a novel Aphid-Ant Optimization Algorithm (AAOA) is employed to optimize the parameters of Quantum Classical CNN model for reducing the

error rate, computational time, computational complexity and improve the classification accuracy[20-22]. In addition, WSN-DS classes such as Blackhole, Flooding, Grayhole, Normal, and TDMA are detected and classified using Hybrid Quantum Classical CNN (HQCCNN) for the effective detection. Figure 1 displays the workflow of the proposed approach.

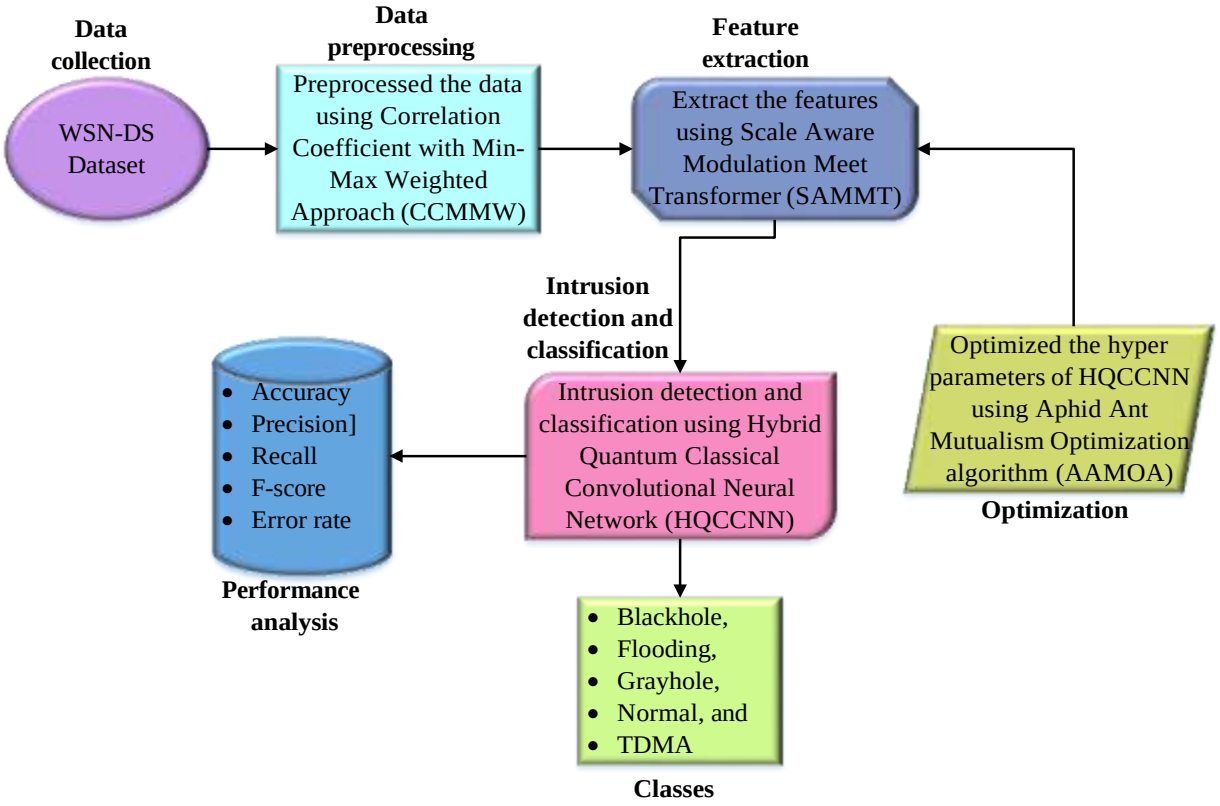

Figure 1: workflow of the proposed approach

3.1 Dataset Description

A publicly accessible dataset on the Kaggle website has been utilised to assess the functionality of the suggested framework, WSN-DS: A dataset designed for wireless sensor networks' intrusion detection systems. It encompasses four distinct types of attacks: Blackhole, Flooding, Grayhole, Normal, and TDMA **.**

3.2 Data Pre-processing using CCMMW Approach

The pre-processing processes involved and concentrate on how normalization and correlation values affect the final data representation in order to illustrate the pre-processing function utilizing the CC with MM weighted method. Ensure all the features are on the same scale using the min-max normalization in equation (1).

$$N(s_i) = \frac{s_i - mi(s)}{ma(s) - mi(x)} \times (new\_ma - new\_mi) + ne\_mi \quad (1)$$

In this equation, the feature values are scaled to a range of 0 to 1. For each feature s_i, after deducting the minimal score, the outcome is divided by the range. (maximum value minus minimum value). The desired range is then reached, in this example, 0 to 1. The calculate the Pearson correlation coefficients (PCC) to assess the linear relationship between each feature and the target label in equation (2).

$$r = \frac{\sum_{i=1}^{n}(s_i - \bar{s})(t_i - \bar{t})}{\sqrt{\sum_{i=1}^{n}(s_i - \bar{s})^2 \sum_{i=1}^{n}(t_i - \bar{t})^2}} \tag{2}$$

This equation calculate each feature's s correlation coefficient (r) with the target label (t). This quantifies the degree to which each feature is associated with the desired label. One indicates a perfect positive correlation (value = 1), a perfect negative correlation (value = -1), and no correlation (value = 0). Then, normalized the weight to adjust the normalized feature scores based on their correlation with the target table in equation (3).

$$v_0 = \left(\frac{V_{i,j} - n_{ij}}{n_{aj} - n_{ij}} \times (new\_ma - new\_mi) \right) + C \left(\frac{V_{i,j} - n_{ij}}{n_{ij} - n_{ij}} (new\_ma - new\_mi) + new\_mi \right) . Cor(V_i, V_{target}) \tag{3}$$

This formula incorporates each feature's Pearson correlation coefficient PCC to alter the normalized values. In this case, the original feature values are represented by $V_{i,j}$, and the min and max values of the feature are denoted by n_{ij} and n_{aj}, respectively. The correlation effect's weighting is determined by the CCC coefficient. The Pearson correlation coefficient between the target and the feature is denoted by $Cor(V_i, V_{target})$. The correlation-weighted normalized data, which incorporates normalization and correlation considerations, is the result of the preprocessing function. By highlighting pertinent aspects, this enhanced data representation seeks to enhance the performance of classification approach.

3.3 Feature Extraction using Scale Aware Modulation Meet Transformer (SAMMT)

The proposed Scale-Aware Modulation Meet Transformer (SAMMT) offers a unique feature extraction method. Together, these modules improve the network's capacity to detect long-range dependencies and multi-scale spatial information, which boosts the network's performance in visual identification tasks.

Using large convolutional kernels, MHMC improves its ability to simulate long-range dependencies by expanding the receptive field. MHMC lowers parameter size and computational cost by splitting input channels into N heads and applying different depth-wise separable convolutions to each head. The kernel size is initially set at 3 × 3 × 3 and grows by 2 for each head, enabling control over receptive fields and multi-granularity data. This could be expressed as equation (4).

$$M_h M_c(S) = Concat(D_{k1\times k1}(s1), ...D_{k_n \times k_n}(s_n)) \tag{4}$$

where $s = [s1, s2, s3, ...sn]$ represents the input character split into different heads in the channel dimension, and $k_i \in \{3,5,...K\}$ indicates the size of kernel the kernel size increasing monotonically by 2 per head.

3.3.1 Scale aware aggregation

The Scale-Aware Aggregation (SAA) approach is introduced in MHMC to improve information exchange across several heads. Features of various granularities generated by MHMC are shuffled and grouped by SAA. This is taking one channel from each head and grouping them together, then doing up-down feature fusion inside each group by employing the inverse bottleneck structure. This procedure can be stated as follows in equation (5-7)

$$M = W_{inter}([G_1, G_2, ...G_M]) \tag{5}$$

$$G_i = W_{intra}([h^i_1, h^i_2 .....h^i_N]) \tag{6}$$

$$h^i_j = DConv_{k_j \times k_j}(s^i_j) \in R^{h \times W \times 1} \tag{7}$$

where W_{inter} and W_{intra} are indicates weight matrices of point-wise convolution. $j \in \{3,5,...N\}$ and $i \in \{3,5,...M\}$ denote the count of heads and groups, respectively $h_j \in R^{h \times W \times 1}$ represents the j^{th} head with depth-wise convolution, and h^i_j represents the i^{th} channel in the j^{th} head.

3.3.2 Scale Aware modulation

The output feature map modulates the value V via the scalar product following the acquisition of multi-scale spatial information by MHMC and their subsequent aggregation with SAA. The output Z is calculated for the input characteristics $S \in R^{h \times W \times 1}$ in the following way in equation (8).

$$Z = M \otimes V, \quad V = W_v S, \quad M = SAA(M_h M_c(W_x S)) \tag{8}$$

where W_v and W_x are the weight matrices of linear layers, and $\otimes$ is the element-wise multiplication. By adjusting dynamically to various inputs, the modulator M achieves adaptive self-modulation. This is memory-efficient and enables channel- and spatial-specific modification of the value following element-wise multiplication, especially for processing high-resolution images.

3.3.3 Evolutionary Hybrid network

Based on the fluctuation pattern in the network's capture range dependencies, the network reallocates computational modules to increase computational performance. To lessen the computational load, Multi-Scale Attention (MSA) blocks are only used starting at the penultimate step. For the penultimate stage, two hybrid stacking tactics are suggested: using SAM blocks for the first half and MSA blocks for the second half, and stacking one SAM block and one MSA block in succession. These tactics are put out as: $(SAM \times 1 + MSA \times 1) \times \frac{N}{2}$, $(SAM \times \frac{N}{2} + MSA \times \frac{N}{2})$. These techniques mimic the change from local to global dependency capture, improving the network's capacity to manage heterogeneous receptive fields. By following these procedure, the Scale-Aware Modulation Meet Transformer extract multi-scale spatial features, and modulates these features adaptively to enhance detection, while ensuring computational efficiency and scalability.

3.4 Intrusion detection an classification using Hybrid Quantum Classical Convolutional Neural Network (HQCCNN)

For wireless sensor networks (WSNs) to remain secure and functional, intrusion detection and categorisation is an essential duty. To improve the accuracy and efficiency of this task, a QCCNN can be utilised. Using the same concepts and formulas, the following explains how QCCNN can be used for intrusion detection and classification in WSNs.

A single filter is parameterised by an array A that has the same form as the window and maps small areas of the input to individual neurones of the outcome. With the predefined window size of $m \times n$ and the input being a 2D array P with size $v \times h$, the first window is situated at the upper left corner of P, specifically $P_{1:m,1:n}$. The linear function is responsible for mapping given in equation (9).

$$P_{1:m,1:n} \to \sum_{1 \le i \le m, ` \le j \le n} P_{i,j} A_{i,j} \tag{9}$$

After it reaches the right edge, the following window slides to the right with a stride rate represented as s, which is typically set to 1. Then, using the same stride value s, it bounces down to the image's (left) beginning and continues the procedure until the entire image has been traversed. Consequently, following the evolution, the result will be a sizeable two-dimensional array given in equation (10).

$$\frac{v-m+1}{s} \times \frac{h-n+1}{s} \tag{10}$$

Furthermore, a three-dimensional array may be used as the input, and many filters could be included in the same layer. For instance, if it had k filters with size $m \times n$ for a 3D array of size $v \times h \times d$ and assumed a stride of s, the outcome array would have the following shape in equation (11).

$$\frac{v-m+1}{s} \times \frac{h-n+1}{s} (d_k) \tag{11}$$

3.4.1 Quantum Convolutional Layer

The filter is rebuilt in our QC layer to utilise the parametric quantum circuit, also known as a quantum filter. Windows of shape $m \times n$ are mapped into quantum states using a quantum filter $|\varphi_i(P_{p:(a+m-1),q:(q+n-1)})$ of $N = mn$ qubits using $|\varphi_i(P_{p:(a+m-1),q:(q+n-1)})$ and then uses the parametric quantum circuit $C(\theta)$ to evolve the quantum stage until the output quantum state φ_o given in equation (12)

$$|\varphi_o\rangle = C(\theta)\,|\varphi_i(P_{p:(a+m-1),q:(q+n-1)}) \tag{12}$$

The feature map may be expressed as follows after you take the expectation rate of the observable $Z^{\otimes N}$ after the evolution given in equation (13).

$$P_{p:(p+m-1),q:9q+n-1)} \to \langle \varphi_o | Z^{\otimes N} | \varphi_o \rangle \tag{13}$$

Since equation (13) is nonlinear, it may directly introduce nonlinearity in the quantum convolutional layer without the requirement for an extra nonlinear function like ReLU. Equation (13) makes it abundantly evident that, in our method, the minimum quantity of qubits needed is the same as the window size. These qubits could be repurposed for our quantum convolutional layer's subsequent window. Because it requires only a small number of qubits and does not require the additional use of quantum RAM (qRAM), the QC layer is thus experimentally friendly and suited for Noisy Intermediate-Scale Quantum (NISQ) scenarios. The cross-correlation inside each window may be more accurately captured by the quantum correlational measurement.

3.4.2 Pooling and Fully Connected Layers

Since they can further induce nonlinearities and are computationally inexpensive, our framework retains the pooling layers and the last fully linked layer in the same manner as CNN.

3.4.3 Parametric Quantum Circuit

Single- and two-qubit layers are interleaved in the parametric quantum circuit. A parametric quantum circuit's total number of gate operations, represented by L, only increases polynomially with the count of qubits N; that is, $L \sim poly(N)$ gates, where L is the total number of gates. In our configuration, rotational y gates (R_y), which are given as follows, make up the single qubit layer and CNOT gates comprise the two-qubit layer given in equation (14).

$$R_y(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \tag{14}$$

A parametric quantum circuit has a total number of parameters equal to the sum of the window size and the circuit depth. For optimisation problems, the gradient of the loss function is frequently helpful. The simplest approach for calculating this gradient is the finite difference method. An input quantum state on a square lattice of n qubits, for example, can be trained using quantum input data. the QCCNN architecture can be modified. The remainder of the design stays the same, but the quantum filter can operate directly on each sub-lattice without the need for a classical-to-quantum encoding phase.

By following these steps, the intrusion has been detected and classified from the feature extracted data

3.6 Optimizing the parameters of HQCCNN using Aphid Ant Mutualism Optimization Algorithm (AAMOA)

Inspired by aphids and ants' mutualistic relationship, the Aphid-Ant Mutualism Optimisation Algorithm (AAMOA) improves both exploration and exploitation skills during the optimisation process. The following describes how to use AAMOA to optimise a QCCNN hyperparameters to improve the accuracy and reduce the loss. The Algorithm 1 explains the optimization process.

Algorithm 1

Step 1 : Initialization

Creating an initial population of binary vectors representing various hyperparameter settings for the HQCCNN.

$X = X_1, X_{2.....} X_D$

Step 2: colonies generation

Divide the population into three colonies: First colony, Second colony, Third Colony

Step 3: Individuals' Update using Ringleader

update positions using the ringleader's position

Step 4: Individuals' Update using male

update positions using the male's position

Step 5: Individuals' Update Using Ant's Head

update positions using the ant's head

Step 6 : Individuals' Flight

Random Flight: Some aphids perform a flight to explore new areas

Step 7: Binarizing the Positions

Binary Conversion: Convert the continuous positions to binary vectors

Step 8: Cross-over Operator

Cross-over: Perform random cross-over between individuals of different colonies

Step 9: Fitness Evaluation

Evaluate each individual's fitness

$$Fitness = w1 * ER * w2 * \frac{|S|}{|O|}$$

Step 10: Termination

Terminate the optimization process when the maximum number of iterations is reached

This procedure incorporates both global and local search mechanisms inspired by natural mutualism, enhancing the optimization of hyperparameters for HQCCNNs. By iterating through these steps, AAMOA seeks to find the optimal hyperparameters that improve the accuracy and reduce the error of the HQCCNN.

4. RESULT AND DISCUSSION

The results and discussion of the CCMM SMT-QCCN-AAO strategy are presented in this section, the CCMM SMT-QCCN-AAO approach is tested on the Windows 10 platform and verified in the NS3. The Table 1 gives the Execution parameter.

Table 1: Execution parameter

Parameter	Value
No of nodes	62
Simulation time	20sec
BS position	Variable
Topology size	800x800 m^2
Node distribution	Nodes are randomly distributed

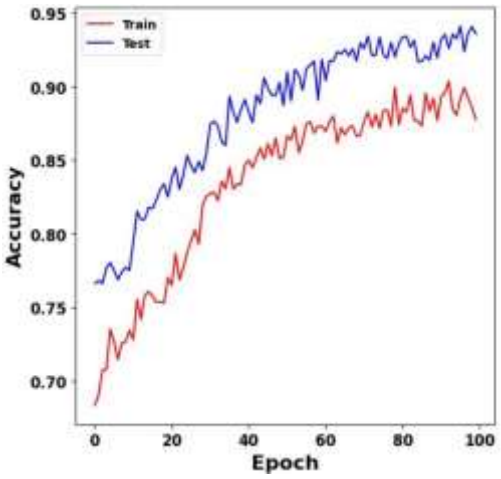

Figure 2: Accuracy validation

Figure 2 shows the 99.9% accuracy WSN-DS dataset training accuracy performance analysis. Training accuracy measures the efficacy of the approach on the training set and gives valuable information about the rate at which the model processes the information it has encountered.

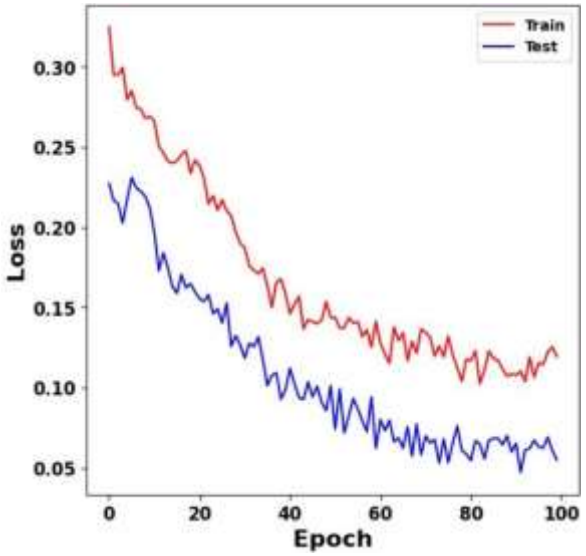

Figure 3: Loss Validation

A representation of the Loss function for the WSN-DS dataset can be found in Figure 3. It is essential to consider the loss function as an indicator of the efficiency of the model at training. When the loss function value is smaller, it indicates that the model is performing with greater efficiency.

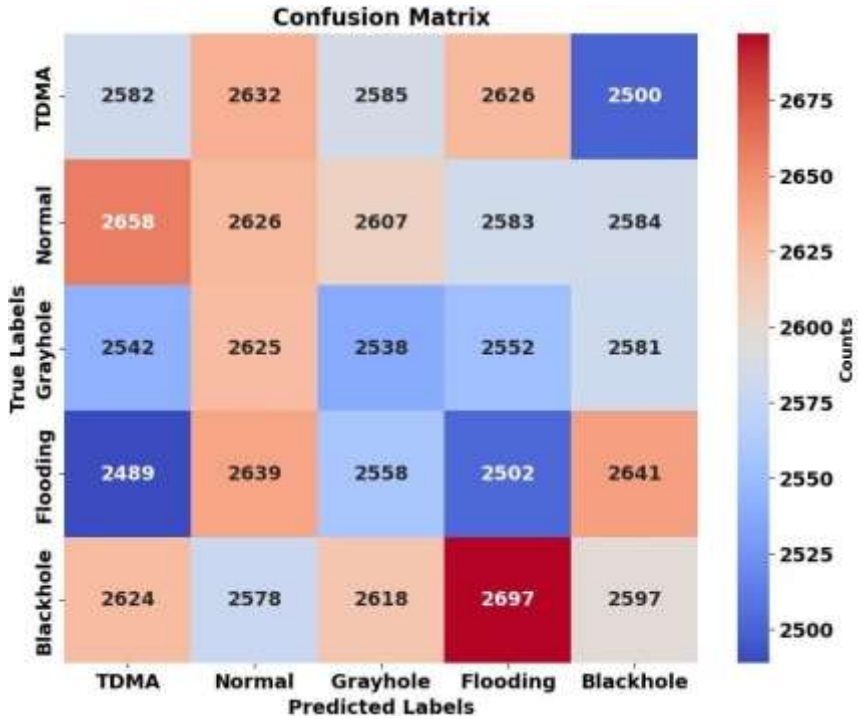

Figure 4: Confusion matrix

Figure 4 shows the performance validation of the confusion matrix for the WSN-DS dataset. The suggested technique performs remarkably well in identifying genuine cases and minimising errors across all datasets, as confirmed by the confusion matrix analysis. This leads to great performance overall in medical picture identification as well as high precision, recall, and accuracy.

4.1 Performance Analysis

The effectiveness of the proposed CCMM SMT-QCCN-AAO method can be evaluated by contrasting it with a number of existing techniques, including CBWSN_VSEMLA [16], SCNN-Bi-LSTM [17], DHN-SCA [18], and ELM-TSAO [19]. This examination aims to assess the analysis of the proposed CCMM SMT-QCCN-AAO method as well as effectiveness metrics such as error rate, recall, f1-score, accuracy, precision, and specificity.

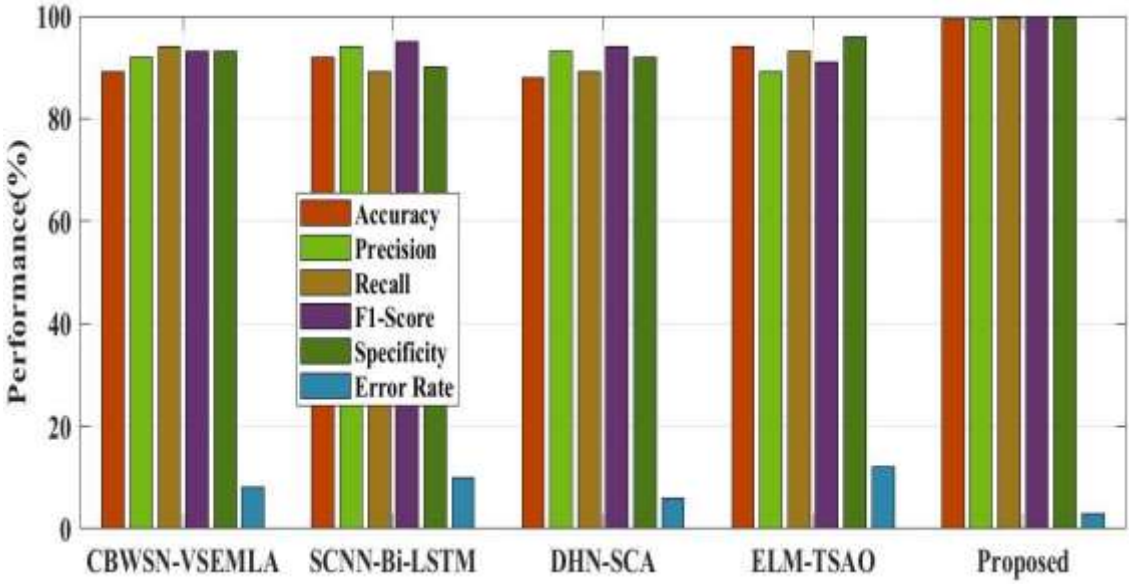

Figure 5: Comparative performance analysis

The accuracy, f1-score, recall, precision, specificity and error rate effectiveness analysis for WSN-DS dataset are displayed in figure 5. The proposed CCMM SMT-QCCN-AAO method performed 99% well across these measures for the WSN-DS dataset. When compared to the previous approaches, the proposed CCMM SMT-QCCN-AAO method earned best performance in all metrics. Table 2 gives the overall effectiveness comparison.

Table 2: Overall effectiveness comparison

Methods	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F-score (%)	Computational time (ms)
CBWSN_VSEMLA	88.82	84.294	83.691	82.691	83.48	127
SCNN-Bi-LSTM	95.83	94.35	92.85	94.85	94.59	128
DHN-SCA	93.39	88	88	88	89.45	75

ELM-TSAO	97.73	94.19	96.90	96.90	96.76	83
proposed	99.671	99.663	99.663	99.667	99.663	49

5. CONCLUSION

This work presented a novel Correlation coefficient min-max Scale Modulation Transformer based Quantum Classical Convolutional Network with Aphid-Ant Optimization (CCMM SMT-QCCN-AAO) for intrusion detection. First, the pre-processing function is applied to the input WSN-DS dataset by removing the noise characteristics using (CCMMW). The Scale Aware Modulation Meet Transformer (SAMMT) was then used to extract the intrusion-based features for additional detection and classification. Subsequently, the Hybrid Quantum Classical CNN model's parameters are optimized using the innovative Aphid-Ant Optimization Algorithm (AAOA) in order to lower the error rate, decrease computing time and complexity, and raise classification accuracy. Additionally, Hybrid Quantum Classical CNN (HQCCNN) is used for the successful detection and classification of WSN-DS classes like Blackhole, Flooding, Grayhole, Normal, and TDMA. From the obtained results, it is observed since the CCMM SMT-QCCN-AAO model performs better than the existing methods by providing improved accuracy of 99.67%, precision of 99.6%, recall of 99.6%, specificity of 99.67% and f1-score of 99.6%. In future, Investigate adaptive defense strategies that can dynamically adjust to changing network conditions and evolving cyber threats.

REFERENCES

1. Aileni RM, Suciu G, Serrano M, Maheswar R, Valderrama Sakuyama CA, Pasca S. The perspective of smart dust mesh based on ioee for safety and security in the smart cities. Integration of WSN and IoT for smart cities. 2020:151-79.
2. N.Anil Kumar, Y.Sukhi, M.Preetha, K.Sivakumar "Ant Colony Optimisation With Levy Based Unequal Clustering And Routing (ACO-UCR) Technique For Wireless Sensor Networks", Journal of Circuits, Systems, and Computers, ISSN: 0218-1266 (print); 1793-6454 (web) Vol .33, Issue3, July 24, 2023. DOI: 10.1142/S0218126624500439
3. Kumar S, Mishra A, Dutta A, Raj A. Collaboration of IoT and Cloud Computing Towards Healthcare Security. InPredictive Analytics in Cloud, Fog, and Edge Computing: Perspectives and Practices of Blockchain, IoT, and 5G 2022 Dec 17 (pp. 1-22). Cham: Springer International Publishing.
4. M.Preetha, K.Sivakumar "An Energy Efficient Sleep Scheduling Protocol for Data Aggregation in WSN,"in the Taga Journal of Graphic Technology Vol.14, PP: 404-414, 2018. Print ISSN 1748-0337, Online ISSN 1748-0345*
5. Lallie HS, Shepherd LA, Nurse JR, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security. 2021 Jun 1;105:102248.
6. N. Mohana Priya, G. Amudha, M. Dhurgadevi, N. Malathi, K. Balakrishnan & Preetha, M. (2024), "IoT and Machine Learning based Precision Agriculture through the Integration of Wireless Sensor Networks", Journal of Electrical Systems (IES), ISSN: 1112-5209, Vol.20, Issue 4, page No- 2292-2299.
7. Shetty T, Negi S, Kulshrestha A, Choudhary S, Ramani S, Karuppiah M. Blockchain for intrusion detection systems. InBlockchain Technology for Emerging Applications 2022 Jan 1 (pp. 107-136). Academic Press.
8. E.S. Phalguna Krishna, N. Praveena, I. Manju, N. Malathi, K. Balakrishnan, & Preetha, M. (2024), "IoT-Enabled Wireless Sensor Networks and Geospatial

Technology for Urban Infrastructure Management", Journal of Electrical Systems (IES), ISSN: 1112-5209, Vol.20, Issue 4, page No- 2248-2256.

9. Azam Z, Islam MM, Huda MN. Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree. IEEE Access. 2023 Jul 18.
10. M. Preetha, D. Dhabliya, Z. A. Lone, S. Pandey, K. Acharjya and G. J, "An Assessment of the Security Benefits of Secure Shell (SSH) in Wireless Networks," 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/SMARTGENCON60755.2023.10442244.
11. Aldarwbi MY, Lashkari AH, Ghorbani AA. The sound of intrusion: A novel network intrusion detection system. Computers and Electrical Engineering. 2022 Dec 1;104:108455.
12. D. Mondal, N. Thangarasu, Preetha. M, Y. S. Ingle, A. Saxena and J. R. R. Kumar, "Investigating the Effectiveness of Internet Key Exchange (IKE) Protocol in Wireless Network Security," 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/SMARTGENCON60755.2023.10441857.
13. Awotunde JB, Misra S. Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks. InIllumination of artificial intelligence in cybersecurity and forensics 2022 Feb 8 (pp. 21-44). Cham: Springer International Publishing.
14. Dr.M.Preetha, Balaji Singaram, Dr.I. Manju, B.Hemalatha, P. Bhuvaneswari "Machine Learning in Breast Cancer Treatment for Enhanced Outcomes with Regional Inductive Moderate Hyperthermia and Neoadjuvant Chemotherapy" Nanotechnology Perceptions, ISSN 1660-6795 2024, Vol: 20, 5s, 245-259.
15. Balaji Singaram, M.S.Vinmathi, Dr.H.B.Michael Rajan, Jeyamohan H, T. Manikandan, "Data-Driven Estimation of Lithium-Ion Battery State-of-Health Prediction Approach Using Machine Learning Algorithm for Enhanced Battery Management Systems", Nanotechnology Perceptions, ISSN 1660-6795 2024, Vol: 20, 7s, 93-103
16. John A, Isnin IF, Madni SH, Faheem M. Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms. Intelligent Systems with Applications. 2024 Jun 1;22:200381.
17. Bukhari SM, Zafar MH, Abou Houran M, Moosavi SK, Mansoor M, Muaaz M, Sanfilippo F. Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks. 2024 Mar 15;155:103407.
18. Gatate V, Agarkhed J. Enhancing intrusion detection in wireless sensor networks through deep hybrid network empowered by SC-attention mechanism. Iran Journal of Computer Science. 2024 Mar 10:1-2.
19. Ravindra C, Kounte MR, Lakshmaiah GS, Prasad VN. Etelmad: anomaly detection using enhanced transient extreme machine learning system in wireless sensor networks. Wireless Personal Communications. 2023 May;130(1):21-41.
20. Srinivasan, S, M.S. Vinmathi, S.N. Sivaraj, A. Karthikayen, C. Alakesan, & Preetha, M. (2024), "A Novel Approach Integrating IoT and WSN with Predictive Modeling and Optimization for Enhancing Efficiency and Sustainability in Smart Cities", Journal of Electrical Systems (IES), ISSN: 1112-5209, Vol.20, Issue 4, page No- 2228-2237.

21. Balaji Singaram, Lakshmi. B, Dr.M.Preetha, V.K. Ramya Bharathi, Dr.S.Muthumari lakshmi, Rakesh Kumar Giri "A Smart IoT-Based Fire Detection and Machine Learning Based Control System for Advancing Fire Safety",Nanotechnology Perceptions, ISSN 1660-6795 2024, Vol: 20, 5s, 229-244.
22. Ejegwa PA, Jana C. Some new weighted correlation coefficients between Pythagorean fuzzy sets and their applications. Pythagorean Fuzzy Sets: Theory and Applications. 2021:39-64.