Advances in Consumer Research
ISSN (Print): 0098-9258
ISSN(Online): 3079-1766

Vol. 2, Issue 4 (2025) https://acr-journal.com/

Securing the Internet of Things with Quantum Feedforward Neural Networks and Contextual Rule Based Signature Detection

Suja Cherukullapurath Mana[1], Bhuvanesh Unhelkar[2], Siva Shankar Subramanian[3], G Nagarajan[4]

[1]Post Doctoral Researcher, Information Systems and Decision Sciences, University of South Florida (USF),8350N. Tamiami Trail Sarasota, Florida, USA.

Email ID: cmsuja@gmail.com

[1]Department of CSE, PES University, Bengaluru, India,560100

[2]Professor, Information Systems and Decision Sciences, University of South Florida,8350N. Tamiami Trail Sarasota, Florida, USA.

Email ID: bunhelkar@usf.edu

[3]Departmentof CSE, KG Reddy College of Engineering and Technology, Moinabad, Telangana, India–501504

Email ID: drsivashankars@gmail.com

[4]Department of CSE, Sathyabama Institute of Science and Technology, Chennai, India,603100

Email ID: gnagarajan.cse@sathyabama.ac.in

Cite this paper as: Suja Cherukullapurath Mana, Bhuvanesh Unhelkar, Siva Shankar Subramanian, G Nagarajan, (2025) Securing the Internet of Things with Quantum Feedforward Neural Networks and Contextual Rule Based Signature Detection. *Advances in Consumer Research*, 2 (4), 1494-1509

KEYWORDS

Internet of Things (IoT), Security, Quantum Feedforward Neural Networks, Contextual Signature Detection, Intrusion Detection System, Network Anomaly Detection, Cybersecurity.

ABSTRACT

In the constantly evolving field of information management systems, ensuring appropriate security measures to prevent cyber invasions is of paramount significance. The dynamic and complex nature of contemporary cyberthreats, especially in the context of the Internet of Things (IoT), frequently proves too much for traditional intrusion detection systems (IDS). The current study emphasises on the difficulties of achieving high precision and real-time speed while maintaining data confidentiality. This study presents an new structure that combines Quantum Feedforward Neural Networks (QFNNs) with Contextual Rule-based Signature Detection (CRSD) to enhance IoT security. QFNNs leverage the principles of quantum computation to proficiently handle high-dimensional IoT network data, resulting in important improvements in detection speed and accuracy. Meanwhile, the Contextual Signature Detection module dynamically adjusts detection processes based on contextual parameters, such as device behavior, network traffic patterns, and temporal fluctuations, ensuring flexible and precise threat identification. The proposed QFNNs were assessed utilizing IoT intrusion datasets and established greater presentation related to conventional neural networks and standard signature-based methods. The findings indicate notable developments in detection accuracy, a decrease in false positives, and developed adaptability to evolving threats. By integrating the computational advantages of quantum neural networks with the adaptability of contextual rule-based detection, this method proposals a scalable and resilient solution for safeguarding IoT networks.

1. INTRODUCTION

The frequency of IoT based attacks, most often those beginning with botnets, has increased in parallel with the use of IoT devices. Botnets signify the most common and severe type of cyberthreat [1] because they are used by remote attackers to infect IoT devices with malware [2]. Thus, enhancing effective strategies to categorize such threats has emerged as crucial because of the fast rate of attacks and the evolution of the approaches used by attackers. Since the emergence of malware, the utilize of machine learning (ML) and deep learning (DL) methods leveraging full-time sequence data has increased dramatically. However, important shortcomings exist in present tools that important be addressed, and existing methods need improvements to efficiently detect and mitigate the threat of botnet attacks on IoT devices [3].

Current developments in hybrid artificial intelligence (AI) approaches have recognized significant potential for improving IoT security. To progress detection models for IoT risks, such as botnets, numerous studies have recommended connection DL with evolutionary procedures [4]. These hybrid AI methods hold promise for striking a balance among detection accuracy and processing efficiency in resource-constrained IoT environments. One essential element in the fight against botnet threats is an intrusion detection system. By leveraging AI, IDSs can classify new kinds of botnet threats. IDS approaches are typically separated into two types: misuse-based approaches that rely on pre-existing signatures and anomaly-based approaches. Various IDSs, such as Snort and Suricata, are available and container mitigate the impact of botnet attacks. These analysis approaches examine malware behavior in specific contexts [5]; this knowledge is mainly useful for DL and ML procedures, which must continuously gather sequence data as the malware operates. In certain scenarios, these methods can uncover how the virus causes method damage [6]. Following a Distributed Denial of Service (DDoS) attack executed by an IoT botnet, organization approaches that learn from prior attacks can help the model more efficiently identify DDoS threats and botnet methods within the same environments [7].

AI methods are presently being utilized to detect IoT hazards due to their increasing detection abilities and capability to diagnose evolving patterns in threat mitigation strategies [8]. However, the removal of IoT risks faces several challenges, including the emergence of new variants of well-known attacks that are more problematic for security methods to detect. To address these challenges, DL and ML have been integrated into security devices to progress their presentation. Recent works have examined the use of AI solutions to improve threat identification in the IoT surroundings [9]. In addition, the mixed AI methods have proven their effectiveness in the improvement of feature selection and model presentation. For example, the current studies display that the integration of QFNNs with CRSD and DL is effective in the dissimilarity diagnosis of IoT networks [10]. DL is one of the important advancements in AI mainly beneficial for a range of practical applications to address challenging and non-linear data.

1.1 Research of our work

This research proposed a novel method to deal with the security issues in IoT network. By incorporating QFNN which takes advantage of the parallel computation capabilities of quantum computing the method is able to accomplish fast and accurate anomaly detection. In addition, a Contextual Rule-based Signature Detection mechanism is employment to identify and respond to threats by utilizing rules and context analysis. When combined, these methods advance the precision and effectiveness of IoT security systems while providing the capacity for large-scale IoT systems, although maintaining an effective defense against novel and sophisticated cyber threats.

1.2 Motivation of this research

The motivation for this research rises as the novel vulnerabilities in IoT methods emerge due to the rising usage and interconnectivity of IoT. It is a problematic that conventional security solutions cannot effectively solve the complexity and the nature of threats in IoT devices. To address this, we introduce QFNNs together with Contextual Rule-based Signature Detection to enhance the security of IoT. The quantum feature nodes of QFNNs create utilize of quantum calculating to procedure data effectively and to identify inconsistencies in a more effective way, while the rule based detection method provides a reliable way to identify known threats. This method is meant to provide an efficient, self-organizing and predictive security method to protect IoT systems from emerging threats.

1.3 The major contributions of this paper:

- To develop an innovative structure that merges Quantum Feedforward Neural Networks (QFNNs) with Contextual Rule-based Signature Detection (CRSD) to improve IoT security.
- QFNNs leverage important calculation concepts to efficiently handle high-dimensional IoT system data, leading to growths in together detection speed and accuracy.
- Finally QFNNs take been evaluated using IoT intrusion datasets and have demonstrated significantly higher presentation connected to conventional neural networks and standard signature-based methods.

1.4 Structure of Our Article

The remaining of the article is organized as follows: Section 2 offerings a detailed literature survey, followed by a explanation of the proposed method in Section 3. Section 4 presents the results section, while Section 5 concludes the article and outlines future work.

2. SURVEY

The IoT has transformed modern technology by allowing seamless connectivity between devices, systems, and services. Conversely, the rapid proliferation of interconnected devices also offerings important security challenges, including vulnerabilities to cyberattacks, data breaches, and privacy violations. This survey inspects new improvements, challenges, and emerging trends in IoT security, with a specific focus on authentication mechanisms, encryption protocols, intrusion diagnosis systems, and secure communication constructions. By addressing these critical problems, the survey aims to

proposal a whole overview of approaches to safeguard IoT methods, confirming reliable and resilient operations in an increasingly related world.

Convolutional neural networks (CNNs) were recommended by Abu Al-Haija et al. [11] as the basis for generating a new, intelligent, and self-governing deep learning-based technique for identifying and categorising cyberattacks in Internet of Things communication networks. For effective parallel processing and fast calculation, their recommended method, the Internet of Things Intrusion Detection and Categorisation System using CNN (IoT-IDCS-CNN), creates utilize of powerful Intel i9-core CPUs and Nvidia GPUs utilizing Compute Unified Device Architecture (CUDA). The proposed IoT-IDCS-CNN was measured using all of the most significant IoT-based attacks since the Network Security Laboratory-Knowledge Discovery Databases (NSL-KDD) dataset. Allowing to the simulation outcomes, the binary-class classifier's cyberattack association accuracy was over 99.3%, while the multiclass classifier's was over 98.2%.

DL-based Early Stage Detection (DL-ESD) is a novel method created by Albishari et al. [12] utilising the IoT Routing Attack Dataset (IRAD) to improve routing attack detection. It integrates version number (VN), decreasing rank (DR), and hello flood (HF). The suggested model's training efficiency was evaluated utilizing binary organization approaches. Outperforming state-of-the-art studies, the method achieved 98.85% prediction accuracy, 97.50% precision, 98.33% recall, and a 97.01% F1-score.

A new hierarchical adversarial attack generation method for GNN-based intrusion detection systems (IDS) in Internet of Things environments was presented by Zhou et al. [13]. By slightly altering critical components in the feature space, identified using salient graph technology, this method generates adversarial samples. To determine which IoT nodes were most vulnerable to assaults, a hierarchical node selection technique founded on random walks was also used. When these two techniques are combined, the detection accuracy of two cutting-edge GNN models decreases by 30%.

An intrusion diagnosis system based on the Transformer model was proposed by Wang et al. [14]. This system learns contextual embeddings of network features through a self-attention mechanism, enabling it to handle together continuous and categorical features simultaneously. On the Tonne IoT dataset, the system demonstrated strong performance, succeeding an accuracy of 95.78% for multi-class organization and 97.95% for binary organization.

Aktar and Nur [15] developed an automated botnet detection and organization algorithm for anomaly detection using the Rat Swarm Optimizer with Deep Learning (BDC-RSODL). The Rat Swarm Optimizer (RSO) technique is employed to identify features and pre-process network data. The RSO technique's capacity to handle high-dimensional data may limit this method's performance, even though it decreases the feature space and increases efficiency. Another powerful tool for identifying botnets is the Long Short-Term Memory (LSTM) methodology.

Shukla et al. [16] introduction an RNN-FET model to analyze data and improve features by integrating FET with bidirectional LSTM. While this approach improves temporal feature analysis, the use of bidirectional LSTM can be computationally expensive and requires longer training time, especially in large-scale IoT networks. Despite the extremely high detection accuracy of these DL-based methods, their computational complexity may prevent them from being used on IoT devices with limited resources, which frequently call for lightweight solutions.

To identify anomalies in real-time network traffic, Thota and Menaka proposed a method [17]. Their research used common criteria to distinguish between different DL and ML algorithms for botnet detection prior to analysing recently extracted packet-captured (pcap) files because the Aposemat IoT 23 dataset used gated recurrent units (GRUs) to identify malware threats. While this approach offers accurate threat diagnosis, its applicability to other types of attacks in IoT networks has not been thoroughly explored.

Abdulkareem et al. [18] suggested a lightweight technique for diagnosis IoT network attacks. Their method reduced feature dimensionality by selecting eight key features using a filter strategy. A stacked ensemble learning model consisting of decision tree (DT), logistic regression (LR), and naïve Bayes (NB) was then trained using these structures, with the DT acting as the meta-learner. This technique succeeded an accuracy of 90.65% in identifying five different types of IoT network attacks.

2.1 Research Gap

The research gap in enhancing IoT security lies in addressing the increasing vulnerabilities of IoT devices as they proliferate across diverse applications, ranging from smart homes to critical infrastructure. Existing solutions often focus on isolated aspects, such as data encryption or access control, but fail to provide comprehensive, lightweight, and scalable security frameworks tailored to resource-constrained IoT devices. However, current approaches do not address the issue of adaptability to new threats and risks including those involving the use of artificial intelligence and zero-day threats. The current situation requires new comprehensive approaches based on the latest technologies, such as machine learning, blockchain, and real-time anomaly detection to achieve comprehensive and preventive IoT security.

3. PROPOSED SYSTEM

The complexity and dynamic nature of contemporary cyberthreats, particularly inside the Internet of Things environment, make it difficult for conventional intrusion detection systems (IDS) to handle, as this study demonstrates. The challenges of

guaranteeing high precision and real-time performance while maintaining data secrecy are highlighted by the expanding body of research. To address these challenges, this paper presents an innovative framework that integrates QFNNs - CRSD to enhance IoT security.

Fig.1 illustrates the block diagram of the proposed model. The proposed diagram outlines a comprehensive IoT security framework aimed at enhancing protection against cyber threats. IoT devices, such as PCs, mobiles, and smart home systems, communicate with cloud computing and social media services, producing large amounts of data. However, attackers attempt to exploit susceptibilities in the IoT network. The data collected is pre-processed to safeguard quality and readiness for analysis. The QFNNs - CRSD form the core security mechanism, analyzing the data to detect anomalies and malicious activity. Finally, the system classifies threats, ensuring effective identification and mitigation of cyberattacks, safeguarding the IoT ecosystem.

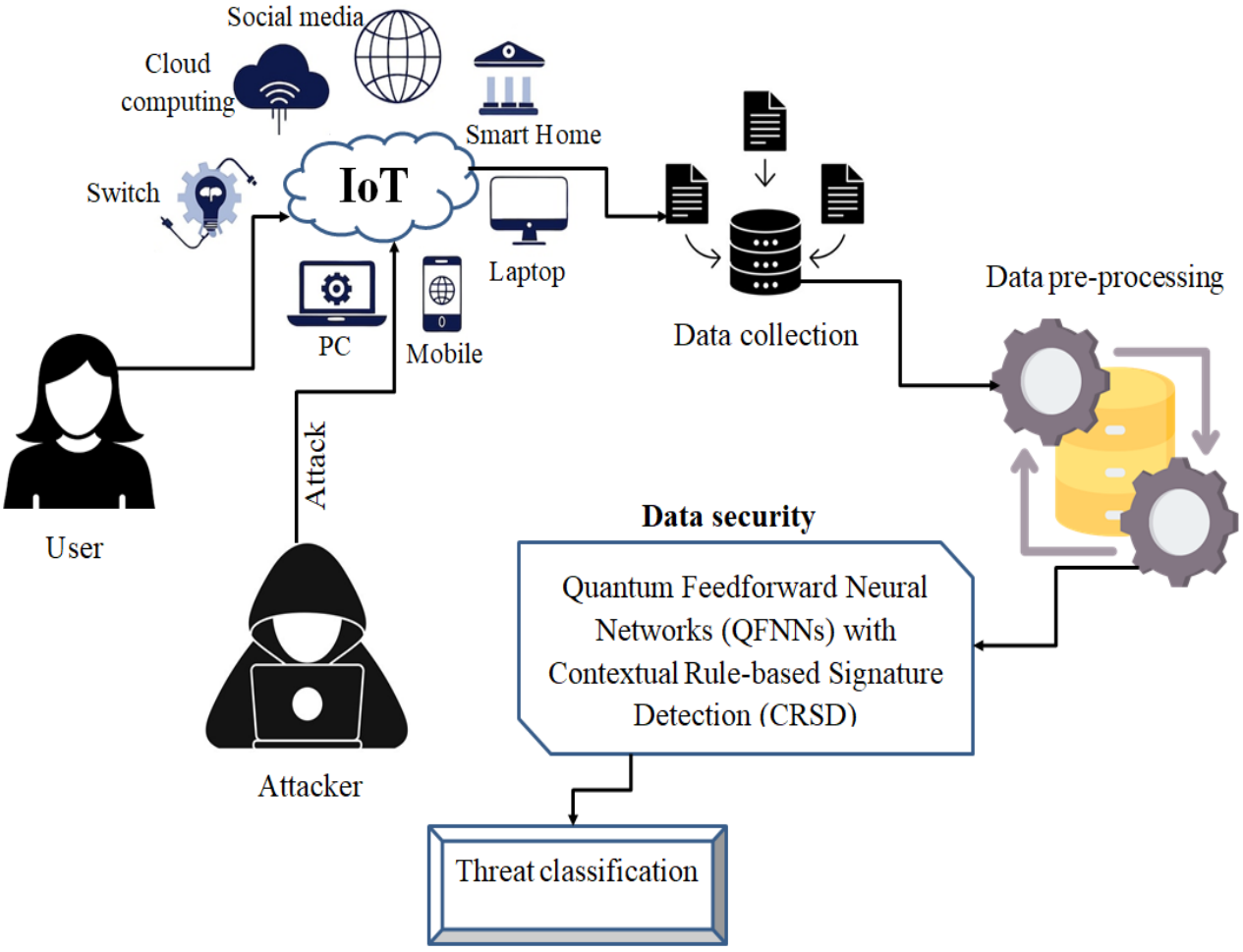

Figure 1: Block diagram of proposed technique

3.1 Dataset

The Australian Centre for Cyber Security's (ACCS) Cyber Range Lab's IXIA PerfectStorm tool produced the raw network packets that make up the UNSW-NB15 dataset. This dataset combines real, contemporary daily routines with synthetic, modern attack behaviors. Reconnaissance, shellcode, fuzzers, DoS, backdoors, worms, and exploits are among the nine attack methods that are included. Twelve algorithms were developed to produce the class label and 49 attributes using the Argus and Bro-IDS tools. Four CSV files include 2,540,044 records in total, of which 175,341 are in the training set and 82,332 are in the testing set [19]. Numerous research projects have made extensive use of the dataset for intrusion detection, privacy protection, threat intelligence, and network forensics across a variety of systems, such as SCADA, Industrial IoT, Network Systems, IoT, and Industry 4.0.

3.2 Preprocessing

For classification, the type of normalization must be preprocessed. The input data is normalized to accelerate the learning process. Data normalization could be necessary to handle numerical issues like accuracy loss from arithmetic errors. those with wide beginning ranges have the potential to dominate gradients, obscuring those with lesser ranges [20]. Feature space

normalizations is better understood as a kernel-based preparation method rather than a preprocessing step because it is not applied externally to input vectors. The gap between the greatest and smallest values in a typical attack, for example, can be as much as nine or 10 times in certain intrusion detection datasets. In this regard, normalizations functions as a special kernel mapping method that simplifies calculations by transforming data onto a more manageable plane. However, because so many data points are involved, sophisticated normalizations techniques can be computationally costly. This Min-Max normalizations technique is quick and effective. Min-Max standardization linearly converts the actual information m into the desired interval $\left(\max_{new}, \min_{new}\right)$.

$$m = \min_{new} + \left(\max_{new} - \min_{new}\right) * \left(\frac{m - \min_x}{\max_x - \min_x}\right) \quad (1)$$

The technique's accuracy in preserving all relationships among the data points is one of its advantages. It does not distort the data in any way.

3.3 Quantum Feedforward Neural Networks (QFNNs)

The Internet of Things (IoT) faces increasing security challenges due to its distributed architecture and limited computational resources. Modern security mechanisms often struggle to balance robust protection with efficiency. QFNNs recommendation a novel method to developing IoT security by leveraging quantum computing principles for anomaly detection, encryption, and threat mitigation. QFNNs integrate quantum operations into the structure of classical feedforward neural networks, harnessing quantum parallelism and entanglement to rise computational effectiveness and accuracy [21]. These networks are mainly effective for real-time IoT security tasks, such as diagnosis anomalies in system traffic, classifying malicious nodes, and management secure communications.

Quantum State Representation: QFNNs encode classical data into quantum states to enable parallel processing. The quantum state $|\psi\rangle$ of n -qubits is denoted as Eq.(2):

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \quad (2)$$

Where α_i are complex amplitudes satisfying $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$.

Quantum Gate Operations: Quantum gates transform input quantum states. For example, a single-qubit gate U acting on $|\psi\rangle$ modifies the state as Eq.(3):

$$U|\psi\rangle = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad (3)$$

Forward Propagation: QFNNs apply quantum gates to simulate classical feedforward layers. For a layer l, the quantum state transformation is in Eq.(4):

$$|\psi^{(l+1)}\rangle = U^{(l)} |\psi^{(l)}\rangle \quad (4)$$

Where $U^{(l)}$ represents the quantum gate operations corresponding to layer l.

Quantum Measurement: At the output layer, quantum measurement collapses the quantum state into classical probabilities. The probability of measuring state $|i\rangle$ is in Eq.(5):

$$P(i) = |\alpha_i|^2 \quad (5)$$

Loss Function: To optimize the QFNN, a cost function such as the Mean Squared Error (MSE) is adapted for quantum states in Eq. (6).

$$L = \frac{1}{m}\sum_{j=1}^{m}\left(P_j - y_j\right)^2 \quad (6)$$

Where P_j is the predicted probability and y_j is the true label.

Gradient Descent in Quantum Context: Parameter updates are performed using hybrid quantum-classical techniques.

$$\theta^{(t+1)} = \theta^{(t)} - \eta\frac{\partial L}{\partial \theta^{(t)}} \quad (7)$$

Where θ represents trainable parameters like rotation angles in quantum gates.

IoT Security Integration: For anomaly detection, the QFNN processes incoming IoT data streams encoded as quantum states. The outputs indicate whether a given data point deviates from normal behavior.

$$Anomaly\ \ Score = \sum_{i \in anomalous\ states} P(i) \quad (8)$$

QFNNs efficiently analyze large datasets, providing enhanced scalability and accuracy for IoT security applications. Future improvements in quantum hardware will further facilitate the real-time deployment of QFNN-based security systems.

3.4 Contextual Rule-based Signature Detection (CRSD)

CRSD is a security background designed to improve the protection of Internet of Things (IoT) devices by leveraging contextual information and rule-based signature detection mechanisms. This method associations traditional signature detection with contextual parameters (e.g., device type, operational environs, and communication patterns) to identify and mitigate security threats more effectively [22]. By incorporating context, CRSD increases the accuracy of intrusion detection systems (IDS), decreases false positives, and adapts to the dynamic nature of IoT environs.

Contextual Awareness: Uses environmental and device-specific data to refine detection rules.

Rule-based Mechanisms: Employments predefined rules to analyze IoT network traffic for malicious patterns.

Dynamic Signature Adaptation: Updates signatures based on new threat intelligence and contextual alterations.

Contextual Rule Representation:

A contextual rule R_i can be expressed as:

$$R_i = \{C_1, C_2, ..., C_m\} \quad (9)$$

Where C_k represents a contextual parameter such as:

- C_1 : Device type (e.g., sensor, actuator)
- C_2 : Network traffic characteristics (e.g., packet size, frequency)
- C_3 : Behavioral patterns (e.g., access time, usage frequency)

Signature Matching Function:

The signature detection estimates incoming network traffic T against a set of signatures S :

$$M(T,S) = \begin{cases} 1 & if\ T\ matches\ S \\ 0 & otherwise \end{cases} \quad (10)$$

Contextual Rule Evaluation:

The contextual rule detection function evaluates traffic T with contextual parameters $\{C_1, C_2, ..., C_m\}$ as:

$$D(T,\{C_k\}) = \begin{cases} 1 & if\ T\ satisfies\ all\ C_k \\ 0 & otherwise \end{cases} \quad (11)$$

CRSD Decision Function:

The CRSD combines signature matching and contextual rule evaluation to detect threats.

$$CRSD(T) = \begin{cases} 1\ if\ M(T,S)=1\ and\ D(T,\{C_k\})=1 \\ 0 \quad otherwise \end{cases} \quad (12)$$

Threat Scoring Function:

To rank potential threats, a threat score TS can be calculated as:

$$TS(T) = \sum_{k=1}^{m} w_k \cdot C_k(T) \quad (13)$$

Where w_k is the weight assigned to the importance of the k -th contextual parameter, and $C_k(T)$ indicates whether the context is satisfied.

By combining these equations, CRSD provides a robust and adaptive framework for IoT security. It not only detects threats using signatures but also incorporates contextual information to enhance detection precision and efficiency. Tab.1 shows the description of mathematical symbol.

3.5 Advantages of proposed method

- Utilizes QFNNs to process high-dimensional IoT data, enhancing precision in threat identification.
- CRSD dynamically adapts detection rules to contextual parameters, reducing erroneous alerts.
- QFNN's quantum-inspired computation accelerates processing, enabling faster response times.
- CRSD adjusts to evolving IoT behaviors and network patterns, ensuring flexible threat detection.

Table 1: Description of mathematical symbol

Symbol	Description
w_k	weight
$C_k(T)$	contextual parameter
TS	threat score
T	traffic
$\{C_1, C_2, ..., C_m\}$	contextual parameters
S	signatures
C_1	Device type
C_2	Network traffic characteristics
C_3	Behavioral patterns
R_i	contextual rule
θ	trainable parameters

P_j	predicted probability
y_j	true label
$\|i\rangle$	probability of measuring state
$U^{(l)}$	quantum gate
l	layer
U	single-qubit gate
α_i	complex amplitudes
$(\max_{new}, \min_{new})$	Min-Max normalization

4. RESULT AND DISCUSSION

4.1 Experimental setup

Initially, we used an HP notebook with an Intel Gen8 CPU and 12 GB of RAM to conduct the experiment for this study. Subsequently, for mobility, we transitioned the experiment to Google Colab. Python 3.10 was the programming language used, and the primary libraries utilized included easyfsl, sklearn, torch, numpy, pandas, matplotlib, and seaborn.

4.2 Performance Metrics

Specificity: The expected percentage of attractive instances is presented in Equation (14), which delivers the mathematical formula.

$$Spe = \frac{T_N}{T_N + F_P} \tag{14}$$

Sensitivity: It shows the percentage of cases that were probable to fail. Equation (15) contains the corresponding mathematical formula.

$$Sen = \frac{T_P}{T_P + F_N} \tag{15}$$

Accuracy: Eq. (16) provides a quantitative expression for the percentage of cases that the model correctly anticipated.

$$Acc = \frac{T_P + T_N}{T_P + F_N + T_N + F_P} \tag{16}$$

Precision: A metric called precision measures the percentage of positive class predictions that turn out to be accurate. Refer to Equation (17) for the mathematical formula.

$$\Pr ecision = \frac{T_P}{T_P + F_P} \tag{17}$$

F-measure: A single metric, called the F-single measure score, was created to achieve a balance between recall and precision constraints. Its mathematical formulation is presented in Eq. (18).

$$F1 = \frac{2T_P}{2T_P + F_P + F_N} \tag{18}$$

False Positive Rate: Equation (19) illustrates the following mathematical formula, which represents the percentage of cases that are incorrectly labelled as negative rather than positive:

$$FPR = \frac{F_P}{T_N + F_P} \quad (19)$$

False Negative Rate: Equation (20) provides a mathematical expression for the percentage of cases mistakenly classified as positive when they should have been negative.

$$FNR = \frac{F_N}{T_P + F_N} \quad (20)$$

Matthews's correlation coefficient (MCC): The MCC is one of the most commonly used measures for classification accuracy. It is widely regarded as a fair metric that can be used even in cases where class sizes differ significantly. Equation (21) provides the definition of MCC.

$$MCC = \frac{T_P T_N - F_P F_N}{\sqrt{(T_P + F_P) - (T_P + F_N)(T_N + F_P)(T_N + F_N)}} \quad (21)$$

Negative Positive Rate (FPR): It is the ratio of subjects who received a true negative diagnosis to all those who received a negative result. NPV represents the proportion of scenarios where every negative prediction was actually correct. Equation (22) provides the formula.

$$NPV = \frac{T_N}{T_N + F_N} \quad (22)$$

False Positive Rate (FPR): The percentage of benign cases that are incorrectly labelled as malicious is known as the FPR. It evaluates the tendency of a detection system to raise false alarms.

$$FPR = \frac{FP}{FP + TN} \quad (23)$$

False Negative Rate (FPR): The percentage of true positive cases (such as threats) that a detection system incorrectly classifies as negative (non-threats) is known as the False Negative Rate, or FNR. A high FNR indicates a failure to detect real threats, which could compromise system security.

$$FNR = \frac{FN}{FN + TP} \quad (24)$$

4.3 Comparative methods

QCCNN [23]: In terms of qubit count and circuit depth, QCNN outperforms contemporary noisy intermediate-scale quantum computers while preserving key characteristics of traditional CNNs, such as scalability and non-linearity.

GRU [24]: Only the acquired weights are shared with the aggregation server, ensuring the privacy of local IoT device data in GRU models.

CDW FedAvg [25]: In addition to implementing the CDW FedAvg technique, which considers the distance between positive and negative classes in each customer dataset, the proposed scheme ensures the accuracy of the customers' data.

Res-QCNN [26]: The Res-QCNN outperforms the current model in learning a unitary function and demonstrates resilience to noisy data.

Table 2: Comparative Analysis of Specificity and Sensitivity

Models	Specificity	Sensitivity
QCCNN	88.45	66.23
GRU	70.12	87.23
CDW FedAvg	78.34	69.91
Res-QCNN	74.81	88.61
Proposed	92.24	96.44

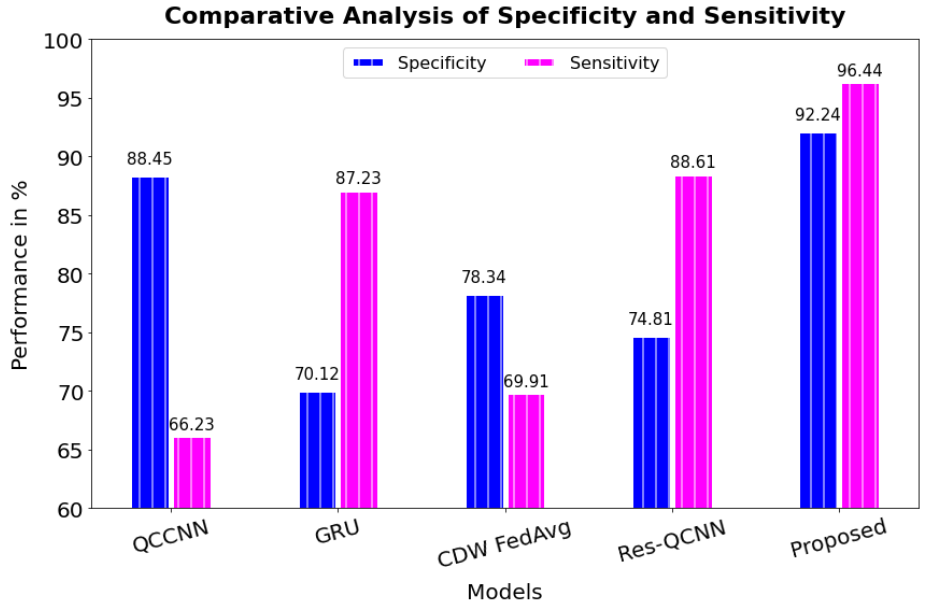

Figure 2: Comparative Analysis of Specificity and Sensitivity

The comparative analysis of various models reveals distinct differences in specificity and sensitivity, as presented in Tab.2 and Fig.2. The QCCNN model achieves a specificity of 88.45% but has a relatively lower sensitivity of 66.23%. The GRU model demonstrates a high sensitivity of 87.23% but exhibits lower specificity at 70.12%. The CDW FedAvg model provides balanced performance, with a specificity of 78.34% and a sensitivity of 69.91%. The Res-QCNN model performs well in sensitivity, achieving 88.61%, but its specificity is slightly lower at 74.81%. In contrast, the proposed method stands out with the uppermost specificity of 92.24% and an exceptional sensitivity of 96.44%, representing greater total performance.

Table 3: Comparative Analysis of Performance Metrics

Models	Precision	F-measure	Accuracy
QCCNN	81.98	62.91	87.34
GRU	73.26	68.95	91.65
CDW FedAvg	70.81	77.76	89.44
Res-QCNN	89.91	90.65	93.98
Proposed	93.45	94.54	98.91

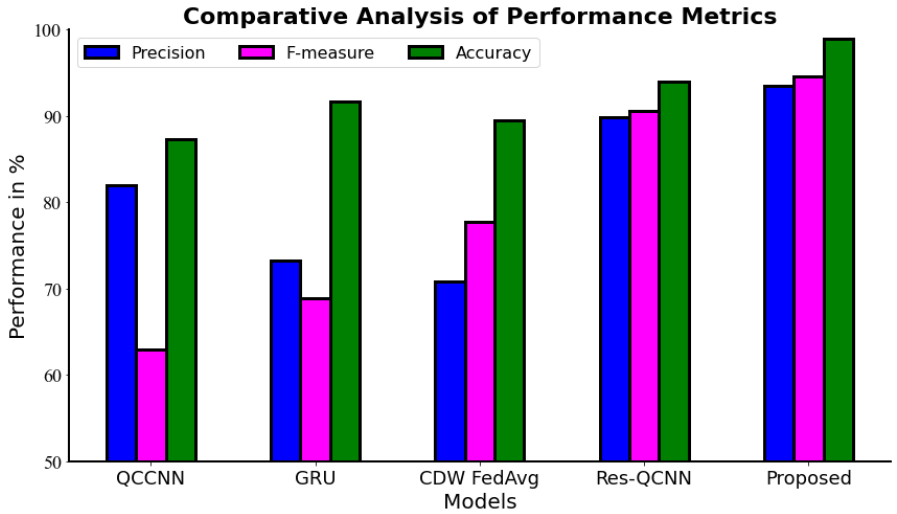

Figure 3: Comparative Analysis of Performance Metrics

The comparative evaluation of diverse models, highlighting their performance in terms of precision, F-measure, and accuracy, is presented in Tab.3 and Fig.3. The QCCNN model accomplishes a precision of 81.98%, an F-measure of 62.91%, and an accuracy of 87.34%. The GRU model establishes a higher accuracy of 91.65%, with a precision of 73.26% and an F-measure of 68.95%. The CDW FedAvg model exhibits an F-measure of 77.76%, a precision of 70.81%, and an accuracy of 89.44%. The Res-QCNN model excels in precision, reaching 89.91%, with an F-measure of 90.65% and an accuracy of 93.98%. The proposed model surpasses all others, accomplishing the highest precision of 93.45%, an F-measure of 94.54%, and an impressive accuracy of 98.91%, representing its greater overall performance.

Table 4: Comparative Analysis of FPR and FNR

Models	FPR	FNR
QCCNN	18.76	22.76
GRU	19.45	25.76
CDW FedAvg	20.55	26.91
Res-QCNN	23.25	20.54
Proposed	15.76	18.76

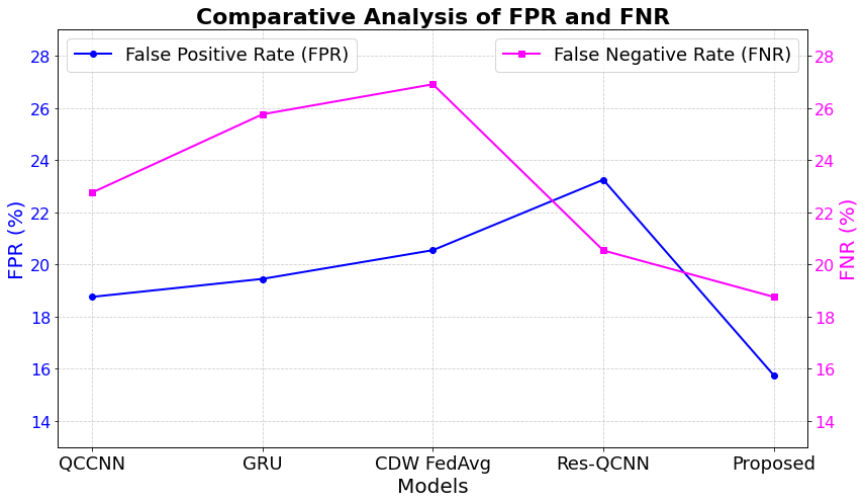

Figure 4: Comparative Analysis of FPR and FNR

Tab.4 and Fig.4 present a comparative analysis of models based on FPR and FNR, revealing varying levels of performance. The QCCNN model has an FPR of 18.76% and an FNR of 22.76%, while the GRU model shows slightly higher rates with an FPR of 19.45% and an FNR of 25.76%. The CDW FedAvg model performs likewise, with an FPR of 20.55% and an FNR of 26.91%. The Res-QCNN model exhibits a higher FPR of 23.25% but a lower FNR of 20.54%. Notably, the proposed model achieves the lowest FPR of 15.76% and FNR of 18.76%, standing out for its greater capability to reduction both false positives and false negatives.

Table 5: Comparative Analysis of MCC and NPV

Models	MCC	NPV
QCCNN	77.21	69.91
GRU	84.56	76.13
CDW FedAvg	88.99	80.45
Res-QCNN	92.34	83.45
Proposed	96.44	90.88

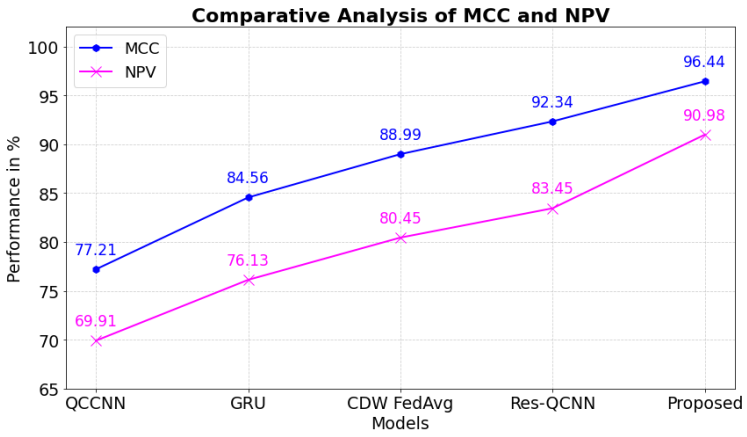

Figure 5: Comparative Analysis of MCC and NPV

Tab.5 and Fig.5 present the comparative evaluation of models based on MCC and NPV, highlighting notable differences in performance. The QCCNN model achieves an MCC of 77.21 and an NPV of 69.91%. The GRU model performs slightly better, with an MCC of 84.56 and an NPV of 76.13%. The CDW FedAvg model founds further improvement, accomplishing an MCC of 88.99 and an NPV of 80.45%. The Res-QCNN model excels with an MCC of 92.34 and an NPV of 83.45%. However, the proposed model outperforms all others, achieving the highest MCC of 96.44 and an NPV of 90.88, reflecting its exceptional predictive accuracy and reliability.

Table 6: Throughput Analysis of Proposed Method

Models	**Throughput**
QCCNN	876.76
GRU	956.33
CDW FedAvg	1276.65
Res-QCNN	1345.98
Proposed	1511.71

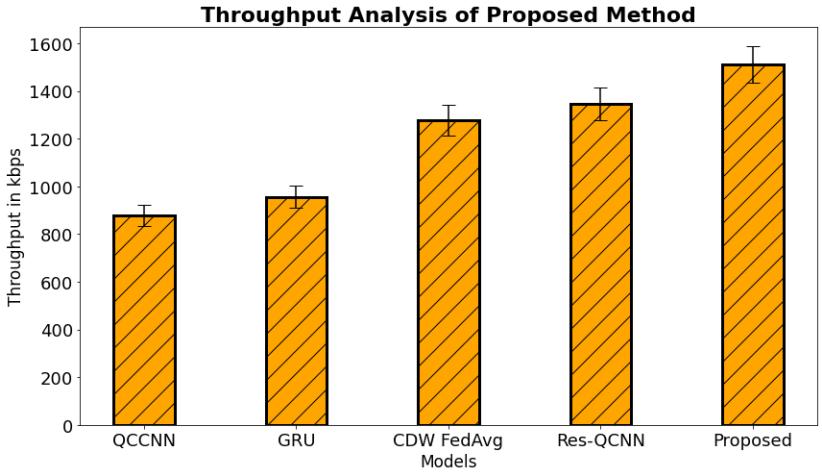

Figure 6: Throughput Analysis of Proposed Method

Tab.6 and Fig.6 present the throughput analysis of the proposed method, representative a important development over other models. The QCCNN model achieves a throughput of 876.76, while the GRU model performs slightly better with 956.33. The CDW FedAvg model exhibits a higher throughput of 1276.65, and the Res-QCNN model further developments with a

throughput of 1345.98. In comparison, the proposed technique outperforms all other models, accomplishing the highest throughput of 1511.71, highlighting its greater efficiency and performance in throughput analysis.

4.4 Ablation Study

Table 7: Ablation Study of Accuracy Comparison

Models	Accuracy
Conventional Neural Networks	89.45
Standard Signature-based IDS	79.45
Proposed Framework (QFNN + CRSD)	98.91

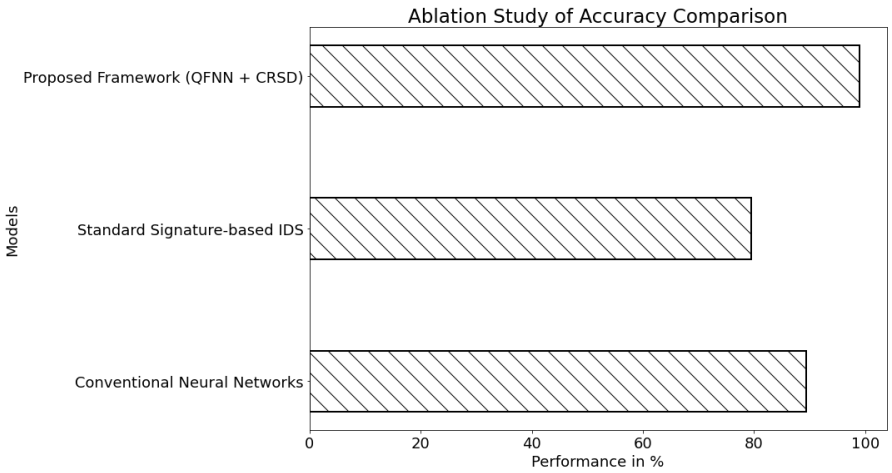

Figure 7: Ablation Study of Accuracy Comparison

Tab.7 and Fig.7 show the ablation study, highlighting the performance comparison between three models: Conventional Neural Networks, Standard Signature-based IDS, and the Proposed Framework (QFNN + CRSD). The results designate that the Proposed Framework achieves the highest accuracy of 98.91%, provocatively outperforming Conventional Neural Networks at 89.45% and Standard Signature-based IDS at 79.45%. This founds the greater efficacy of integrating QFNNs-CRSD in improving detection accuracy and adaptability for IoT security.

Table.8 Comparison of the proposed tehnique with the other models

Author's	Security threat	Validation dataset strategy	Accuracy
Almiani et al. [27]	Network	The NSL-KDD Dataset	94.27%
Mohammadi et al. [28]	Network	The NSL-KDD Dataset	91.39%
Basar et al. [29]	Network	TheUNSW-NB15Dataset	98.6%
Thamilarasu et al. [30]	Network	The DDoS Dataset	98.7%
Our Model	Network	UNSW-NB15	98.91%

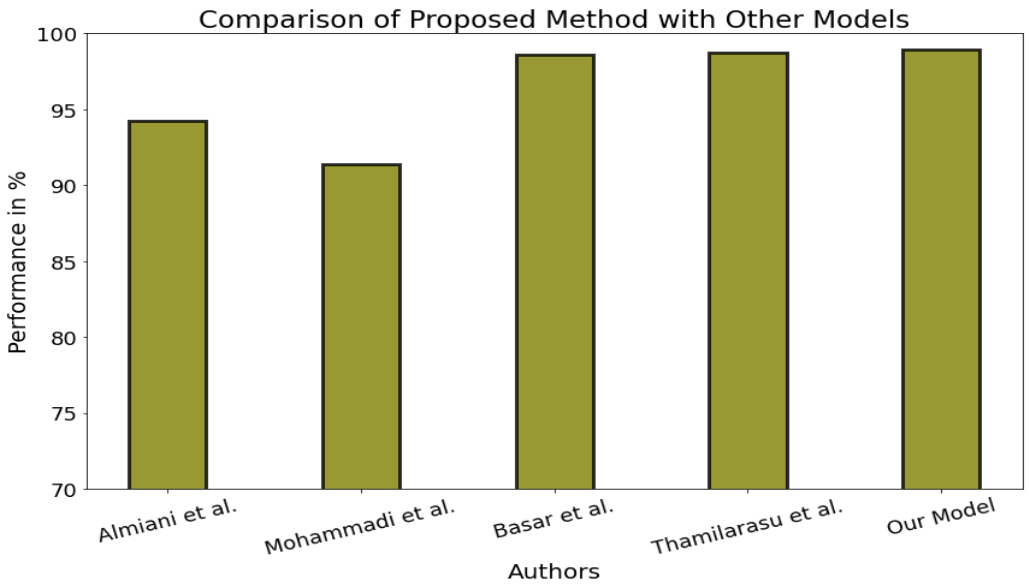

Figure 8: Comparison of the proposed method with the other models

Tab.8 and Fig.8 present a comparison of the proposed method with other models, representative its greater performance in addressing network security threats. Almiani et al. and Mohammadi et al. validated their methods utilizing the NSL-KDD dataset, achieving accuracies of 94.27% and 91.39%, correspondingly. Basar et al. utilized the UNSW-NB15 dataset, accomplishing an accuracy of 98.6%, while Thamilarasu et al. focused on the DDoS dataset, obtaining an accuracy of 98.7%. In contrast, our proposed model, validated utilizing the UNSW-NB15 dataset, achieves the highest accuracy of 98.91%. This underscores the efficiency and robustness of the proposed technique in handling problematic network security challenges.

4.5 Limitations

The proposed framework of QFNN in conjunction with CRSD brings considerable advancements in terms of accuracy, flexibility, and response time for IoT security. Nonetheless, it has some drawbacks. The utilize of quantum computation concepts may be an problem in terms of practical implementation because at the moment there is no mass quantum hardware. Furthermore, the contextual rule-based detection method requires a great deal of calibration and updating in order to be applied to new IoT settings. However, it is also significant to note that this assessment was done on a relatively small IoT network with a relatively simple and homogeneous threat landscape, and scaling this to larger and more complex IoT networks with different threat characteristics may need further tuning and validation.

5. CONCLUSION

The integration of QFNNs with CRSD as proposed means an important step in enhancing the security of IoT networks. As a result of the utilization of quantum principles in computation, QFNNs effectively enhance the performance of the detection accuracy and speed of high-dimensional data. To accomplish flexibility and accuracy, the CRSD module adapts to the contextual parameters such as device behaviour and network traffic. Experimental outcomes prove the effectiveness of this framework over the traditional methods and demonstrate better accuracy, fewer false alarms, and better compatibility with new threats.

The future work will be aimed at extending the applicability of the framework in more complex and extensive IoT settings, as well as at its real-world testing in the edge and cloud infrastructures. However, the combination of quantum computing technologies into new advanced approaches of adaptive learning could be more effective. Some of the proposes for further research are: investigating the robustness of the proposed framework against new types of attack scenarios, and expanding the applicability of the proposed framework to cover multi-modal security threats in different IoT systems.

REFERENCES

[1] Baruah, S.; Borah, D.J.; Deka, V. Reviewing Various Feature Selection Techniques in Machine Learning-based Botnet Detection. *Concurr. Comput.* 2024, *36*, e8076. https://doi.org/10.1002/cpe.8076

[2] Terumalasetti, S.; S R, R. Artificial Intelligence-Based Approach to Detect Malicious Users Using Deep Learning and Optimization Techniques. *Multimed. Tools Appl.* 2024, 1–23. https://doi.org/10.1007/s11042-024-19872-8

[3] Lifi, H.; Khrissi, S.; Nossir, N.; Lifi, M.; Hnawi, S.K.; Tabbai, Y.; Zouhair, S.; Anoua, R.; Ait Ali, M.;

Benkhouja, K. New Analytical Model of Human Body Arm Movements under Various Solicitations by the Finite Element Analysis. *Eur. Phys. J. Appl. Phys.* 2023, *98*, 28. https://doi.org/10.1051/epjap/2023230002

[4] Singh, N.J.; Hoque, N.; Singh, K.R.; Bhattacharyya, D.K. Botnet-based IoT Network Traffic Analysis Using Deep Learning. *Secur. Priv.* 2024, *7*, e355. https://doi.org/10.1002/spy2.355

[5] Alkhonaini, M.A.; Al Mazroa, A.; Aljebreen, M.; Ben Haj Hassine, S.; Allafi, R.; Dutta, A.K.; Alsubai, S.; Khamparia, A. Hybrid Sine-Cosine Chimp Optimization Based Feature Selection with Deep Learning Model for Threat Detection in IoT Sensor Networks. *Alex. Eng. J.* 2024, *102*, 169–178. https://doi.org/10.1016/j.aej.2024.05.051

[6] Ayad, A.G.; Sakr, N.A.; Hikal, N.A. A Hybrid Feature Selection Model for Anomaly-Based Intrusion Detection in IoT Networks. In Proceedings of the 2024 International Telecommunications Conference (ITC-Egypt), Cairo, Egypt, 22–25 July 2024; pp. 1–7. https://doi.org/10.1109/ITC-Egypt61547.2024.10620456

[7] Ayad, A.G.; Sakr, N.A.; Hikal, N.A. A Hybrid Approach for Efficient Feature Selection in Anomaly Intrusion Detection for IoT Networks. *J. Supercomput.* 2024, *80*, 26942–26984. https://doi.org/10.1007/s11227-024-06409-x

[8] Saurabh, K.; Sharma, V.; Singh, U.; Khondoker, R.; Vyas, R.; Vyas, O.P. HMS-IDS: Threat Intelligence Integration for Zero-Day Exploits and Advanced Persistent Threats in IIoT. *Arab. J. Sci. Eng.* 2024, 1–21. https://doi.org/10.1007/s13369-024-08935-5

[9] Saurabh, K.; Gajjala, D.; Kaipa, K.; Vyas, R.; Vyas, O.P.; Khondoker, R. TMAP: A Threat Modeling and Attack Path Analysis Framework for Industrial IoT Systems (A Case Study of IoM and IoP). *Arab. J. Sci. Eng.* 2024, *49*, 13163–13183. https://doi.org/10.1007/s13369-023-08600-3

[10] Gelgi, M.; Guan, Y.; Arunachala, S.; Samba Siva Rao, M.; Dragoni, N. Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors* 2024, *24*, 3571. https://doi.org/10.3390/s24113571

[11] Abu Al-Haija, Q., & Zein-Sabatto, S. (2020). An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. *Electronics*, *9*(12), 2152. https://doi.org/10.3390/electronics9122152

[12] Albishari, M., Li, M., Zhang, R., & Almosharea, E. (2023). Deep learning-based early stage detection (DL-ESD) for routing attacks in Internet of Things networks. *The Journal of Supercomputing*, *79*(3), 2626-2653. https://doi.org/10.1007/s11227-022-04753-4

[13] Zhou, X.; Liang, W.; Li, W.; Yan, K.; Shimizu, S.; Kevin, I.; Wang, K. Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system. IEEE Internet Things J. 2021, 9, 9310–9319. https://doi.org/10.1109/JIOT.2021.3130434

[14] Wang, M.; Yang, N.; Weng, N. Securing a smart home with a transformer-based iot intrusion detection system. Electronics 2023, 12, 2100. https://doi.org/10.3390/electronics12092100

[15] Aktar, S.; Nur, A.Y. Robust Anomaly Detection in IoT Networks Using Deep SVDD and Contractive Autoencoder. In Proceedings of the 2024 IEEE International Systems Conference (SysCon), Montréal, QC, Canada, 15–18 April 2024; pp. 1–8. https://doi.org/10.1109/SysCon61195.2024.10553592

[16] Shukla, P.; Krishna, C.R.; Patil, N.V. Iot Traffic-Based DDoS Attacks Detection Mechanisms: A Comprehensive Review. J. Supercomput. 2024, 80, 9986–10043. https://doi.org/10.1007/s11227-023-05843-7

[17] Thota, S.; Menaka, D. Botnet Detection in the Internet-of-Things Networks Using Convolutional Neural Network with Pelican Optimization Algorithm. Automatika 2024, 65, 250–260. https://doi.org/10.1080/00051144.2023.2288486

[18] Abdulkareem, Sulyman Age, Foh, Chuan Heng, Carrez, François, Moessner, Klaus, 2024. A lightweight SEL for attack detection in IoT/IIoT networks. J. Netw. Comput. Appl. 230, 103980–103993. https://doi.org/10.1016/j.jnca.2024.103980

[19] https://www.kaggle.com/datasets/alextamboli/unsw-nb15

[20] Kadry, H., Farouk, A., Zanaty, E. A., & Reyad, O. (2023). Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security. Alexandria Engineering Journal, 71, 491-500. https://doi.org/10.1016/j.aej.2023.03.072

[21] Xiao, H., Chen, X., & Xu, J. (2022). Using a deep quantum neural network to enhance the fidelity of quantum convolutional codes. Applied Sciences, 12(11), 5662. https://doi.org/10.3390/app12115662

[22] Díaz-Verdejo, J., Muñoz-Calle, J., Estepa Alonso, A., Estepa Alonso, R., & Madinabeitia, G. (2022). On the detection capabilities of signature-based intrusion detection systems in the context of web attacks. *Applied*

Sciences, *12*(2), 852. https://doi.org/10.3390/app12020852

[23] Perumal SK, Kallimani JS, Ulaganathan S, Bhargava S, Meckanizi S. Controlling energy aware clustering and multihop routing protocol for IoT assisted wireless sensor networks. Concurrency Computat Pract Exper. 2022;e7106. doi: 10.1002/cpe.710

[24] Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated-learning-based anomaly detection for IoT security attacks. IEEE Internet of Things Journal, 9(4), 2545-2554. https://doi.org/10.1109/JIOT.2021.3077803

[25] Zhang, W., Lu, Q., Yu, Q., Li, Z., Liu, Y., Lo, S. K., ... & Zhu, L. (2020). Blockchain-based federated learning for device failure detection in industrial IoT. IEEE Internet of Things Journal, 8(7), 5926-5937. https://doi.org/10.1109/JIOT.2020.3032544

[26] Abd El-Aziz, R. M., Taloba, A. I., & Alghamdi, F. A. (2022). Quantum computing optimization technique for iot platform using modified deep residual approach. Alexandria Engineering Journal, 61(12), 12497-12509. https://doi.org/10.1016/j.aej.2022.06.029

[27] M. Almiani, A. Abughazleh, A. Al-Rahayfeh, S. Atiewi, A. Razaque, Deep recurrent neural network for IoT intrusion detection system, Simul. Model. Pract. Theory 101 (2020). https://doi.org/10.1016/j.simpat.2019.102031

[28] P. Santhosh Kumar, B. Sathya Bama, Chiranjit Dutta, D. Vijendra Babu, Green energy aware and cluster-based communication for future load prediction in IoT, Sustainable Energy Technologies and Assessments, Vol.52,2022,102244, https://doi.org/10.1016/j.seta.2022.102244

[29] G. Thamilarasu, S. Chawla, 'Towards deep-learning-driven intrusion detection for the internet of things, Sensors (Switzerland) 19 (9) (2019). https://doi.org/10.3390/s19091977

fffff