scientific reports

Check for updates

OPEN

Quantum intrusion detection system using outlier analysis

Tae Hoon Kim [1] & S. Madhavi [2]

In the feld of cybersecurity, hackers often enter
owing to the huge amount of network trafc that ma
between authorized trafc and abnormSaelrvdiacte a (pDDoS)c
attackers is still a major difculty. This researc
Machine Learning (QML) to improve security protoc
Our strategy enhances detection accuracy and spee
networks. The approach includes creating a datase
and then turning it into quantum bits via angle e
entropy, and quantum state fdelity to distinguish
dispersed randomness of network ,hewahdiecrh daaitdas iisn mie
security concerns. The suggested QML-based method
current models, including AMM-CNN and ANN models,
attacks. This advancement leads to more efective

Keywords Qubit, Entropy, Quantum state machine, Fidelity, Key distribution, Distributed denial of service

Due to the latest infrastructures and remote access to the hosts in many Internet of Things (IoT) technology-based applications, much vulnerability is introduced. This raised the need for novel intrusion detection systems. Distributed Denial of Service Attacks (DDoS) is one such vulnerability that is caused to the networks. The main feature of this attack is that it creates large, unusual traffic so that the host would be overwhelmed by the traffic. Also, the attacker may send malicious packets to consume the host resources. Under such situations, slowly the system denies the service requests made by the authentic users too in the network.

The intruder attacks the intended system in several ways:

- Sending unnecessary traffic,
- Trying to stop the traffic from reaching its specific destination,
- Consuming all the resources available at a particular system and making it fall off fewer resources at hand.
- Overhearing the IOT devices.
- DNS amplification, etc.

Hence, to differentiate the DDoS attack from normal traffic, some of the features are listed below.

- Difference in time between the establishment of two connections for communication.
- Protocols like TCP, UDP, etc.
- Number of source and destination bytes that are exchanged.
- Number of connections from and to a host at an instant in time.

Signifcance of the proposed study

Many techniques are implemented to detect such anomalies in the network. Since the computational power of the quantum systems is very high, the performance of a quantum intrusion detection system overrides the performance of traditional intrusion detection systems. Hence, in real-time network applications, quantum intrusion detection systems are very significant since they detect such anomalies quickly before any huge damage is caused to the system. Also, the quantum deep neural networks yield high accuracy in detecting the intruder when compared to the traditional intrusion detection systems. DDoS attacks are very difficult to detect since it is difficult to estimate the distribution randomness of the abnormal behavior in the intruder patterns in the

[1]School of Information and Electronic Engineering and Zhejiang Key Laboratory of Biomedical Intelligent Computing Technology, Zhejiang University of Scienc[2]Departmand of Techn
Computer Science and Engineering, PVP Siddhartha Institute of Technology, Kanuru, Vijayawada, Andhra Pradesh,
Indiaemail: mmadhavi@pvpsiddhartha.ac.in

input feature. Hence, in such scenarios, entropy-based outlier detection methods are mostly applicable for DDos attacks, as the entropy method calculates the uncertainty in the state.

Generally, there exist various kinds of noise, such as shot noise N_0, the technical excess noise x, the electrical noise V_{el}, and the channel excess noise #. The detector's electronic noise is expressed as $V_{el} = V_{el}N_0$ and the technical excess noise of the system is expressed as $h = \#N_0$. Then, if T indicates channel transmittance, then $y_B = tRXA + ZR$, where, $t_R = \sqrt{\#T} \in R$ and zR follows a Gaussian distribution with a mean of 0 and a variance of $(V_{el} + N_0 + \#T\xi)$.

A certain amount of noise is quite natural in a system. But if the observed noise level is above a level threshold then it indicates the presence of an intruder. The observed pattern may be slightly deviated from the normal pattern, and after some number of rounds, a clear pattern deviation might be observed. If A represents the system in its normal state and E represents the attacker System, then entropy is defined on the normal system and attacked system by using H(A|E). The difference in these two systems' entropy is calculated. Outlier analysis is used to find the abnormal and normal system behavior patterns in the data sets. If the difference reaches above an allowed level of threshold, then the intruder's presence is detected.

The innovation and novelty of the proposed study are.

- Combination of Quantum Computing and Machine Learning: This study proposes combining quantum computing techniques with machine learning to enhance communication system security. This recent merging of two frontier fields represents an emerging field of research.
- Application of Quantum State Fidelity: It is unique to use quantum state fidelity as a metric in the creation of a secure communication system. To ensure the privacy and integrity of communication channels, this method makes use of the special qualities of quantum systems.
- Use of Angle Embedding method for Quantum Bit Conversion: Among Amplitude, Basis and Angle encoding methods, the angle encoding method gives better performance. The Amplitude encoding needs a small number of bits to represent the features in the data set, but it needs a larger number of gates to build the appropriate state vector. However, the angle encoding method needs as many qubits as the features but needs a smaller number of gates to design the required state vector.

  Hence we used the angle embedding to transform preprocessed data into quantum bits. This is an optimal technique for quantum data representation from classical data with a small number of gates and qubits among the Basis, Amplitude and Angle encoding methods. Generally, in many research implementations of quantum intrusion detection systems, the input states are quantum mechanical. In our proposed work, we used quantum embeddings of the input bits and then entangled the states using CNOT gates.

- High Detection Accuracy: Remarkably, Distributed Denial of Service (DDoS) attacks can be detected with a 99.87% detection accuracy. While previous studies have explored similar topics, the accuracy of the proposed solution is remarkable and demonstrates its efficacy in addressing security concerns.

In Section II, the related literature is discussed. In Section III, the protocol for detecting intruders using a Quantum Intrusion Detection System using outlier analysis (QIDS-OA) is presented. In Section IV, the results and a comparative study are presented. In Section V, the conclusions are presented. Section VI presents the limitations and future studies.

Related studies

The use of quantum machine learning (QML) for enhancing security intrusion detection with large datasets is proposed by Kalinin and Krundyshev. Since traditional machine learning often struggles with speed and accuracy in big data contexts, the study compared QML methods, specifically quantum support vector machines (QSVM) and quantum convolutional neural networks (QCNN), with conventional approaches. Using a proprietary dataset that formats network packets for QML, their results showed that QML methods achieve high accuracy (98%) and process data twice as fast as traditional machine learning algorithms[1]. The researchers discovered quantum machine learning algorithms that had code readily accessible and compared them to conventional equivalents using appropriate datasets. Their assessment focused on the duration of execution and the level of precision. Researchers discovered that quantum variational support vector machines (SVMs) sometimes surpassed traditional SVMs in multiclass classification tasks. The research determined that quantum multiclass SVMs have the potential to be very profitable as quantum computing technology progresses and the quantity of qubits grows[2]. Thapa and Mailewa reviewed the roles of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in modern network security. The paper outlines the main functions of IDS and IPS, their operational mechanisms, and their significance in protecting information systems. It also examines various IDS and IPS tools that can enhance system security and provides insights into how these systems contribute to robust protection against security threats[3]. Kilincer et al. reviewed the use of machine learning methods in cybersecurity intrusion detection, focusing on various datasets like CSE-CIC IDS-2018, UNSW-NB15, ISCX-2012, NSL-KDD, and CIDDS-001. They applied max-min normalization to these datasets and evaluated classical machine learning algorithms: Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Decision Tree (DT). The study found that these approaches yielded promising results in some cases, highlighting their potential for enhancing IDS systems. The findings underscore the value of integrating machine learning techniques into IDS development to improve detection and security[4]. Through an examination of many artificial intelligence-based methodologies, the researchers presented strategies for developing and putting into practice intrusion detection systems. This thorough analysis highlights machine learning's adaptability and potency in bolstering network security against changing threats. The research descended into the domain of quantum machine learning

methods[5], providing an in-depth examination of their potential and performance attributes. The researchers attempted to evaluate the effectiveness of a number of quantum machine learning algorithms in practical settings by running them on a quantum computing platform enhanced with cloud computing capabilities. The potential of quantum computing to completely transform the field of intrusion detection and cybersecurity is shown by this empirical investigation. The study discussed identifying malicious code in HetNets with less than 5G of capacity by using a multi-objective RBM model. They recommended methods aimed at lowering data fusion losses and raising HetNets' classification precision[6].

The potential and complexities of intelligent artificial intelligence systems in many contexts were discussed[7–11]. The examination of several ML/DL computations in the administration of smart cities and communities was demonstrated[8]. It utilized technologies integrated with emerging trends in information technology to facilitate the development of smart cities. The benefits and drawbacks of different ML/DL strategies for intrusion detection were studied[9]. Gouveia and Correia reported the network discovery using unsupervised quantum machine learning. A quantum encoder was used by the authors in the implementation of an anomaly detection system[11]. For use in network intrusion systems, a quantum autoencoder based on deep neural networks is created. The authors used a unique and successful e-commerce mobile payment risk model to anticipate trends in e-commerce mobile payment risk[12].

The authors studied the Quantum Evolutionary Algorithm[13]. Zhang used UCI repository and KDD CUP 99 datasets and implemented a method for intrusion detection systems using dimensionality reduction for the classifier[14].The Parameterized Quantum Circuits for Learning Cooperative Quantum Teleportation were presented[15]. Zhang et al. reported an enhanced quantum random-walk search method for multiple solutions[16]. The method can also be employed to find the running time complexity of the optimised quantum random-walk search algorithm.The authors described the ANN model for quantum attack detection; this model is not appropriate for large-scale datasets due to its long calculation time and several parameter combinations[17]. The articles give great detail on the development of several ML techniques for traffic monitoring and identifying unusual node activity inside the network[18–28]. To demonstrate attack detection, methods like Quantum Convolutional Neural Networks (QCNN), support vector machines, random forests and decision trees were used.The attack detection was demonstrated using various techniques like decision trees, random forests etc[19]. , The authors proposed an attention mechanism module to enhance the detection capability of the CNN model. The main aim of this module was to find the most relevant features in a feature set.In[21], authors studied DDoS attacks in peer-to-peer networks. In this paper, the authors executed a method for image recognition in deep networks. They proposed a quantum tomography algorithm and implemented the algorithm using the MIST data set and proved the efficiency of the QCNN. In[22], the authors studied a detection system using a support vector machine.In this proposed method the training and testing times are optimized.The quantum version of SVM is used to implement a network intrusion detection system on two data sets UNB NSL KDD and two data UNSW NB15[23]. This method obtained good error correction rates even at low signal-to-noise ratios.In[24] authors gave a deep computation method for long-distance quantum key distribution. They utilized a long-distance continuous-variable measurement-device-independent quantum key distribution (CV-MDI-QKD) protocol with discrete modulation. This kind of discrete-modulated scheme has good compatibility with efficient error correction code, which leads to higher reconciliation efficiency even at a low signal-to-noise ratio. In[25] authors presented Quantum Cryptography and Quantum Key Distribution Protocols. In this paper, the authors studied quantum cryptography, its functions and QKD protocols extensively.In-depth research on quantum-dot entangled photon sources was conducted, and real-world quantum communication was also reported using quantum key distribution in quantum dots[26]. A method for secure key distribution was proposed by Langenfeld et al.[27]. The authors implemented a quantum method for distributing the key securely. They implemented a method by increasing the attenuation length by a factor of two. In[28], the authors presented a work on how to train deep quantum neural networks. A method in quantum feed-forward neural networks was optimised for quick optimization. The proposed method uses fidelity as a cost function and uses less memory leading to small training times for deep network optimization. Several articles discussed hierarchical quantum classifiers using quantum circuits[29–39].A comprehensive investigation of intrusion detection based on deep learning methods was presented. This analysis used a variety of intrusion detection systems to analyse the data[30]. Anomaly-based intrusion detection systems for IoT networks were studied through deep learning models[31]. A CNN-based intrusion detection system was compiled using NID and BOT-IOT datasets. In[32], the authors presented a deep study on Cooperative Fuzzy Q-learning in Network. The authors implemented a method for wireless systems called Cooperative IDS which is based on Fuzzy Q-learning and Co-FQL optimization algorithmic technique. The data sets NSL-KDD and CAIDA DDoS Attack 2007 were used in the training phase and this method yielded high accuracy in detection rates. In[33], the authors presented an approach for assessing amplified reflection DOS on the Internet of Things. In this paper, the authors implemented an intrusion detection method in IOT devices. They basically tested all the decision flows during the protests and finally, the method was applied to the AR-DDoS. Results proved that the proposed method yields better results. In[34], the authors studied the Anonymous Email Network Characteristics. It implemented a method for Social network analysis to detect various attacks. The email network database from 29 university faculties is used in the proposed study to understand the behavior of small email networks.A new DoS defense method using the signature method is reported[35]. In this work, the authors proposed a method for detecting DoS attacks in IOT devices. The proposed method is analyzed and proved to achieve better results than the existing study. In[36], the authors found various solutions for Intrusion Detection and Prevention in IoTs using machine and deep learning methods. They described the importance of AI-based protocols for intrusion detection or prevention. Various AI-based machine learning and deep earning techniques are described for the task of intrusion detection-prevention systems. In[37], the authors implemented a method for feature extraction in IoT using machine and deep learning methods. The work proposed a method for feature extraction using various machine learning and deep learning algorithms. In[38], the authors performed

a survey of authentication methods in IoT. It described the basics of authentication in IoT devices and various attacks while using such devices.A comprehensive study is made by the authors. In[39] a systematic review is made on Quantum Machine Learning for Network Intrusion Detection Systems. In[40] the authors discussed various fundamental aspects of quantum machine learning, deep learning techniques, and various optimisation algorithms in detail. In[41] the authors discussed a literature review in the area of quantum neural networks for an intrusion detection system like hybrid quantum-classical, support vector machines. The models are compared at the end of the study. In[42] the authors presented a detailed study on how quantum adversarial generative networks and implemented using qiskit. In[43] authors discussed WSCO-based QNN for intrusion detection systems using Elliptical curve cryptography. In[44] authors an ensemble-based intrusion detection system is implemented.

In the proposed study outlier analysis, min-entropy method, and quantum state fidelity are used to design a secured quantum communication state for a safer communication system. The data set is generated from network traffic patterns and converted into quantum bits using angle embedding. The proposed detection approach performs better than the traditional methods since the distribution randomness of the intruder's abnormal behaviors in the patterns can be measured accurately.

In the proposed study outlier analysis, min-entropy method, and quantum state fidelity are used to design a secured quantum communication state for a safer communication system. The data set is generated from network traffic patterns and converted into quantum bits using angle embedding.

Materials and method for the proposed qu

We used Qiskit and Pennylane to simulate the Quantum Neural Networks. The open-source program Pennylane provides high-level wrappers for Quantum Neural Networks (QNNs). QNodes in Pennylane were used to represent quantum functions, which were essential for developing and modelling QNNs in this experiment. Qiskit was used to encode features by using techniques such as ZZFeatureMap from its circuit library. In practical communication, the channel transmittance is highly likely to be controlled by Eve. A slight change in the channel transmittance causes significant parameter estimation errors. However, in practical implementations, the transmission of legitimate optical signals and the presence of real detectors and electronic components introduce inherent fluctuations, which pose challenges for accurate estimation. To address these challenges, Alice and Bob must engage with multiple iterative computations to achieve precise estimation.

Moreover, the estimation process usually occurs after the completion of the key transmission. In the unfortunate event of detecting an attack, the entire key data must be discarded, leading to substantial time and resource waste. Hence, an efficient quantum denial-of-service (DoS) attack defense solution is needed to resist such attacks effectively. Bob can input the received keys into the model sequentially, and in the event of detecting any anomalous data, the transmission process will be immediately terminated. Hence, a quantum intrusion detection system that is fast and accurate is essential. To overcome this problem, a Quantum Intrusion Detection System using outlier analysis (QIDS-OA) was proposed in this study.The implementation method of the proposed Quantum Intrusion Detection System using outlier analysis (QIDS-OA) is depicted in Fig. 1. There are several steps involved in implementing it. To make a secure connection for communication, several steps are involved in QIDS-OA computations. First of all, data is acquired using the network traffic patterns. Then the dataset underwent many stages of preprocessing. After these preprocessing steps were finished, 87 essential features were discovered and are listed in Table 1. Among other important elements of network traffic flow, these features include time stamps, source and destination IP addresses, source and destination ports, protocols, and indicators of potential attacks.These features are then converted to quantum states using the quantum circuit depicted in Fig. 2.

Basis quantum encoding is performed on the initial qubits. The quantum layer performs Angle Embedding to encode the data to a quantum state. Each classical input data bit x is encoded into a quantum state angle encoding using the mapping $x \rightarrow \rho\ (x)$. The purpose of the encoding part is to load classical data by encoding it into the quantum state of the qubits.The features in the data point x are encoded using the angle embedding method to create a quantum state $|\psi z$.

The Rx gate in a quantum circuit is as follows.

$$R_z(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

The researchers then chose an optimization algorithm to be used in the training process.A parameterized quantum circuit is a feed-forward network where the outputs from the previous layer are set as the inputs to the next round. A hidden layer is implemented as one entangling layer.This objective function characterizes the distance between the predictions and known labeled data.

The implementation steps of the proposed Quantum Intrusion Detection System using outlier analysis (QIDS-OA) are explained in Algorithm 1. Algorithm 1 also describes the experimental setup procedure through its various phases like channel setup, data build phase, preprocessing phase, feature map phase, Ansatzphase, training and testing phases with optimized functions for the proposed QIDS-OA.

Algorithm 1. QIDS-OA

//The mathematical formulation of the propsoed QIDS is as follows.

Step 1: Channel setup(Channel Transmittance): If x and y represent the interrelated data shared by users, then the channel transmittance T with excess noise ϵ like shot noise N_0, technical noise ξ, electrical noise V_{el}, technical excess noise #,

Then $y_B = t_R x_A + Z_R$

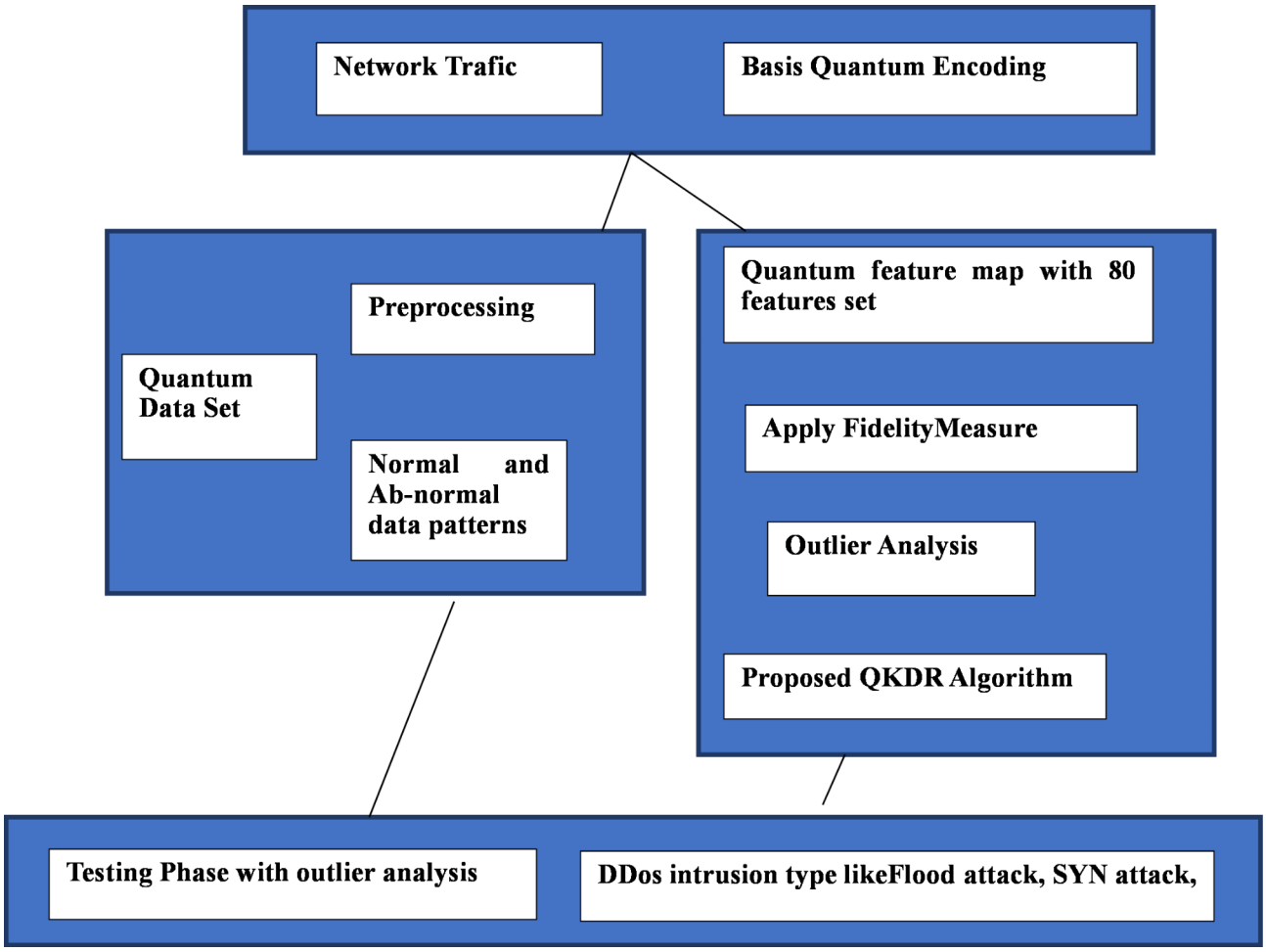

Fig. 1. Architecture of proposed Quantum Intrusion Detection System using outlier analysis (QIDS-OA).

Where, $t_R = \sqrt{\#T} \in R$ and Z_R follows a Gaussian distribution with a mean of 0 and a variance of (V_{el}+ N_0+ $\#T\xi$,).

And if the channel transmittance changes the presence of Eve/noise is predicted.

Step 2: Data build phase: A dataset containing attack types and normal types was created. As shown in Fig. 1, the network traffic data is stored in a data set X.

Step 3: Preprocessing phase: Table 1 shows various important features obtained after the preprocessing phase. The dataset was subjected to various data pre-processing techniques such as removing blank values and replacing them with median values, infinity values and very large values with '0'. Also, data items with a correlation factor above a certain threshold were removed. Finally, 87 features as mentioned in Table 1 were obtained after the preprocessing phase.

Step 4: ZZ Feature Map Construction phase:

//This phase is to prepare the quantum states. The necessary quantum circuit is shown in Fig. 2.

$$R_x(\theta) = e^{-i\varnothing\frac{X}{2}} \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \quad (1)$$

$$R_y(\theta) = e^{-i\varnothing\frac{Y}{2}} \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \quad (2)$$

$$R_z(\theta) = e^{-i\emptyset\frac{z}{2}} \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\emptyset/2} \end{bmatrix} \quad (3)$$

SNO	Attribute	SNO	Attribute	SNO	Attribute
1	Fwd Packet Length Max	27	Flow duration	53	BwdAvg Bulk Rate
2	Fwd Packet Length Min	28	Packets per second	54	SubflowFwd Packets
3	Max Packet Length	29	Packet Transmission	55	SubflowFwd Bytes
4	Min Packet Length	30	Packet delay note	56	SubflowBwd Packets
5	Average Packet Size	31	Packet Rate	57	SubflowBwd Byte
6	FWD Packets/s	32	byte rate	58	Fwd PSH Flags
7	Fwd Header Length	33	PktAvg Size	59	Bwd PSH Flags
8	Fwd Packet Length std	34	Utilization	60	Fwd URG Flags
9	Min Seg Size Forward	35	Packet Delay	61	Bwd URG Flags
10	PKTDELAY	36	Packet send time	62	PSH Flag Count
11	FROMNODE	37	Packet reserved time	63	FIN Flag Count
12	TONODE	38	The first packet Sent	64	SYN Flag Count
13	SRCADD	39	the last packet reserved	65	RST Flag Count
14	Source port std. deviation	40	Bwd Header Length	66	ACK Flag Count
15	Destination port std. deviation	41	Fwd Header Length	67	URG Flag Count
16	Protocol	42	min seg size forward	68	Down/Up Ratio
17	Flow Duration	43	Active Mean	69	Bandwidth bytes per sec
18	Number of packages	44	Active Std	70	Idle Min
19	Total Backward Packets	45	Active Max	71	FwdAvg Bytes/Bulk
20	Total Length of Fwd Packets	46	Active Min	72	FwdAvg Packets/Bulk
21	Total Length of Bwd Packets	47	Idle Mean	73	FwdAvg Bulk Rate
22	Bwd Packet Length Max	48	Idle Std	74	BwdAvg Bytes/Bulk
23	Flow Bytes/s	49	Idle Max	75	BwdAvg Packets/Bulk
24	AvgFwd Segment Size	50	Fwd Header Length		
25	Sequential Number	51	Bwd Header Length		
26	Number of Packets	52	Average Packet Size		
76	Minimum, maximum, mean values of packet length and standard deviation				
77	Average number of characters printed in packet data				
78	Minimum, maximum, average packet lifetime and standard deviation				
79	Average number of characters printed in packet data				
80	Minimum, maximum, average packet lifetime and standard deviation				
81	Minimum, maximum, mean of packet sequence number and standard deviation				
82	Minimum, maximum, average batch confirmation number and standard deviation				
83	Minimum, maximum, average packet window size and standard deviation				
84	Minimum, maximum, mean interval between bursts and standard deviation				
85	src packets retransmitted or dropped				
86	destination packets retransmitted or dropped				
87	service like ftp, http, smtp, ssh, dns				

Table 1. Network traffic containing flows.

This is expressed as.

$$\left|\psi(\theta)\right\rangle = R_y(\theta)\left|0\right\rangle + e^{i\phi}R_y(\theta)\left|1\right\rangle\Big| \tag{4}$$

This phase in the algorithm acts as an encoder to embede each features as rotation angles. After embedding the feature map the entaglement layer is used for better tuning the features.

Step 5: Entaglement Phase.

One Hadamard gate was applied to each qubit immediately after encoding. Figure 2 shows the overview of the proposed quantum circuit. In this procedure, Quantum states are first prepared. The states are then quantum-embedded. Rθ is applied to this state, which is a product of two unitaries R(X1; Y1; 0) and trainable parameters R(θ1; θ2; θ3) to implement a strongly entanglement layer. Let QL denotes the number of strogly entaglement layers. Four qubit devices are taken from pennylane for the encodding process. Five layers with four R(X) rotations were used with rotation angles uniformly between 0 rad and 2 π rad and four CZ operations.

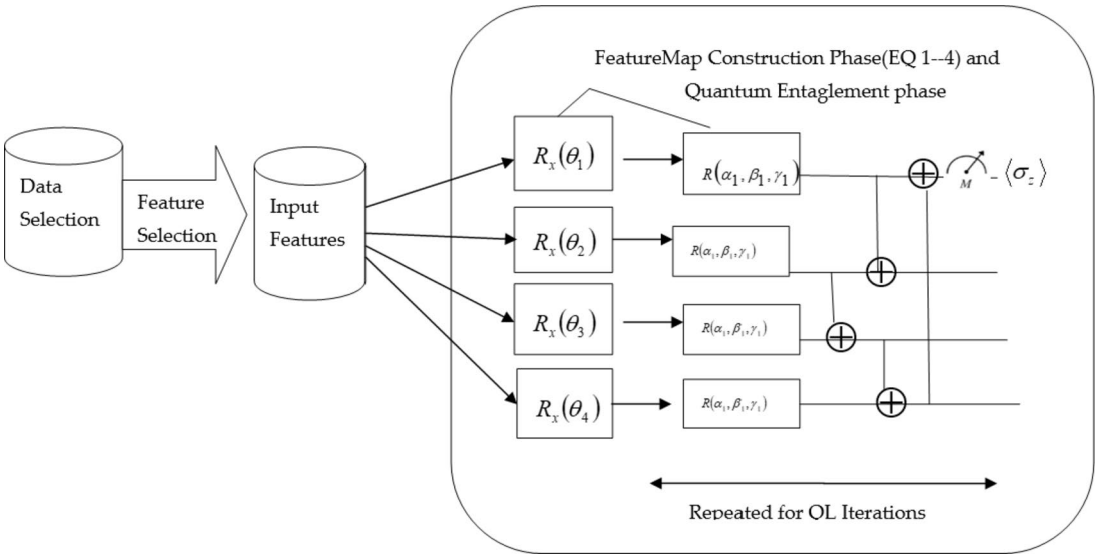

Fig. 2. Overview of the proposed quantum circuit (experimental setting of the proposed quantum circuit).

The CNOT gaates are applied neighbouring pairs of qubits. At the end a simple pauli Z measurement with the associated ansatz was used for Entrpy calculation. The output is a Pauli Z measurement on the qubits.

Step 6: Training Phase: The QIDS-OA model was trained with the known pattern sets of data that contain no eavesdropper. The DDoS attacks were then introduced to create abnormal data patterns. Then, the system was trained with the abnormal data patterns. Now, the classifier is ready to be constructed and fit it. Pauli gates were applied to the qubit.

Step 7. Proposed detection phase: After preparing the quantum states, in the training phase, the difference in the fidelity between these states is calculated with the trained normal and abnormal data patterns.

a. For each state $\rho = \langle \phi_\rho |$, in the features map
b. For each $\sigma = \langle \phi_\sigma |$, in the normal abnormal states in the training data set

$$\text{Calculate Fidelity F} = \left(\text{tr}\sqrt{\sqrt{\rho}\,\sigma\,\sqrt{\rho}}\right)^2 \tag{5}$$

c. // Detection with entropy. If an observable fidelity is found between the states then the Entropy which is a measure of the randomness in behavious of the states through its unpredictable values in the features is calculated. The uncertainty in the state is measured generally using the following formula.

   If (p(xi)) is the probability of occurrence of the ith outcome then calculate Entropy (H(X))

$$H(X) = -i\sum_{i=1}^{n} p(x_i \log_2 p(x_i))$$

d. If a lower bound ω was defined on the amount of entropy so that the abnormal data point would be identified, and If S denotes observed dissimilarity and T denotes the allowed minimum dissimilarity. Then.

   Calculate the outlier factor is defined as

$$FOF \quad y_n = \frac{\sum \text{S(X)}}{T} \tag{6}$$

e. //This entropy is cumulatively stored in outlier sets in every round i€ {1, …, n} of the protocol. i.e. $y_n = y_{n-1} + z_n$ where $y_0 = 0$ and Z_n denotes the change added.
f. ///If the system is normal and had no attacks the traffic distribution would be normal and the entropy value will be small. But if the attacker attacks the system, a huge network traffic creates abnormal traffic patters and If a transactions contains more frequent patterns, then its entropy will be large that is its FOF > 1.
g. After training the system with n test rounds, for the known patterns and if An, En represent the tested and normal states at round n then the min-entropy of the system was used where $H_{min}^{\varepsilon}(A^n|E^n)$ is minimum of FOF
h. Step 8: End.

Evaluation metrics

The various metrics used for model testing. These are defined as follows:

$$\text{True negative rate}\ \ \text{TNR} = \frac{\text{TN}}{(\text{TN} + \text{FP})}$$

$$\text{True Positive rate}\ \ \text{TPR} = \frac{\text{TP}}{(\text{TP} + \text{FN})}$$

$$\text{False positive rate}\ \ \text{FPR} = \frac{\text{FP}}{(\text{TN} + \text{FP})}$$

$$\text{False Negative rate}\ \ \text{FNR} = \frac{\text{FN}}{(\text{TP} + \text{FN})}$$

$$\text{Accuracy} = \frac{\text{TN} + \text{TP}}{\text{TN} + \text{TP} + \text{FN} + \text{FP}}$$

Precision represents the percentage of predictions that are correct.

$$Precision\ = \frac{TP}{TP + FN}$$

Recall represents the percentage of appropriate items recognized by the model

$$Recall\ = \frac{TP}{TP + FN}$$

False Discovery Rate (FDR) provides a way to linearly measure the expected number of false positives based on precision. It is defined as.

False Discovery Rate = 1- Precision

$$F1\text{-}Score\ = \frac{2 \times\ TP}{2 \times\ TP + FP + FN}$$

where.

True positive (TP): an attack is present and is correctly detected and alerted by the QIDS-OA.
True negative (TN): no attack is present and the QIDS-OA correctly considers it as normal.
False positive (FP): no attack is present but QIDS-OA misinterprets it as an attack and reports a false alert.
False negative (FN): an attack is present but not detected by the QIDS-OAand no alert is reported.

Results and discussion

Simulations were conducted using Qiskit SDK v1.1 (Link: https://qiskit.org/) and PennyLane v0.38 (https://pennylane.ai/) software. The communication data without any attack and data under DDoS attacks were collected. The data obtained were split into a ratio of 70:15:15 (training: validation: testing). Pennylane is an open-source software framework that has a bunch of high-level wrappers for constructing quantum circuits for Quantum Neural Networks. The 100,000 data samples with 87 features were given to the proposed model. Next, these feature vectors were passed to the model for training to learn the features of different attackstrategies. To train the classifier for detecting network attacks, two datasets were generated as training sets like normal data that have no attacksand datasetsthat have been attacked by Eve's DDoS attack. The angle encoding was performed on the collected data. The ZZFeatureMap in the Qiskit circuit library was used.

The distribution of testing nodes across different attack types in a DDoS attack experiment is shown in Table 2. In this configuration, 6000 nodes are set up to represent typical network activity and function as a baseline for safe actions. Each of the four attack simulations, HTTP flooding, ACK flooding, port scanning, and SYN flooding, has 1000 nodes assigned to it.While ACK flooding floods a network with TCP ACK packets,

	Normal	HTTP flooding	ACK flooding	Port scanning	Syn flooding
No of testing nodes	6000	1000	1000	1000	1000

Table 2. Number of nodes assumed for each attack type.

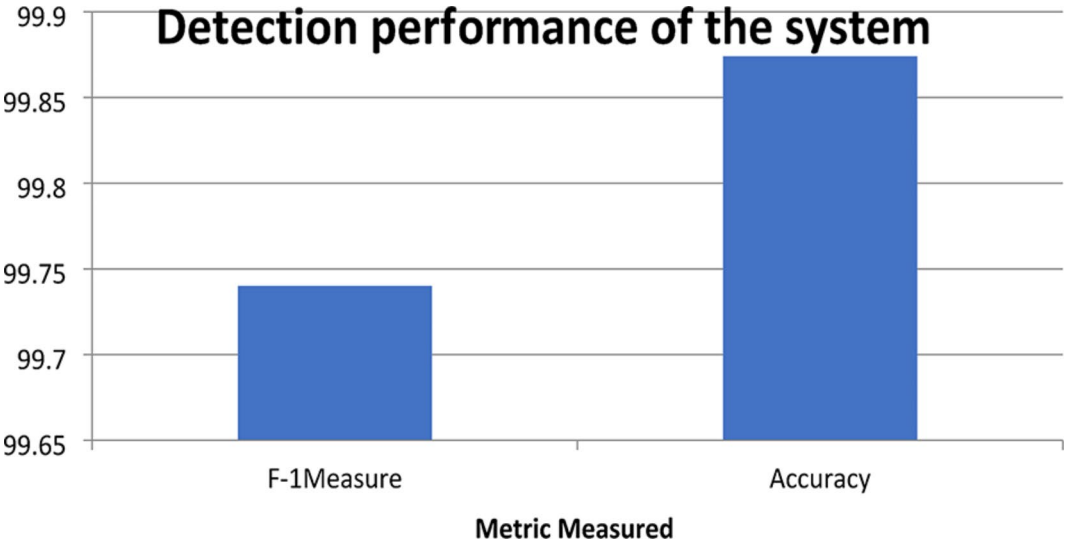

Fig. 3. Detection accuracy.

Percentage of deviation	Normal	HTTP flooding	ACK flooding	Port scanning	Syn flooding
Normal	5988	3	4	2	3
HTTP flooding	1	998	–	–	–
ACK flooding	4	–	989	–	–
Port scanning	0	–	–	1000	–
Syn Flooding	3	–	–	–	990

Table 3. The confusion matrix for the test dataset.

HTTP flooding entails sending an excessive amount of HTTP requests to a server. SYN flooding uses TCP handshakes to induce denial of service, while port scanning looks for open ports and services.

Algorithm 1 was repeated until the loss was minimized to a value less than 0.2. The training phase for 500 epochs was implemented with a learning rate equal to 0.005. For each epoch, the fidelity was calculated. After the first 120 epochs, an accuracy of 0.998 was obtained. The results showed that the proposed intrusion detection had high accuracy (99.897%). Hence, it was proven that the proposed model detects DDoS attacks accurately on the application it is implemented. Hence, the proposed model is trained successfully to identify all attacks with a maximum accuracy of 99.897%. Figure 3 shows the Detection Accuracy.

The confusion matrix, as shown in Table 3, offers a comprehensive analysis of the performance of a classification model on a test dataset, including diverse categories of network activities such as normal behavior and various forms of attacks. The matrix's rows correspond to the actual labels of the data points, while its columns reflect the predicted labels generated by the model.

In the context of Table 3, the rows represent the actual classes of data instances in the test dataset, categorized into normal network behavior and specific attack types such as HTTP flooding, ACK flooding, port scanning, and SYN flooding. For instance, the first row indicates that out of 6000 instances classified as normal, the model correctly identified 5988 as normal. However, it incorrectly classified 3 instances as HTTP flooding, 4 as ACK flooding, 2 as port scanning, and 3 as SYN flooding. This highlights both the model's ability to accurately recognize normal behavior and its susceptibility to misclassifying normal instances as various types of attacks. Similarly, subsequent rows detail the model's performance in detecting specific attack types, showing both correct predictions and misclassifications. Such granularity allows researchers to pinpoint where the model excels and where it needs improvement, guiding further refinement of the model's parameters or training data to enhance its overall accuracy and reliability in real-world cybersecurity applications. The confusion matrix thus provides crucial insights into the strengths and limitations of the classification model, essential for optimizing its performance and robustness against diverse and evolving cyber threats.

Figure 4 shows the detection performance of the system for each attack type. For example, the 5988 nodes were identified as normal nodes out of the 6000 normal nodes assumed. Similarly, 998 malicious nodes of type HTTP flooding were identified among 1000 packet-dropping nodes which were assumed initially. The precision and recall percentages are nearly 99% since the false positives, false negatives are less while true negatives and true positives are more. Hence the proposed QIDS-OA method can be used for successful secured communication.

The study introduced a novel model, QIDS-OA, designed for detecting Denial-of-Service (DOS) attacks by using Entropy and outlier analysis. It was benchmarked against existing methods such as AMM-CNN[19] and an ANN model[17], both established in the field of intrusion detection. In[19], the authors proposed AMM-CNN, which incorporates an attention mechanism to achieve a high accuracy rate of 98.7% in detecting DOS attacks. This was notably superior to the ANN model[17], which achieved a detection accuracy rate of 91.6%. The comparison clearly demonstrated the effectiveness of AMM-CNN over traditional ANN approaches. Additionally[10], implemented a Network Intrusion Detection System (NIDS) using datasets like UNB NSL KDD and UNSW NB15, achieving accuracy rates below 95%. This suggests variability in performance across different datasets and methods.

In contrast, the presented QIDS-OA model employed a sophisticated approach combining Entropy and outlier analysis, resulting in a remarkable detection accuracy rate of 99.897%. This achievement slightly surpasses the performance of AMM-CNN[19], thus establishing QIDS-OA as a state-of-the-art solution for DOS attack detection. Overall, the study underscores the advancements made in intrusion detection through QIDS-OA, highlighting its efficacy in achieving high accuracy rates and outperforming existing models like AMM-CNN[19] in detecting DOS attacks.

Conclusions

The DDoS attacks are more difficult to identify and the negative impact of their attack on the performance of the network is immense. The real users will not get access to the resources once the network is attacked by the DDos. Also, in the case of huge data inputs, traditional machine learning (ML) methods meet several barriers like speed and accuracy. In this paper, we used angle embedding and quantum entanglement for efficient manipulation of the complex structures in classical data with less time and with more accuracy. The study is implemented using Pennylane a quantum library in Python and Qiskit. The proposed method outperforms the existing traditional DDoS detection methods. The experiment results show that both the QIDS-OA model and AMM-CNN models effectively detect DoS attacks. Though both of the models considered a large amount of data processed and the complex feature mapping of the data, the QIDS-OA model had an accuracy rate of 99.897% and outperformed the AMM-CNN model with an attack detection accuracy of 98.7%. The reasons for the outstanding performance of the proposed method over the traditional methods which led to obtaining a high performance in detecting the DDos attacks are.

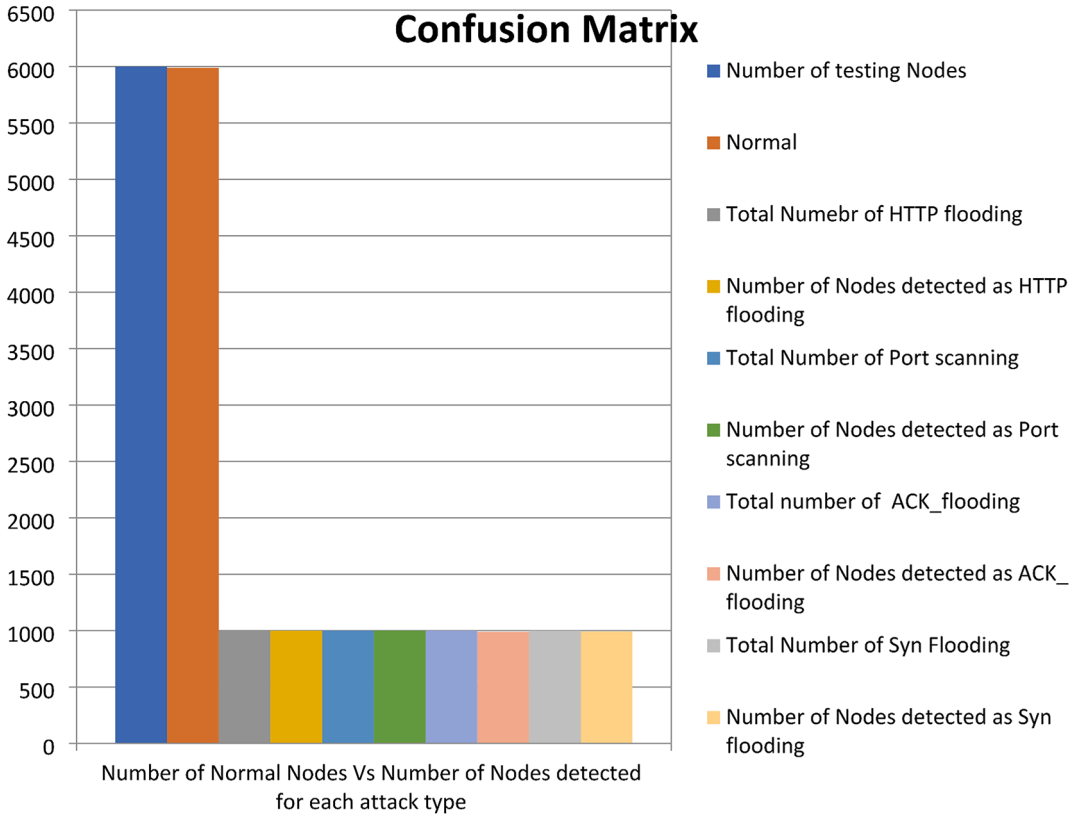

Fig. 4. Detection performance of the system for each attack type.

- The propsoed method applied angle embedding and entaglement on the initial data inputs which increased the performance by using less qubits to represent the classical data and also reduce the compelxity of the detection process .
- The entropy function and outlier analysis are used in the implementation of the detection method which reduces the false alarm rates and finally improves the detection accuracy.

Limitations of the study and future work

This study shows that Quantum Neural Networks (QNNs) simulated with Qiskit and Pennylane frameworks can identify DDoS attacks with promising results; however, there remains space for improvement. In controlled experiments, the use of simulated data yielded important insights into the possible applications of quantum computing in intrusion detection. The model's resilience and adaptability to a wider range of network conditions may be strengthened in the future by adding more varied and real-world datasets. Model performance could be maximized by investigating several feature encoding methods in addition to ZZFeatureMap. Superdense and Hamiltonian Encoding methods could be applied to convert classical data into qubits. Further work could concentrate on enhancing scalability to manage bigger datasets and operational demands in real time, ensuring effective use of computational resources. Broader benchmarking against a wider array of cutting-edge Intrusion Detection System (IDS) systems could offer thorough insights into the model's efficacy and competitive edge, even though comparison analysis with conventional methodologies and modern approaches like AMM-CNN shows encouraging results.

Data availability

The datasets generated and/or analyzed during the current study are not publicly available due to data sharing agreements with collaborating institutions, but are available from the corresponding author on reasonable request.

Received: 20 February 2024; Accepted: 30 October 2024
Published online: 07 November 2024

References

1. Kalinin, M. & Krundyshev, V. Security intrusion detection using quantum machine learning techniques. *J. Comput. Virol. Hacking Techniques*. **19**, 125–136 (2023).
2. Havenstein, C., Thomas, D. & Chandrasekaran, S. Comparisons of performance between 1uantum and classical machine learning. *SMU Data Sci. Rev.* **1** (2019).
3. Thapa, S. & Mailewa, A. The role of intrusion detection/ prevention systems in modern computer networks: A review. In *Conference: Midwest Instruction and Computing Symposium (MICS)*, Vol. 53, 1–14. (2020).
4. Kilincer, I. F., Ertam, F. & Sengur, A. Machine learning methods for cyber security intrusion detection: datasets and comparative study. *Comput. Netw.* **188**, 107840 (2021).
5. Pushpak, S. N. & Jain, S. An introduction to quantum machine learning techniques. In *2021 9th International Conference on Reliability Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, (2021).
6. Cui, Z. et al. Malicious code detection under 5G HetNets based on a multi-objective RBM model. *IEEE Netw.* **35**(2), 82–87 (2021).
7. Parisi *Hands-On Artificial Intelligence for Cybersecurity Implement Smart AI Systems for Preventing Cyber Attacks and Detecting Threats and Network Anomalies* (Packt Publishing, 2019).
8. Heidari, N. J., Navimipour, & Unal, M. Applications of ML/DL in the management of smart cities and societies based on new trends in information technologies: a systematic literature review. *Sustain. Cities Soc.* 104089. (2022).
9. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J. & Ahmad, F. *Network Intrusion Detection System: A Systematic Study of Machine Learning and deep Learning Approaches* (Transactions On Emerging Telecommunications Technologies, 2020).
10. Gouveia & Correia, M. Towards quantum-enhanced machine learning for network intrusion detection. In *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, (2020).
11. Madhavi, S. Anomaly detection using deep neural network Quantum Encoder, ISSN 2409–2665 Journal of Logistics. *Inf. Service Sci.* **9**(2), 118–130. https://doi.org/10.33168/LISS.2022.0207 (2022).
12. Vaghela, K. E-commerce mobile payment risk trend prediction. *Int. J. Smart Bus. Technol.* **8**(2), 31–40 (2020).
13. Ma, W. P. A novel quantum neural network based on multi-level activation function. *Laser Phys. Lett.* **18**(2), 025201 (2021).
14. Zhang, Z. F. Feature selection for network intrusion detection based on quantum evolutionary algorithm. *Comput. Appl.* **33**(05), 1357–1361 (2013).
15. Feng, Y. Y., Zhou, J., Zhang, D. B. & Shi, J. J. Parameterized quantum circuits for learning cooperative quantum teleportation. *Adv. Quantum Technol.* **5**, 2200040 (2022).
16. Zhang, Y. C., Bao, W. S., Wang, X. & Fu, X. Q. Optimized quantum random-walk search algorithm for multi-solution search. *Chin. Phys. B*. **24**, 110309 (2015).
17. Yiyu et al. Detecting quantum attacks: a machine learning based defense strategy for practical continuous-variable quantum key distribution. *New. J. Phys.* **22** 083073 (2020).
18. Alzahrani, A. O. & Alenazi, M. J. Designing a network intrusion detection system based on machine learning for software de-fined networks. *Future Internet,*. **13**(5), 111 (2021).
19. Yin, W., Zhou, Y. & Huang, D. Denial-of-service attack defense strategy for continuous variable Quantum Key distribution via Deep Learning. *Mathematics*. **11**, 2681. https://doi.org/10.3390/math11122681 (2023).
20. Kerenidis, I., Landman, J. & Prakash, A. Quantum algorithms for deep convolutional neural networks. (2020).
21. Ranjbar, L. & Khorsandi. S. A collaborative intrusion detection system against ddos attack in peer to peer network. In *Software Engineering and Computer Systems*, 353–367. (Springer, 2011).
22. Zhang, H., Yi, Y. & Wu, J. Network intrusion detection system based on incremental support vector machine. In *Contemporary Challenges and Solutions in Applied Artificial Intelligence*, 91–96. (Springer, 2013).
23. Payares, E. & Martinez-Santos, J. C. Quantum machine learning for intrusion detection of distributed denial of service attacks: a comparative overview. In *Proceedings of SPIE Quantum Computing, Communication, and Simulation*, 47 (2021).
24. Ma, H. X. et al. Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation. *Phys. Rev. A*. **99**, 022322 (2019).
25. Padamvathi, V., Vardhan, B. V. & Krishna, A. *Quantum Cryptography and Quantum Key Distribution Protocols: A Survey*, 556–562 (IEEE, 2016).

26. Basso Basset, F. et al. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **7**, eabe6379 (2021).
27. Langenfeld, S., Thomas, P., Morin, O. & Rempe, G. Quantum repeater node demonstrating unconditionally secure key distribution. *Phys. Rev. Lett.* **126**, 230506 (2021).
28. Beer, K. et al. Training deep quantum neural networks. *Nat. Commun.* **11**, 808. https://doi.org/10.1038/s41467-020-14454 (2020).
29. Grant, E. et al. Hierarchical quantum classifiers. *Npj Quantum Inf.* **4**, 65 (2018).
30. Khan, A. R. et al. Deep learning for intrusion detection and security of internet of things (IoT): current analysis, challenges, and possible solutions. *Secur. Commun. Netw.* **2022** 4016073. https://doi.org/10.1155/2022/4016073 (2022).
31. Saba, T., Rehman, A., Sadad, T. & Kolivand, H. & Bahaj, S. A. Anomaly-based intrusion detection system for IoT net-worksthrough deep learning model. *Comput. Electr. Eng.*, **99**, Article ID 107810. https://doi.org/10.1038/s41467-020-14454-2 (2022).
32. Shamshirband, S. et al. Co-FQL: Anomaly Detection using Cooperative fuzzy Q-learning in Network. 1345–1357. (2015).
33. Kim T.-H. et al. A methodological approach for assessing amplified reflection distributed denial of service on the internet of things. *Sensors*. **16**(11), 1855 (2016).
34. Kim, T.-H. et al. Estimation of anonymous email network characteristics through statistical disclosure at-tacks. *Sensors*. **16**(11), 1832 (2016).
35. Kim, T.-H. et al. NewDoS defense method based on strong designated. *Verifier Signatures Sens.* **18**(9), 2813 (2018).
36. Kim, T.-H. et al. Machine and deep learning solutions for intrusion detection and prevention in IoTs: a survey. *IEEE Access* **10**, 121173–121192 (2022).
37. Kim, T.-H. et al. Machine and deep learning amalgamation for feature extraction in Industrial Inter-net-of-things. *Comput. Electr. Eng.* **97**, 107610 (2022).
38. Kim, T.-H. et al. A comprehensive survey of authentication methods in internet-of-things and itconjunctions. *J. Netw. Comput. Appl.* **204**, 103414 (2022).
39. Faker, O. & Cagiltay, N. E. Quantum machine learning in intrusion detection systems: a systematic mapping study. In *Intelligent Sustainable Systems. WorldS4 2023. Lecture Notes in Networks and Systems*, (eds Nagar, A. K. et al.) Vol. 817. https://doi.org/10.1007/978-981-99-7886-1_9 (Springer).
40. Alchieri, L., Badalotti, D., Bonardi, P. & Bianco, S. An introduction to quantum machine learning: from quantum logic to quantum deep learning. *Quant. Mach. Intell.* **3**, 1–30 (2021).
41. Nicesio, O. K., Leal, A. G. & Gava, V. L. Quantum machine learning for network intrusion detection systems, a systematic literature review. In *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA*, 1–6 https://doi.org/10.1109/ICAIC57335.2023.10044125 (2023).
42. Rahman, M. A., Shahriar, H., Clincy, V., Hossain, M. F. & Rahman, M. A quantum generative adversarial network-based intrusion detection system. In *IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), Torino, Italy, 2023*, 1810–1815. https://doi.org/10.1109/COMPSAC57700.2023.00280 (2023).
43. Kadry, H., Farouk, A., Zanaty, E. A. & Reyad, O. Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security. *Alex. Eng. J.* **71**, 491–500 https://doi.org/10.1016/j.aej.2023.03.072 (2023).
44. Abbas, A., Khan, M. A., Latif, S., Ajaz, M. & Shah, A. A. Ahmad a new ensemble-based intrusion detection system for internet of things arab. *J. Sci. Eng.* **47**(2), 1805–1819 (2022).

Author contributions

The author Tai Hoon Kim conceptualised the paper and wrote the manuscript. The author S. Madhavi prepared the figures and tables. Both the authors reviewed and finalised the manuscript.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.M.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.