Unsupervised Anomaly Detection in IoMT environments enhanced by Quantum Machine Learning

PhD Dissertation Proposal

by

Mireya Lucia Hernandez Jaimes

Doctoral Advisors:

Dr. Alfonso Martínez Cruz
Dra. Kelsey Alejandra Ramírez Gutiérrez

Instituto Nacional de Astrofísica, Óptica y Electrónica

January, 2025
Santa María de Tonantzintla, Puebla, CP 72840

Contents

Abstract

The growing advances in the Internet of Medical Things (IoMT) have brought several benefits to healthcare services. Regrettably, dense connectivity to the IoMT network provides an attractive target for cyber attackers. In response, researchers have deployed anomaly detection methods based on Machine Learning (ML) to detect cyberattacks. These methods involve recognizing the network patterns of malicious activities. Unfortunately, the lack of labeled data and novel cyberattacks limit the adoption of supervised ML models. Unsupervised ML models have been used as promising solutions. However, their performance remains suboptimal due to the challenges posed by the heterogeneous nature of IoMT data, which complicates the extraction and selection of relevant network traffic features—critical processes to ensure the effectiveness of these methods. Several studies have proposed hybrid solutions that synergize supervised and unsupervised ML models rather than enhancing unsupervised learning to detect unknown security threats in IoMT environments. Beyond these environments, researchers have used advanced unsupervised DL-based algorithms such as generative models and autoencoders. However, they are usually computationally intensive for constrained IoT devices. Moreover, most studies rely on pre-extracted and pre-processed network traffic features, overlooking the challenges present in the current feature engineering processes, such as large number of features, inconsistencies in collecting network traffic data, and feature extraction tools that are incompatible with certain protocols due to the lack of security standards in IoMT. These issues complicate the feature engineering process, which hinders the reliability of anomaly detection. Consequently, cutting-edge technologies are required to find a balance between anomaly detection performance and learning efficiency for anomaly detection in IoMT environments. The inherent parallelism and computational advantage of quantum computing over classical systems have resulted in its application to machine learning, known as Quantum Machine Learning (QML). Recent advances in anomaly detection using QML have demonstrated improved pattern recognition and reduced computational cost. However, the effectiveness of QML in detecting anomalies through unsupervised learning for IoMT environments remains to be demonstrated. Therefore, we propose exploring QML for unsupervised anomaly detection to enhance security in these environments.

1 Introduction

The Internet of Things (IoT) has revolutionized the healthcare industry, giving rise to what is known as the Internet of Medical Things (IoMT), which offers numerous benefits, such as improving patient care and reducing costs for users. This environment requires multiple communication protocols to enable interoperability between different healthcare systems, sensors, and medical devices [1].

Regrettably, this heterogeneity results in devices that frequently lack essential security standards. In addition, their limited resources, constrained memory capacity, limited ability to update their software, and lack of robust cryptographic mechanisms make them highly vulnerable to various types of cyberattacks. Unfortunately, cyber threats are constantly evolving, using new and unseen patterns or methods. Consequently, anomaly detection is increasingly seen as a key component in modern cybersecurity strategies [2–6].

The growing volume of data generated within IoMT environments drives the adoption of ML in cybersecurity. ML algorithms have been widely utilized to detect intrusions and anomalies to secure IoMT environments against cyberattacks [7, 8]. However, the scarcity of labeled data in these environments and novel security threats challenge the full adoption of supervised ML models. Unsupervised ML-based anomaly detection approaches seem a promising solution [9]. Additionally, unsupervised methods have the potential to find intricate patterns and relationships within the data, which could improve model generalization [10]. However, their performance remains inferior compared to supervised ML models, suggesting that extracting and selecting relevant features for anomaly detection is a challenging task in IoMT environments. In response, these approaches are likely to synergize with supervised ML models rather than replace them [11, 12]. However, generating enough outlier data to effectively train these algorithms can be time consuming and sensitive to human error, making it challenging to identify anomalies that were not observed during the learning phase, suggesting that these approaches are not advanced enough to identify unknown malicious patterns efficiently in heterogeneous IoMT environments. Beyond IoMT settings, unsupervised DL-based models have been proposed; however, they are usually expensive for resource-constrained devices. Thus, the development of advanced techniques to improve the detection of anomalies could enhance IoMT security.

A new research field, known as Quantum Machine Learning, has emerged to improve classical solutions due to its ability to process vast amounts of data simultaneously and its potential for enhanced pattern recognition. This novel technology has the potential to improve security solutions, such as anomaly and intrusion detection methods [3, 13, 14]. Although the application of QML for anomaly detection is still in its infancy, previous studies have shown improvements over classical ML models, including enhanced learning efficiency and pattern recognition [15–17]. As a result, this study explores its potential in anomaly detection through unsupervised learning for IoMT environments, which remains to be demonstrated.

1.1 Motivation

Current predictions on the global IoMT market are expected to surpass USD 1,940.75 billion by 2033 [18]. Regrettably, the healthcare industry is one of the three most frequently targeted sectors, alongside educational and government organizations, and experiences an estimated 2,000 weekly cyberattacks [19]. Since 2011, the healthcare industry has endured the most expensive data breach costs compared to other organizations, such as finance, manufacturing, technology, energy, and pharmaceuticals. [20]. As a result, security solutions are necessary to ensure the security of data users and patient safety.

In recent years, Artificial Intelligence (AI) and automation have improved cybersecurity capabilities, including network monitoring and anomaly detection [4]. AI and Machine Learning were ranked as the second most effective strategies in reducing average data breach costs, after employee training as the leading cyber defense [20]. Moreover, the global market for AI in cybersecurity solutions is projected to reach a value of 133.8 billion dollars by 2030 [21].

Anomaly detection in networks can be considered an important step in the detection of a cyberattack [3]. In addition, anomaly detection is becoming an additional layer for proactive protection of IoT-based systems [22]. Although anomaly detection methods based on ML algorithms have proven to be an essential security solution for IoMT environments, the number and variety of cyberattacks continue to increase and these environments will remain attractive to cybercriminals because their complex and heterogeneous nature brings several unsolved security issues [2]. As a result, more advanced security solutions are required [23].

At present, Quantum Computing is becoming more prominent because of its inherent parallelism and computational advantage over classical systems [24]. By 2029, its global market is expected to reach 5.3 billion dollars [25]. A common application of this research field is Quantum Machine Learning (QML), which is expected to introduce several benefits over classical approaches in terms of computational costs and pattern recognition [3, 13, 14, 26, 27]. Although QML-based anomaly detection is at early stages, it shows significant promise [28]. Integrating QML into unsupervised anomaly detection opens up opportunities to leverage its capabilities for identifying anomalies and enhancing IoMT security.

1.2 Justification

In light of the growing popularity of IoMT and the recognition of ML as a key cyber defense strategy, the urgent need for more advanced security approaches capable of detecting anomalies caused by cyberattacks continues to persist. This led us to consider the emerging research field of Quantum Machine Learning as a promising direction to enhance the performance of classical unsupervised ML models in identifying anomalies within IoMT environments.

1.3 Problem Statement

The performance of unsupervised ML-based anomaly detection methods for IoMT environments is still inferior compared to supervised approaches. In response, most methods are likely to synergize with supervised ML models rather than substituting them. Regrettably, these models do not address the detection of anomalies that were not encountered during training, and the scarcity of labeled data further challenges their adoption in IoMT environments. Beyond IoMT, unsupervised DL models have demonstrated promising results; however, they are usually expensive for resource-constrained devices. These challenges present an opportunity for exploration and analysis of advanced technologies, such as Quantum Machine Learning, to develop efficient unsupervised anomaly detection methods and secure IoMT environments against cyberattacks and trade-off anomaly detection performance and learning efficiency.

Formally,

Consider z devices $\{d_1, d_2, \ldots, d_z\}$ that constitute an IoMT architecture of k layers. The network packets are collected in n discrete time intervals with constant length $T = \{t_1, t_2, \ldots, t_n\}$, where each t_i represents the start time of a time interval. Thus, the total network flows, P, monitored throughout the architecture, can be described as follows.

$$P = \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{z} \{p_j(t, L) \mid L \in \{L_1, L_2, \ldots, L_k\}, t \in [t_i, t_{i+1}]\} \right\} \tag{1}$$

where $p_j(t, L)$ represents the network packets generated by device d_j from its respective layer L within a time interval.

Let Φ denote the feature extraction process applied to the P network flows collected over n time intervals:

$$\Phi(P) = \begin{bmatrix} \phi_{1,1} & \phi_{1,2} & \cdots & \phi_{1,m} \\ \phi_{2,1} & \phi_{2,2} & \cdots & \phi_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{n,1} & \phi_{n,2} & \cdots & \phi_{n,m} \end{bmatrix} \tag{2}$$

Where $\phi_{n,m}$ represents the m-th network traffic feature extracted within the n-th time interval.

An anomaly caused by a cyberattack within the network may be reflected in the change of one or more network traffic features, expressed as follows.

$$F_{attack} : \Phi(P)_B \rightarrow \Phi(P)_M \tag{3}$$

Where $\Phi(P)_B$ and $\Phi(P)_M$ represent the network traffic features extracted in a benign and malicious scenario, respectively.

Assume that A is an unsupervised anomaly detection algorithm that maps each feature vector from Eq. 2 to a benign or malicious scenario:

$$A(\Phi(P)) : [\phi_{i,j}]_{j=1}^{m} \rightarrow y_i \tag{4}$$

Where $y_i \in \{Y_{Benign}, Y_{Malicious}\}$ is the type of scenario assigned to the network flow collected within the i-th time interval.

The performance of current unsupervised ML algorithms developed for anomaly detection continues to exhibit suboptimal performance compared to supervised ML models. However, the scarcity of labeled data in IoMT hinders the adoption of supervised ML algorithms. As a result, this study aims to explore the potential of Quantum Machine Learning in enhancing anomaly detection performance to secure IoMT environments.

$$\mathcal{A}_{QML} \longrightarrow \underset{\mathcal{A}_C}{Enhanced}(\mathcal{D}) \tag{5}$$

Where $\mathcal{A}_{QML}$, A_C and $\mathcal{D}$ represent the QML-based algorithm, classical algorithm, and anomaly detection performance, respectively.

1.4 Research Questions

Our research is driven by the following questions that aim to integrate Quantum Machine Learning (QML) into unsupervised anomaly detection for IoMT environments:

- Which quantum operators can transform network traffic features into quantum states for anomaly detection in IoMT environments?
- How to detect network anomalies caused by cyberattacks in IoMT environments by leveraging Quantum Machine Learning?
- How to enhance the performance of current unsupervised ML-based anomaly detection methods for IoMT by using Quantum Machine Learning?

1.5 Hypothesis

The adoption of Quantum Machine Learning into unsupervised anomaly detection for IoMT environments could enhance the balance between anomaly detection performance and learning efficiency. This emerging field holds promise for advancing

the state-of-the-art in unsupervised anomaly detection to secure IoMT environments against cyberattacks.

1.6 Objectives

1.6.1 General Objective

Design an unsupervised anomaly detection method for IoMT environments based on Quantum Machine Learning.

1.6.2 Specific Objectives

1. Design a novel algorithm based on quantum operations to transform IoMT network traffic features into quantum states for unsupervised anomaly detection.
2. Develop a new algorithm that leverages Quantum Machine Learning to detect IoMT network anomalies caused by cyberattacks.
3. Integrate algorithms proposed in objectives 1 and 2 to develop the unsupervised anomaly detection approach for IoMT environments.
4. Achieve comparable performance of classical unsupervised ML-based anomaly detection methods in diverse IoMT environments.

1.7 Expected Contributions

The expected contributions of this study are:

- A new algorithm capable of transforming network traffic features into quantum states for unsupervised anomaly detection in IoMT environments.
- A new unsupervised QML-based anomaly detection method that detects network anomalies caused by cyberattacks with performance comparable to that of classical solutions in IoMT environments.

1.8 Scope and Limitations

It is expected that this study will contribute to future research in unsupervised anomaly detection methods through Quantum Machine Learning for IoMT environments. We examined the limitations and advantages of current ML-based anomaly detection methods. Furthermore, we examine the feature engineering applied to the IoMT network traffic, as the effectiveness of ML models is significantly influenced by the quality of the extracted and selected characteristics.

This work is limited to review and analyze the QML's implementation into anomaly detection in IoMT, excluding works that leverage QML in other applications. Our proposal may not be fully deployed on quantum hardware and could be limited to quantum simulators; however, we will investigate strategies to evaluate our proposal with the challenges associated with the Noisy Intermediate-Scale Quantum (NISQ) era. A QML-based approach could address the problem proposed in this study from a fundamentally different perspective, which may lead to a more effective security solution in IoMT.

1.9 Document Organization

This document is organized as follows. Section 2 briefly describes the main concepts of this study. Section 3 discusses related work to anomaly detection using supervised and unsupervised machine learning and quantum machine learning for IoMT, IoT, and beyond these environments. Section 4 contains the methodology to achieve the objectives and the schedule of activities for the PhD program. Section 5 presents the preliminary results of our study and Section 6 provides the final conclusion.

2 Theoretical Framework

2.1 IoMT Overview

Internet of Medical Things (IoMT) is an application of the Internet of Things (IoT) that improves healthcare services, including real-time monitoring, personal care in medical crises, online treatment, support prevention of diseases, and hospital or clinic administration [29]. It encompasses diverse short-range and long-range communication protocols, such as WiFi, Bluetooth, Radio Frequency Identification (RFID), Zigbee, LoRaWAN, NB-IoT and LTE. However, this leads to limited security features [30].

Therefore, an extensive network with numerous interconnected medical IoMT devices, sensors, and systems will likely be more attractive for a variety of attack scenarios that could jeopardize these entities and their users [31]. Unfortunately, security in IoMT environments remains an open challenge due to its complex nature, heterogeneity, scalability, interoperability, resource-constrained devices, and lack of standard communication protocols [30, 32].

2.2 Machine Learning for Anomaly Detection in IoMT

The advent of artificial intelligence technology, such as Machine Learning and Deep Learning, to secure IoMT environments could provide significant benefits to patient safety and privacy [29, 33]. Machine Learning (ML) algorithms learn from historical data and make future predictions. Deep Learning (DL) is a subset of ML that is inspired by the structure and operation of the human brain. It transforms data into higher-dimensional representations, enabling the model to learn and perform complex and non-linear tasks. The learning process of ML and DL can be classified as follows [34].

- **Supervised Learning** associates the independent characteristics of data samples with a designated dependent attribute (label or class). The learning process can be described as the quest to discover the optimal model that correlates the input with the expected output.
- **Unsupervised Learning** associates the data samples without a pre-designated

dependent attribute (label). ML models trained with this learning process often associate relationships and patterns within the data by finding inherent data structures.

Feature engineering encompasses feature extraction and selection. The first refers to the representation of the input data in its numeric representation. The latter involves selecting the most relevant features for improved ML's performance [35].

Several unsupervised ML-based models have been developed for anomaly detection. An anomaly is generally described as a pattern that diverges considerably from what is considered normal. Several methods use network traffic features to find anomalous patterns derived from cyberattacks. Some of the most frequently used unsupervised ML and DL algorithms in cybersecurity to detect anomalies are listed below [36–38].

A. One-Class Support Vector Machine

The Support Vector Machine (SVM) can classify two classes by mapping all instances to a high-dimensional space and then using a linear SVM to distinguish between them. In contrast, the One-Class SVM (OC-SVM) tries to find a small region that contains most of the one-class instances. Anomaly detection relies on identifying instances outside of this region.

B. Local Outlier Factor

The Local Outlier Factor (LOF) measures the density deviation of a data point relative to its neighbors through the local density principle. It determines outliers by calculating the ratio of an observation's local density to the mean density of its neighboring points.Thus, observations with notably reduced density relative to their surrounding points are recognized as outliers.

C. Isolation Forest

The Isolation Forest (IF) is an ensemble model that detects outliers by performing recursive partitioning of the data with random splits. Anomalies are detected by isolating data points that have low isolation scores or are easier to isolate.

D. Autoencoder

The Autoencoder (AE) is a type of neural network designed to reduce data dimensionality and subsequently reconstruct it. In anomaly detection, the algorithm is trained to learn normal data patterns. Therefore, anomalies are detected by their increased reconstruction error, suggesting a greater difference from the learned usual patterns.

E. Generative Adversarial Networks

The Generative Adversarial Networks (GANs) are based on two neural networks known as the generator and the discriminator. The first produces synthetic samples, while the latter determines whether they are genuine or artificially generated. Thus, a well-trained generator should be able to accurately produce samples of a typical IoMT scenario, which can be utilized for anomaly detection methods.

2.3 Preliminaries of Quantum Computing

This section describes the fundamental concepts of quantum computing for understanding the QML algorithms used for anomaly detection.

A. Quantum bit

A quantum bit (qubit) is the fundamental unit of information utilized to represent data in quantum computing and can be seen as the quantum counterpart of the traditional bit. Qubits are usually described through ortho-normal vectors using ket notation [39, 40]:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{6}$$

B. Superposition

Unlike a classical bit, which can exist in the state 0 or 1, a qubit can be in the superposition of both states, represented as:

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \tag{7}$$

Where α and β represent the complex probabilities amplitudes of each state [40].

Therefore, a dataset of N instances can be expressed as a superposition of all

computational basis states:

$$|\psi\rangle = \sum_{i=0}^{N-1} |d_i\rangle \tag{8}$$

Where each instance of the dataset is encoded as $|d_i\rangle$ [41].

C. Entanglement

This quantum qubit property refers to its ability to interact with other qubits, suggesting that the state of one qubit directly influences the state of the other qubit. Thus, a measurement or any other operation performed on one of the entangled qubits will immediately have an effect on the other qubit, causing it to collapse into a new state. An entangled pair refers to qubit pairs that are related or connected. An intriguing aspect of entanglement is that when we measure the state of a qubit, its entangled partner will inherently show the opposite result of that measurement [42].

D. Measurement

It is a crucial process to obtain the expected results after computing quantum algorithms, where the result values are represented in classical bits. The qubits are measured after a quantum operation to understand what occurs. This means that qubits will collapse into one of the superposed states [40].

E. Quantum Gates

Quantum gates are unitary operators described as unitary matrices that transform a state vector into a new one without modifying its norm. Operations include gates that act on a single qubit state or on pairs of qubits [40]. Some examples are presented below, and the following sections explain how they can be used.

$$R_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \tag{9}$$

$$\text{Hadamard (H)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{10}$$

$$\text{Pauli-Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{11}$$

$$\text{Pauli-Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{12}$$

$$\text{Pauli-X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{13}$$

2.4 Quantum Machine Learning for Anomaly Detection

Quantum Machine Learning (QML) is an emerging research field in computer sciences that integrates ML and quantum operations to solve the tasks faced in classical ML and improve traditional solutions [13].

This integration can be classified into four principal types:

- *Classical-Classical:* quantum-inspired classical algorithms applied to classical data.
- *Classical-Quantum:* quantum algorithms applied to classical data.
- *Quantum-Classical:* classical algorithms applied to quantum data.
- *Quantum-Quantum:* quantum algorithms applied to quantum data.

In the literature, classical-quantum and classical-classical approaches are the most explored [40, 43].

2.4.1 Feature Mapping

Feature mapping in quantum machine learning refers to the transformation of classical data into quantum states in a high-dimensional Hilbert space. The process involves converting a data point x into a collection of gate parameters for a quantum circuit, generating a quantum state $|\psi_x\rangle$ [44]. There are different feature mapping methods in the literature described as follows.

A. Angle embedding

This technique maps a collection of N features onto the rotation angles of n qubits, where $N \leq n$, employing the R_x gate, which constitutes one of the rotation operators and performs a single-qubit rotation around the angle θ, expressed in Equation 9.

B. Amplitude embedding

This method involves encoding parameters into the amplitudes of a state. The circuit P_{input} is used to prepare states by encoding the dataset into the quantum system's state. It maps an input data point $x \in \mathbb{R}^n$ to a vector of amplitudes $P(x)$ of $\log \frac{n}{2}$ dimension that defines the quantum state $|P(x)\rangle$ [45].

C. Variational embedding or Variational Quantum Circuit (VQC)

This method encodes parameters into quantum circuits. Assume that every data point d_i within the dataset D possesses N features, such that each feature can be represented with the parameter θ_i at the initial quantum state $|0\rangle$ of a qubit [45].

D. ZZ Feature Map

This technique is a second-order Pauli-Z evolution circuit that performs a non-linear mapping of the n classical features to the n qubits. It involves applying pairwise interactions between qubits using the Pauli-Z gate, defined in Equation 11. ZZ string refers to the application of this Pauli's gate on two qubits [46], expressed as follows.

$$ZZ = Z \otimes Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{14}$$

2.4.2 QML algorithms

This section presents the most frequent quantum algorithms for anomaly detection in cybersecurity.

A. Quantum Support Vector Machine

The Quantum Support Vector Machine (QSVM) performs the Least Squares

SVM (LS-SVM) using quantum computers. The LS-SVM is a version of the SVM that applies the least squares linear system instead of the loss function [44]. Rather than using an external feature mapping technique to convert classical data to quantum states, it directly computes the quantum kernel, which involves a quantum circuit that encompasses the Hadamard and Pauli-Z gates, expressed in Equations 10 and 11, respectively [41, 44]. Thus, during training process, the QSVM encodes the classical data into the quantum feature space through the quantum kernel, which capture intricate patterns of the input data. The algorithm also identifies the support vectors to define the optimal hyperplane in the quantum feature space [47].

B. Quantum Neural Network

The Quantum Neural Network (QNN) encompasses an input, output, and L hidden layers, similar to its classical counterpart. The key difference are the hidden layers of qubits, which operate in the initial state of the input qubits and typically generate a mixed state for the output qubits [48]. Training a quantum-based neural network involves finding the most optimal parameters of the hidden layers to reduce the loss error, similar to the classical approach. However, classical optimizers such as descent must be adjusted for a quantum framework [47].

3 State-of-the-Art

3.1 ML-driven Anomaly Detection for IoMT

This section discusses current anomaly detection methods based on supervised and unsupervised ML models for IoMT environments.

Several anomaly detection methods are based on supervised ML and DL algorithms, including Decision Tree (DT), Random Forest (RF), Logistic Regression (LR), Artificial Neural Networks (ANN), and Recurrent Neural Networks (RNN). Some of these works focus mainly on developing new IoMT datasets [12, 49–54] to evaluate anomaly and intrusion detection methods, integrate explainable artificial intelligence techniques [55–60], apply Federated Learning [55, 61, 62], integrate blockchain technology [63], and improve anomaly detection performance through feature selection techniques [54, 57, 64–72], hyperparameter tuning [60, 64, 73–75], and custom supervised ML or DL algorithms [74, 76–81].

Few studies assessed the effectiveness of unsupervised learning for anomaly detection in securing IoMT networks. For instance, Ahmed et al. [50] presented a novel IoMT dataset called ECU-IoHT. They evaluated this dataset by splitting it into different attack scenarios to individually assess each type of attack and applying several unsupervised ML algorithms, such as Local Outlier Factor (LOF), Influenced Outlierness (INFLO), and K-Nearest Neighbor (K-NN). Unfortunately, the experimental results are presented solely through non-labeled visual representations, making it challenging to determine exact values, with no detailed data provided in the text. The performance metrics used were F1-score and Area Under the Curve (AUC). INFLO algorithm appears to demonstrate the best anomaly detection performance.

Zubair et al. [12] introduced a new IoMT dataset, which was divided into two subsets: one comprising devices that use the Basic Rate / Enhanced Data Rate (BR / EDR) protocol and the other consisting of Bluetooth Low Energy (BLE). The ecosystem based on BR / EDR was evaluated using five supervised and four unsupervised ML algorithms, such as LR, DT, SVM, RF, MLP, LOF, K-means, Naive Bayes (NB), and Isolation Forest (IF). The NB algorithm, configured as an unsupervised approach, outperformed the other unsupervised ML models with a 92.4% accuracy, 77.15% F1-score, 63.68% Recall, and an area under the curve (AUC)

score of 82%.

Zukaib et al. [11] proposed an intrusion detection system based on meta-learning, which consists of multiple detection layers that leverage various supervised ML models, including DT, RF, ANN, Adaptive Boosting (AdaBoost), Multi-Layer Perceptron (MLP), eXtreme Gradient Boosting (XGBoost), and an unsupervised Mean-Shift Clustering (MS-CL) model for detecting known and unknown attacks, respectively. Although the MS-CL is in the second layer of attack detection, it achieves an accuracy, precision, recall, and F1-score of 62.86%, 64.54%, 62.86%, and 61.75%, respectively. In response, two supervised RF models were integrated into the third detection layer to reduce false positive and false negative rates of the MS-CL model, achieving equal accuracy, precision, recall, and F1-score of 99.50%.

Several anomaly detection methods for IoMT rely on supervised ML models. However, the scarcity of labeled data limits its widespread integration into IoMT environments, and its effectiveness in detecting unknown attacks is uncertain. Additionally, the performance of unsupervised ML-based anomaly detection methods needs improvements, and in response, current works still leverage supervised ML algorithms for enhanced anomaly detection. Unfortunately, the challenges posed by unknown attacks and the limited availability of labeled data persist. As a result, more advanced techniques are required to improve the effectiveness of unsupervised learning to detect anomalies presented in IoMT networks.

3.2 IoMT Network Traffic characterization

The effectiveness of any ML-based method is significantly dependent on the quality and relevance of the characteristics, suggesting that it is crucial to consider feature extraction and selection techniques in the development of these methods. Thus, this section outlines the feature engineering techniques applied in current approaches for IoMT environments.

Recently, there has been notable growth in generating datasets that include IoMT network traffic, particularly due to the necessity to assess ML-driven security solutions, such as Integrated Clinical Environment (ICU) [54], Enhanced Healthcare Monitoring System (EHMS) [49], Intensive Care Unit (ICU) [51], ECU Internet of Health Things (ECU-IoHT) [50], BlueTack [12], CICIoMT2024 [52], and IoMT

Traffic Data [53] dataset, as shown in Table 3.2. Some of these datasets offer only pre-extracted network traffic features without providing the raw network data (PCAP files), such as EHMS, ECU-IoHT, and BlueTack dataset. Regrettably, in the absence of raw data, the extraction of novel features using alternative techniques is unattainable. Moreover, it is crucial that the raw data available is sufficient to generate relevant feature vectors that accurately represent the network traffic in IoMT environments for effective anomaly detection, implying that the size of PCAP (Packet Capture) files is important. For example, the IoMT Traffic Data and CICIoMT2024 datasets provide more than 10 million network packets. The ICE dataset is slightly smaller, containing roughly 9 million network packets. On the other hand, the ICU provides approximately 187 thousand network packets.

IoMT dataset	Year	Devices	Attacks	Features	Feature Extractor Tool	Raw Data Available
ICE	2019	5	4	32	Argus	✓
EHMS	2020	4	2	35	Argus	X
ICU	2021	32	4	52	Wireshark	✓
ECU-IoHT	2021	8	6	9	Argus and Wireshark	X
BlueTack	2022	3	4	19	-	X
CICIoMT	2024	40	18	39	Dpkt	✓
IoMT Traffic Data	2024	-	10	30	Zeek Flowmeter and Tshark	✓

Table 1: Overview of IoMT datasets.

Most works proposing a novel IoMT dataset do not define the network flows and neither do they explain how network traffic features are extracted using different packet-sniffing tools. Typically, a network flow represents a sequence of packets that share common characteristics, such as source and destination IP addresses, source and destination ports, and protocol type. Alternatively, a flow can also be defined based on the timestamps of the network packets. For instance, the features from the CICIoMT dataset were extracted using sliding windows of 10 and 100 network packets, with different scenarios employing either a 10-packet window or a 100-packet window. However, this inconsistency in window size limits the evaluation of ML-driven security solutions, which affects the generalizability of anomaly detection methods, as they may not perform equally well across different attack scenarios and packet windows. The IoMT Traffic Data dataset collects network flows based on common characteristics of the IP and Bluetooth protocols, generating a distinct set of features for each type of protocol. This situation is also presented in the pre-extracted network features from the CICIoMT dataset, which challenges the development of ML-anomaly detection models capable of generalizing across these

sets of features. Moreover, this could involve challenges related to the heterogeneity of handling large-scale feature sets, such higher computational costs. Additionally, the IoMT Traffic dataset offers not only a flow-based feature set but also a packet-based one. However, handling a large volume of features becomes computationally expensive and time consuming, especially considering the diverse range of devices and communication protocols in IoMT environments. Regarding the ICU and ICE datasets, the first does not define the flow collection process, making it difficult to reproduce and compare the performance of ML-driven solutions under the same conditions. The ICE dataset provides pre-extracted features from 10-second time windows. However, the definition of this time window is unclear and it does not guarantee that it will be sufficient to detect other types of attack, as the dataset contains only ransomware family attacks.

Table 2 summarizes the pre-extracted network traffic features of the IoMT datasets, which are classified based on flow-based which describes in general terms the sequence of network packets, packet-based refers to those characteristics extracting metainformation , typical non-numeric, and the Additionally, another challenge related to pre-extracted network features is the efficiency of the tool, as some tools do not support all protocols, limiting their ability to extract some type of feature across a wide range of protocols that may be presented within an IoMT environment.

Type	Network Traffic Features
	Source/Destination bytes, load, missing bytes, active inter packets, total network packets.
	Dropped network packets.
Flow-based	Duration.
	Network packets per second.
	Source/Destination Jitter.
	Speed of data transmission.
	Maximum, Minimum, Average, Standard Deviation of network packets size.
	Source/Destination IP address.
Packet-based	Type of protocol.
	Timestamp.
TCP-based	Length of TCP header, flags (e.g., ack, fin, psh, syn, reset, urg), total number of SYN/ ACK / FIN /RST packets, and checksum.
UDP-based	Counter for UDP protocol.
IP-based	Time to Live (TTL).
MQTT-based	Client ID, flags (e.g. conack, passwd, qos, willflag), length of the message, and type of message (e.g., Connect, publish).
Bluetooth-based	Length of the L2CAP based packet, events generated by HCI, and connection HCI ACL.
Other protocols	Counter indicating the presence of HTTP, DNS, Telnet, SMTP, SSH, ICMP, IGMP, and IPv.

Table 2: Summary of network traffic features used in current ML-based anomaly detection methods for IoMT.

In some ML-based anomaly detection methods for IoMT, feature selection has been applied to mitigate overfitting and enhance model generalization. For example, Dhanya et al.[75] applied the AutoEncoder (AE) model to reduce the dimensionality of the features of the network traffic by selecting the most relevant network features. The supervised XGBoost algorithm optimized by the Genetic Algorithm (GA) was used for anomaly detection. Al-Hawawreh et al. [82] evaluated a Constractive Deep AE for data fusion, as it prioritizes feature representation over reconstruction. Moreover, they proposed a supervised hybrid Quantum Deep Learning approach for anomaly detection, discussed in the following section. Wagan et al. [83] used the

dynamic Fuzzy C-Means clustering and proposed two customized Long Short Term Memory (LSTM) algorithms for feature selection and anomaly detection. However, these works utilize the pre-extracted network traffic features, and the issues related to this remain unsolved.

Most works rely on pre-extracted network features to evaluate the effectiveness of ML and DL models in detecting anomalies caused by cyberattacks. However, the pre-extracted network traffic features provided for the IoMT datasets challenge the generalization of current approaches. Unfortunately, limited attention has been directed to how different network flow exporter tools and feature engineering techniques could impact the development of ML-based anomaly detection methods in IoMT environments. Additionally, given the extensive number of features and the variety in devices, it is crucial to balance computational efficiency for resource-constrained devices with ML performance. Therefore, innovative methods must be developed to address these issues and improve feature engineering to boost anomaly detection in IoMT settings.

3.3 Unsupervised Anomaly Detection for IoT

This section explores unsupervised anomaly detection methods for IoT-based environments, beyond IoMT settings. We provide further insights into advances in unsupervised learning for anomaly detection using network traffic information.

Zixu et al. [84] presented an anomaly detection method based on the Generative Adversarial Network (GAN) and autoencoder (AE) due to the scarcity of large amounts of labeled samples in IoT. The proposal is based on a hierarchical architecture for a distributed IoT network, where GAN models are trained locally and their parameters are sent to a central controller using encrypted channels for data privacy. New samples are created through a generator model using these parameters at the central controller, which are used to train an AE model for anomaly detection. The results show higher accuracy, precision, recall, and F1-score compared to traditional unsupervised ML algorithms used for anomaly detection, including K-means, IF, OCSVM, and LOF.

Alsaedi et al. [85] developed an unsupervised misbehavior detection (USMD) framework to identify zero-dat attacks on cyber-physical systems. The USMD con-

sists of a deep autoencoder architecture that incorporates a temporal dependencies network based on the LSTM model and a temporal attention unit. They evaluated their proposal on various datasets, including sensor data from various environments such as the Internet of Things, a large water treatment plant, a water distribution testbed, and a small-scale gas pipeline testbed. In the IoT environment, USMD outperforms other methods in terms of recall, F1-score, and AUC score. The Isolation Forest model achieved the highest precision. For the other datasets, USMD consistently delivered the best results in terms of F1-score and AUC score.

Arifeen et al. [86] introduced a Hyper-ledger Fabric distributed ledger technology, which integrates the autoencoder model into a chaincode consensus mechanism to identify anomalous data before storing them on the blockchain. The Minifabric tool was used to implement the proposed AE-based chaincode consensus mechanism, which was trained using 80 IoT network features. The proposed blockchain showed a maximum latency of 3.19 seconds and a throughput of 1.3 TPS. The performance in anomaly detection exhibited an accuracy, precision, and recall range of 0.89 to 0.96. However, more research is needed to evaluate the compatibility of using AE in blockchain for IoT, particularly compared to current consensus mechanisms.

Boppana et al. [87] proposed the GAN-AE method to detect unknown intrusions in IoT environments for devices based on the MQTT protocol, which integrates the autoencoder into a generative adversarial network. The proposal achieved higher accuracy, precision, recall, and F1-score than the traditional autoencoder and achieved comparable performance compared to a supervised intrusion detection method proposed in the literature. Unfortunately, it is limited to the MQTT protocol, whereas IoT encompasses a wide range of protocols.

Sharmila et al. [88] introduced a Quantized Autoencoder (QAE) for intrusion detection to enhance computational efficiency in IoT devices. The AE model integrates post-training optimization techniques such as pruning, clustering, and quantization to reduce its complexity. Pruning involves selecting the most relevant neurons while clustering the layer weights into clusters. The last technique, quantization, refers to the process of converting the 32-bit floating point weights and biases into 8-bit unsigned integers and 16-bit floating point representations. The results demonstrated reduced memory utilization and CPU requirements while maintaining anomaly detection performance comparable to the traditional AE model. Unfortunately, this proposal was evaluated on a single IoT-based dataset containing only

two types of cyberattacks.

Vaisakhkrishnan et al. [89] proposed an intrusion detection system and evaluated four different DL algorithms, including an unsupervised learning model, the autoencoder. They used the extension of stochastic gradient descent, called Adam optimizer, to strengthen the efficacy of DL-based intrusion detection systems for IoT-based environments, such as healthcare organizations. The results show that autoencoder achieves comparable performance in terms of accuracy, precision, recall, and F1 score compared to supervised DL-based models, such as CNN, Transformer, and LSTM. Despite their effectiveness, these models might put a strain on resource-limited IoMT devices.

Recently, there is significant interest in unsupervised DL-based models, particularly generative models and autoencoders. Unfortunately, these models are usually expensive for resource-constraint environments such as IoMT. Only one work focused on developing a lightweight AE model. In addition, It was observed that many studies rely on a single dataset to evaluate their proposals, which restricts their ability to be assessed in various IoT environments. Although these DL-driven anomaly detection methods achieve performance comparable to traditional supervised and unsupervised ML-based methods, a balance between anomaly detection performance and learning efficiency is required, along with evaluations with extensive attacks and IoT applications such as IoMT.

3.4 QML-driven Anomaly Detection

This section introduces anomaly detection methods based on Quantum Machine Learning (QML). Since the application of QML into anomaly detection methods is still in its early stages, we also include works beyond IoT-based environments.

Two studies specifically addressed IoMT environments. For instance, Laxminarayana et al. [17] proposed an activation function for a quantum-based deep learning model (QDL) to detect intrusions using the KDDCup99 dataset. Although this dataset does not reflect the main characteristics of an IoMT network, this work introduced an IoMT architecture to illustrate the role of the proposed system in detecting malicious intrusions. The proposed QDL-based architecture consists of a parameterized quantum circuit within the classical neural network, resulting in a

small architecture capable of recognizing significant patterns. The results showed comparable accuracy performance compared to more complex classical models, including RNN, CNN, and LSTM algorithms. However, the dataset used may not reflect the main characteristics of an IoMT environment. The second work was conducted by Al-Hawawreh et al. [82], which introduced differential privacy techniques to protect sensitive IoMT data during the learning process of the proposed quantum-based neuronal network to detect attacks. The evaluations were performed on two IoMT datasets known as EHMS and ICU, which contain network traffic generated by medical devices in normal conditions and during a cyberattack. The classical data was transformed using the amplitude embedding technique. The quantum-based neuronal network uses a variational quantum circuit within the hidden layer of the network. The findings indicated similar outcomes for accuracy, precision, recall, and F1-score, regardless of the use of privacy techniques. In addition, the accuracy and recall results were similar compared to previous studies. However, the performance of its classical counterpart remains uncertain.

Beyond IoT-based environments, fourteenth works introduced Quantum Machine Learning into anomaly detection using network traffic information, described as follows. Huang et al. [90] used the normalized mutual information (NMI) technique and the Quantum Wavelet Neural Network (QWNN) for feature selection and anomaly detection, respectively, using the KDDCup99 dataset. The QWNN outperformed the k-means, KNN, PCA-SVM, K-means-NB, and NMI-ANN approaches regarding false positive and true positive rates, while achieving the lowest time complexity.

Gouveia et al. [41] evaluated the Quantum Support Vector Machine (QSVM) algorithm to detect intrusions on the NSL-KDD and UNSW-NB15 datasets, which includes network traffic data from malicious and benign scenarios. The autoencoder model was introduced to encode the network flows and improve QSVM's performance. The experimental results revealed accuracy performance comparable to that of the classical SVM algorithm.

Kalinin et al. [91] proposed an encoding technique to transform network traffic characteristics from the IoT Network Intrusion dataset into qubit representations. In addition, they evaluated the QSVM model as an intrusion detection algorithm to classify different types of cyberattacks, such as HTTP-based flooding and port scanning. Although it demonstrated higher accuracy than classical SVM in most

cases, its performance in detecting SYN flooding and OS scanning attacks requires improvement. Moreover, the QSVM was notably faster than SVM during the processing of massive data.

Payares et al. [44] evaluated the performance of the QSVM, a hybrid Quantum Neural Network (H-QNN), and an ensemble model based on quantum principles in intrusion detection using the CIC-DDoS2019 dataset, which consists of distributed denial of service attacks. They applied Principal Component Analysis (PCA) for feature dimensionality reduction and used the angle embedding method to encode the network traffic features into qubits. The H-QNN outperformed in terms of accuracy, recall, precision, F1-score, and memory usage. Unfortunately, a comparison with the classical counterparts has been overlooked.

Zhang et al. [92] introduced a Quantum Neural Network (QNN) to detect attacks using network traffic collected in 2005 by other authors. The results show a low F1-score and recall, suggesting information loss during the preprocessing step due to the limited qubits required to represent all characteristics of the network traffic. However, this architecture helps to prevent the gradient explosion problem faced by its classical counterpart.

Gong et al. [45] proposed a Variational Quantum Neural Network (VQNN) composed of three layers, which implements the principles of a Variational Quantum Circuit (VQC), to detect malicious intrusions in networks using five features of the KDDCup99 dataset. The VQNN with eight single-layer VQC outperformed classical models including ANN, SVM, KNN, NB, and DT with respect to false positive and negative rates, precision, recall, and F1 score. Moreover, it exhibited lower performance in detecting anomalies on NISQ-based devices relative to the simulator, yet it still surpassed the SVM and NB algorithms.

Kalinin et al. [93] compared the performance of the QSVM and Quantum Convolution Neural Network (QCNN) models in detecting intrusions using a network dataset. In most attack types, QSVM exhibited a greater area under the curve compared to the classical SVM, which accurately identified only two types of attack. Similarly, QCNN outperformed the classical CNN algorithm in most types of attacks. Additionally, both quantum-based models showed training times shorter than those of their classical counterparts with large input data, and this advantage increased as the input data size was further expanded.

Alomari et al. [46] applied several preprocessing techniques, such as Min-Max, standard scaler, FastICA, and ZZFeatureMap, to improve QSVM's performance in detecting distributed denial of service attacks. This approach outperformed other quantum-based methods, including traditional QSVM, in accuracy, recall, precision, F1-score, and error rate. However, the results obtained within an NISQ framework were slightly lower.

Rahman et al. [94] assessed the effectiveness of two parameterized quantum circuits utilizing two classical optimizers and the NSL-KDD dataset to identify network attacks. The PCA algorithm was applied to reduce the feature space. Next, the ZZFeatureMap technique was used to transform the classical data into quantum states. The EfficientSU2 circuit optimized by the COBYLA technique showed the highest accuracy performance with the top three features selected by PCA. However, further comparisons with classical solutions for this task are absent; comparisons are made solely with a study that evaluated a variational quantum classifier on the IRIS dataset, which is used for flower species classification.

Barletta et al. [16] integrated QBoost, a QML algorithm deployed in the D-Wave Leap Quantum Cloud (DLQC), with QRadar, a SIEM system provided by IBM. This hybrid method uses QBoost for intrusion detection and QRadar for configuring rules to identify the known behavior of cyberattacks. This proposal was evaluated in the CIC-IoT-2023 dataset, which contains network cyberattacks, such as DoS and spoofing attacks. The accuracy, precision, recall, and F1-score outcomes of QBoost were compared to those of the RF algorithm. Training and prediction times were significantly reduced with the QBoost algorithm.

Kukliansky et al. [23] introduced a Quantum Neural Network (QNN) into intrusion detection systems. They assessed a smaller version of their proposal on the lonQ's Aria-1 quantum computer using the UNSW-NB15 dataset, which encompasses malicious and typical network traffic. In addition, they proposed the certainty factor, a novel metric to evaluate the susceptibility of quantum results to errors caused by noise. The QNN architecture relies on an ultralean circuit to consider the noise constraints of quantum devices. Furthermore, a new classical data encoding technique is introduced to reduce quantum resources. This work showed comparable F1-score performance compared to classical methods and demonstrated its potential within a NISQ framework.

Bhattacharya et al. [95] proposed a Quantum Neural Network (QNN) to secure

Industrial Internet of Things (IIoT) networks against cyberattacks. The CIC-IDS-2018 dataset was supplemented with real-time IIoT data to evaluate its performance in detecting cryptojacking attacks. This method consists of two levels: detection and filtration. The detection level encompasses the QNN model, which consists of three layers that extract different features from the users. The weights are iteratively computed through a new quantum-based optimizer. The classification of malicious and benign network traffic is performed by the filtration layer through a threshold computed using a novel quantum metric. This approach outperformed two quantum-based methods regarding accuracy, F1-score, recall, false error rate, and mean absolute percentage error. Regrettably, no comparisons with classical approaches are presented.

Abreu et al. [47] investigated the effectiveness of VQC, QSVM, and QCNN in identifying network cyberattacks. All quantum-based models achieved different performance across six NISQ-based devices, showcasing the distinctive influence of noise from each device. The authors compared their best F1-score performance with that of the RF, SVM, and CNN algorithms across all datasets, demonstrating that quantum-based models outperform classical models, particularly the VQC approach. However, their F1-score in the multi-class classification of attacks decreased, and in some cases, classical models outperformed them. Therefore, even though the results are promising, the performance variations indicate that quantum-based models may offer potential benefits in specific situations, but they have not yet completely outperformed classical models.

Kumar et al. [96] introduced an intrusion detection system based on QSVM for small data training sets. They utilize eight attributes derived from flows based on the 5-tuple, consisting of sequential network packets with the same source and destination IP address, source and destination ports, and type of protocol. However, some cyberattacks may go undetected using these types of feature, such as Man in the Middle (MiTM) attacks like IP spoofing, or attacks that leverage protocols other than IP. This is particularly critical to consider given the heterogeneity of IoT environments. In addition, this study compared different feature maps, including the ZZFeature map, ZFeature map, and PauliFeature, to assess the effects of modifications in quantum states derived from specific feature values on the performance of the QSV. The proposed system outperforms classical solutions, including DT, GNB, KNN, RF, SVM, ANN, CNN, and LSTM.

Furthermore, we identified three works that leveraged quantum computing to enhance classical ML algorithms for detecting anomalies in networks, described below. Chen et al. [97] developed the QALO-K approach to cluster data and detect network intrusions, which consists of a classical k-means classifier optimized by a quantum-driven ant lion algorithm. They evaluated this proposal on seven datasets for clustering analysis; each dataset represents different types of data and attributes for different purposes, such as flower species classification. This approach outperformed the related work regarding the sum of intra-cluster distance, excluding one dataset. Moreover, it demonstrated faster convergence than the k-means algorithm optimized by the classical ant lion Optimizer (ALO-k). For intrusion detection, the proposal was evaluated solely on the KDDCup99 dataset, which contains malicious and typical network traffic. The QALO-k method achieved a higher accuracy and detection rate than the ALO-k and K-means models.

Li et al. [15] used quantum annealing to select relevant features from the NSL-KDD dataset, which consists of four types of network attacks. They performed feature correlation through Pearson's correlation coefficient and mutual information. Next, these features were used to train the Support Vector Machine (SVM) classifier. This approach reduced feature selection time and training time in comparison to traditional feature selection techniques, such as Particle Swarm Optimization (PSO), while achieving comparable accuracy.

Dong et al. [98] proposed a quantum-based beetle swarm algorithm to optimize the Incremental Extreme Learning Machine (IELM) for intrusion detection using the KDDCup99 and CIC-IDS-2017 datasets. The proposed optimizer integrates classical swarm and beetle antennae algorithms using quantum principles to compute the weights and thresholds of the IELM model. The results showed a reduced computational complexity of the ELM while improving its accuracy and convergence rate. Furthermore, it showed similar results for precision, F1 score and true positive rate, while achieving a lower false positive rate compared to IELM optimized by the genetic algorithm and PSO, as well as other classical models such as SVM.

Regarding unsupervised learning, only one work leveraged quantum principles for anomaly detection beyond IoMT and IoT settings. Guo et al. [99] introduced a quantum version of the Local Outlier Factor (LOF) algorithm, which is frequently used for unsupervised anomaly detection. This quantum LOF method follows three steps as well, with its main distinctions being the incorporation of amplitude esti-

mation, minimum search, QRAM data structure, quantum amplitude estimation, and Grover's algorithm. The complexity analysis revealed an exponential speedup regarding the number of data points and their dimension compared to the classical LOF. Unfortunately, the anomaly detection performance was not analyzed.

Most QML-based anomaly detection approaches demonstrate performance comparable to that of DL-based models, with simpler architectures and improved training and testing times. It appears that quantum feature mapping can capture complex patterns and correlation between features. However, more analysis of the performance of these novel models is needed, since several of the existing works overlook comparisons with classical systems, so further assessment is required to fully understand the limitations and advantages of QML over the classical solutions. Nine works proposed a novel QML model, while other nine studies evaluated existing QML algorithms for anomaly detection, with QSVM being the most popular. Unfortunately, the selected datasets to evaluate their performance are typical outdated and do not reflect complex environments such as IoT and IoMT. Moreover, only one study proposed an unsupervised QML model; however, its anomaly detection performance was not assessed, only its complexity.

3.5 Discussion

Supervised ML models have been widely used for anomaly detection in IoMT environments; however, their effectiveness in detecting unknown attacks is uncertain and the scarcity of labeled data in these environments limits its adoption. In response, a few studies have explored unsupervised ML models, but their lower performance has led to efforts to synergize them with supervised ML algorithms for improved results. On the other hand, current methods rely on pre-extracted network features, which limit the generalization capability of ML models due to inconsistencies in pre-processed IoMT datasets and feature extraction tools that are not specifically designed for IoMT environments or do not support all available protocols. Furthermore, given the large number of features and the diversity of IoMT devices, careful attention to feature engineering is crucial in the development of these methods.

Beyond IoMT, unsupervised DL-based models such as generative adversarial networks and autoencoders have gained popularity for detecting anomalies in IoT. However, although their performance shows comparable performance to those

of supervised and unsupervised ML models for IoMT, they are usually expensive for resource-constraint devices. Thus, advanced technologies are required to develop simpler architectures and comparable detection performance for unsupervised anomaly detection in IoMT, such as quantum machine learning. Although this emerging technology is still in its infancy, it has shown promising results in supervised anomaly detection with respect to pattern recognition and learning efficiency; however, robust analysis and assessment of their benefits and limitations are still missing, particularly with respect to unsupervised anomaly detection for IoMT environments.

4 Research Proposal

4.1 Methodology

To achieve the objectives of this study, we propose the following methodology, as illustrated in Figure 1.

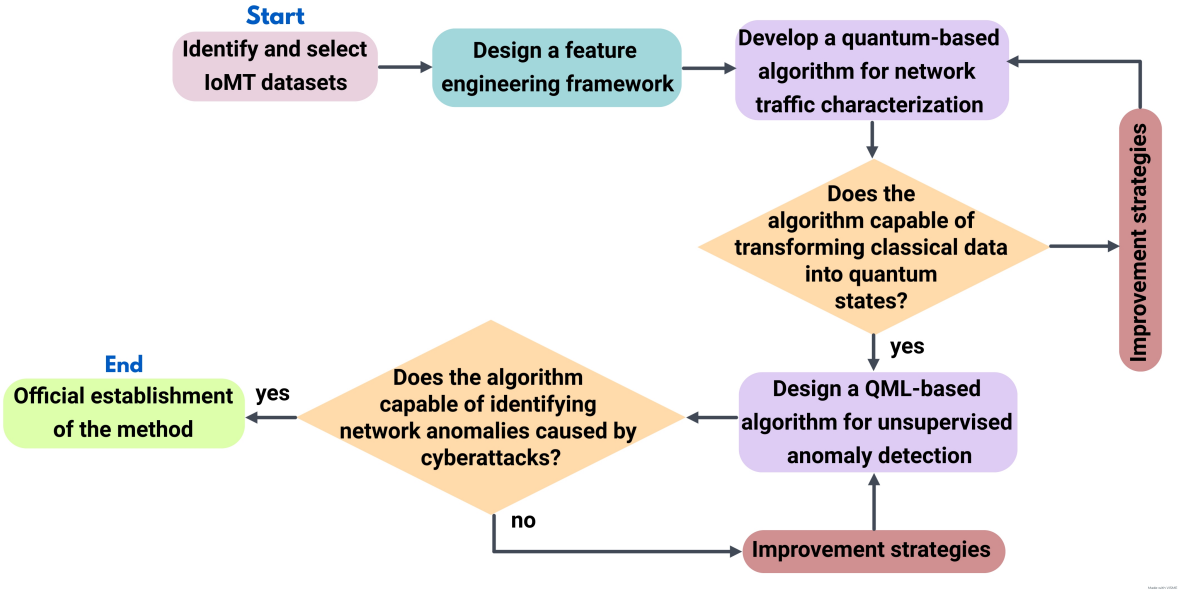

Figure 1: Proposed methodology.

- Identify and select IoMT datasets:
  - Obtain datasets based on IoMT environments, specifically designed for anomaly detection related to cyberattacks.
  - Review and analyze the key characteristics of IoMT environments as reflected in datasets.
  - Select well-suited IoMT datasets that align closely with the specific requirements of our study.
- Design a feature engineering framework:
  - Assess the most common feature extraction and selection techniques used in IoMT networks.

  - Analyze the different network traffic features and preprocessing steps used to model ML algorithms for anomaly detection in IoMT and beyond IoMT environments.
  - Devise a strategy to characterize network traffic for unsupervised anomaly detection in IoMT.

- Develop a quantum-based algorithm for network traffic characterization:
  - Identify and examine algorithms centered on quantum principles that can convert classical data into quantum states.
  - Evaluate and analyze the use of quantum operators to convert network traffic characteristics into quantum states.
  - Design an algorithm using the most appropriate quantum operators that align with our goal of developing an unsupervised anomaly detection method.

- Design a QML-based algorithm for unsupervised anomaly detection:
  - Identify and analyze QML algorithms applied in the field of supervised and unsupervised anomaly detection.
  - Explore and assess different quantum operators and circuits used in the literature for anomaly detection.
  - Design an unsupervised anomaly detection algorithm for IoMT networks based on QML principles.

- Assess and compare the QML-based anomaly detection method:
  - Incorporate the previously proposed algorithms to create a new unsupervised QML-based anomaly detection method that detects network anomalies to defend IoMT from cyberattacks.
  - Devise a strategy to assess the performance of the proposed method considering a NISQ framework.
  - Establish a baseline for comparison, including classical methods and current QML-based techniques.

4.2 Activities Schedule

This section outlines the overall schedule of the Ph.D. program, spanning four years from January 2024 to January 2028. We divided each year into three quatrimesters: I January-April, II May-August, and III September-December, as depicted in Figure 2.

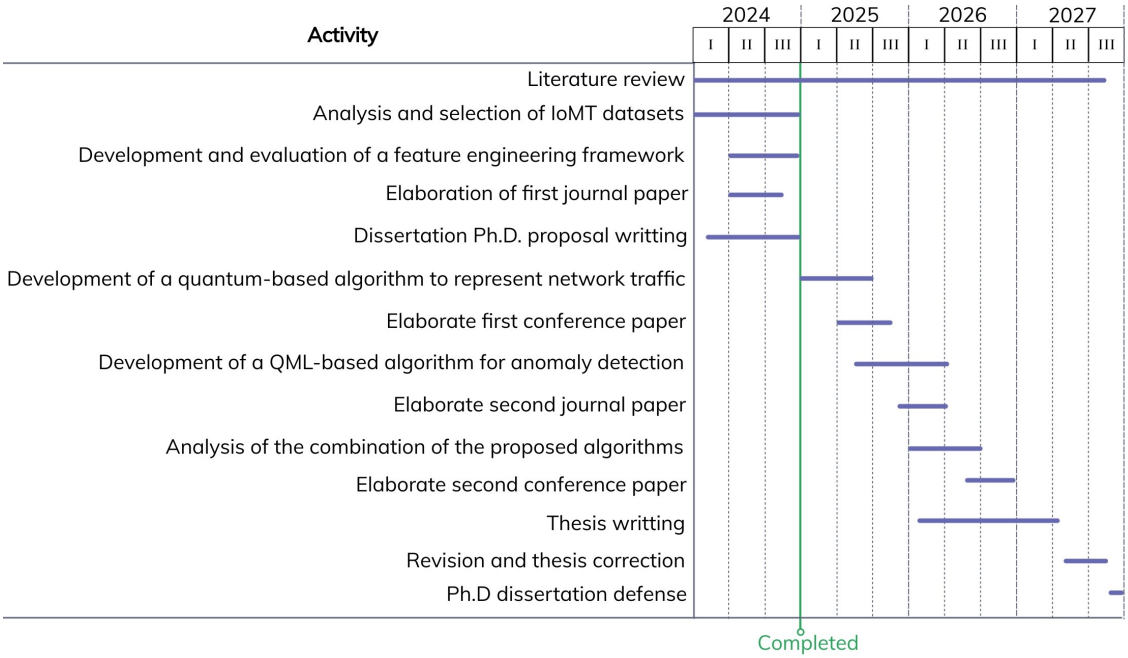

Figure 2: Chronogram of activities for PhD program.

4.3 Publications Plan

The expected publications and their objectives are presented below.

- First journal paper.
  Some of the preliminary findings were presented in a special session of IoT security at the *Estudio de Sistemas Complejos y sus Aplicaciones (EDIESCA)* 2024 congress. We were invited to submit our congress paper to the Integration Journal, which is briefly discussed in Section 5.

  - Hernandez-Jaimes, M. L., Martinez-Cruz, A., & Ramírez-Gutiérrez, K. A., & Morales-Reyes A. (2025). *Network Traffic Inspection to Enhance Anomaly Detection in the Internet of Things Using Attention-Driven Deep Learning.* [Manuscript under major reviews]

- First conference paper.
  Present the advances of our quantum-based algorithm for the characterization of network traffic to detect malicious behavior. We selected three possible conferences: IEEE World Forum on Internet of Things, International Conference on the Internet of Things, and IEEE International Conference on Internet of Things and Intelligence System. *Estimated submission date: July 2025*

- Second Journal paper.
  Present the advances of our unsupervised anomaly detection method based on QML principles for IoMT enviroments. We selected two possible journals: Internet of Things; Engineering Cyber Physical Human Systems and Journal of Biomedical and Health Informatics. *Estimated submission date: April 2026*

- Second conference paper.
  Present more findings of our research. We selected three possible conferences: IEEE International Conference on AI in Cybersecurity, IEEE Conference on Artificial Intelligence, and IEEE International Conference on Cyber-Physical Systems *Estimated submission date: November 2026*

5 Preliminary Results

This section presents the preliminary results obtained from the first and second steps of the proposed methodology: select IoMT datasets and design a feature engineering framework.

We selected the two most recent and extensive IoMT datasets, as described below.

- *CICIoMT* dataset was developed in the Canadian Institute of Cybersecurity (CIC) by Dadkhah et al. [52] contains 25 real and 15 simulated IoMT devices based on Wi-Fi, Bluetooth, and MQTT protocols, respectively. Moreover, it includes several types of attack scenarios, including MQTT Publish flood, MQTT Connect Flood, TCP Flood, UDP flood, ICMP Flood, Vulnerability scan, OS Scan, Ping Sweep, Port Scan, and ARP spoofing. This dataset also provides 39 network traffic features, such as header length, flags counts, and total network packets.

- *IoMT Traffic Data* dataset reflect a sports clinic scenario, which integrates three different areas: adversary, general, and wireless body. It was developed by Areia et al. [53] and encompasses 10 types of cyberattacks targeting WiFi-based, Bluetooth-based, MQTT-based, and COAP-based IoMT devices, including 4 variations of denial of service, ARP-based spoofing, MQTT-based malaria, network scanning, CAM table overflow, and two bluetooth-based attacks. A total of 40 network traffic features were extracted, such as total network packets, total bytes, byte difference, and payload ratio.

We proposed a feature engineering process for improved unsupervised anomaly detection using One-Class Support Vector Machine in IoMT environments, as illustrated in Figure 3. We train an OC-SVM model in a benign IoMT scenario and evaluate its anomaly detection performance on benign and malicious IoMT scenarios.

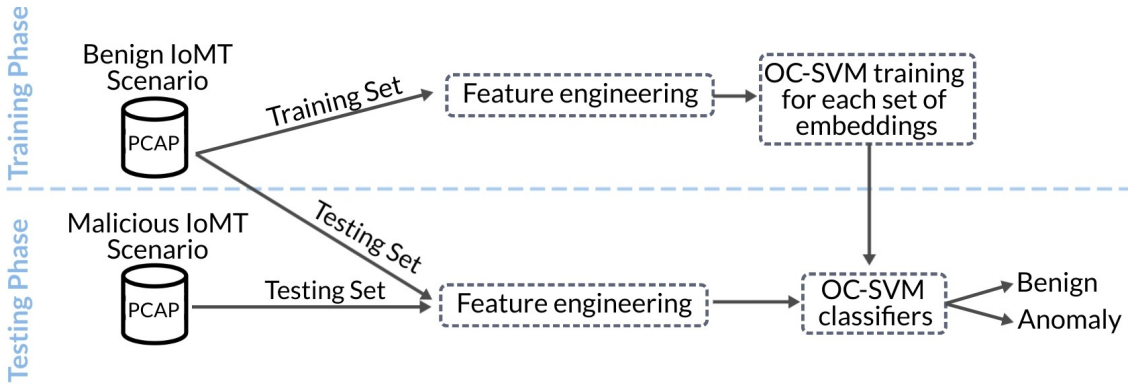

Figure 3: Flow diagram of the proposed anomaly detection method.

Given network traffic captured in a PCAP file, we monitored the sequences of network packets within one second, as this time interval has been proven to improve anomaly detection performance using the proposed method. First, we compute a flow-based embedding, which consists of eight flow-based features, including the total number of packets, the sum of all packet sizes, average packet sizes, minimum and maximum packet sizes, standard deviation packet size, average interval time between packets, as well as the minimum and maximum time intervals. Next, we compute a protocol-based embedding by defining a vocabulary of unique protocols from a benign IoMT scenario. Thus, we map the presence and absence of these protocols within each 1-second network flow, as described in Algorithm 1.

Algorithm 1 Protocol-based Embedding Workflow

Require: PCAP file

Ensure: Set of protocol-based embeddings

Begin

Let $V = \{p_1, p_2, \ldots, p_D\}$ be the set of unique communication protocols in the PCAP file.

Let $F = \{f_1(t), f_2(t), \ldots, f_n(t)\}$ be the set of 1-second network traffic flows, where each $f_n(t)$ represents a network flow, which comprises of network packets collected within n-th 1-second interval.

for $f_n(t)$ in F **do**

Let $E_n = [e_1, e_2, \ldots, e_i]$ be the protocol-based embedding, where $i \in \{1, 2, \ldots, D\}$ and:

$$e_i = \begin{cases} 1 & \text{if protocol } p_i \text{ is present in } f_n(t) \\ 0 & \text{otherwise} \end{cases}$$

Return $\{E_1, E_2, \ldots, E_n\}$

End

We propose an attention-driven Deep Neural Network (DNN) to compute a third feature embedding, called context embedding, by leveraging flow-based and protocol-based embeddings. The proposed attention-driven DNN is inspired by the Word2Vec method and the Scaled-Dot product attention mechanism. The former is widely recognized for its use as an embedding technique, while the latter serves as a powerful mechanism to focus on relevant features, particularly in natural language processing tasks [100–102]. The key difference between our proposal and these methods is that we are adding an attention layer into the Word2Vec structure based on the Scaled-Dot product attention mechanism for generating context embeddings from the network traffic. Figure 4, shows the proposed attention-driven DNN architecture. This architecture comprises four layers: input layer, hidden layer, attention layer, and output layer, with flow-based and protocol-based embeddings serving as the input and output layers, respectively.

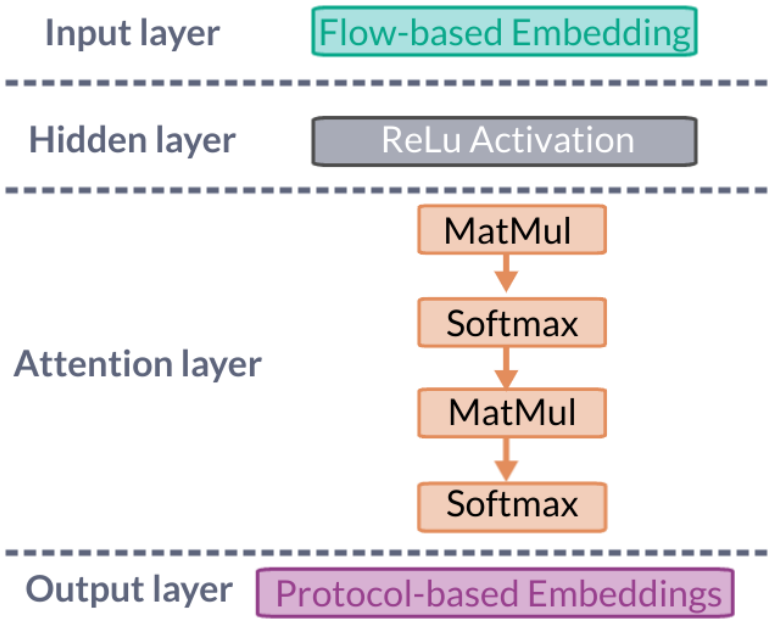

Figure 4: Proposed architecture for the attention-driven DNN algorithm.

The hidden layer is the same size as the input layer and utilizes the Rectified Linear Unit (ReLU) activation function to help mitigate the vanishing gradient problem. Attention Layer consists of two MatMul and two Softmax modules. The output of the hidden layer is transformed into three matrices: *Query (Q)*, *Key (K)*, and *Value (V)* by using the first MatMul module, which computes the dot product between Q and K with d_k dimensionality, as shown in Equation 15.

$$S = \frac{QK^T}{\sqrt{d_k}} \tag{15}$$

Next, the Softmax function is applied to the Score Matrix S to convert it into a probability distribution, as shown in Equation 16.

$$\text{Attention Weights} = \text{Softmax}(S) = \frac{e^{S_{ij}}}{\sum_{j=1}^{k} e^{S_{ij}}} \tag{16}$$

After obtaining the attention weights from the Softmax function, the next step is to multiply these weights by the V matrix. This is done through Equation 17.

$$\text{Output} = \text{Attention Weights} \cdot V \tag{17}$$

The output of this second MatMul operation is a weighted sum of the values, where each value in the matrix V is scaled according to the corresponding attention weight. The results are then passed on to the Softmax function to calculate the probabilities, producing the protocol-based embeddings.

Training the proposed attention-driven DNN involves minimizing the binary-categorical error function between the predicted protocol-based embedding ($\hat{E}$) and the ground truth protocol-based embedding (E) for each 1-second network flow, as shown in Equation 18.

$$H(E, \hat{E}) = -\frac{1}{N} \sum_{i=1}^{N} \left[E_i \log(\hat{E}_i) + (1 - E_i) \log(1 - \hat{E}_i) \right] \tag{18}$$

After training the proposed DL-based model, the output-weighted values of the Softmax function in the attention layer represent our context embedding of the 1-second network traffic flow. As a result of the feature engineering process, we obtain flow-based, protocol-based, and context-based embeddings for every captured 1-second network traffic flow. Subsequently, we concatenate these three types of embeddings, as shown in Figure 5.

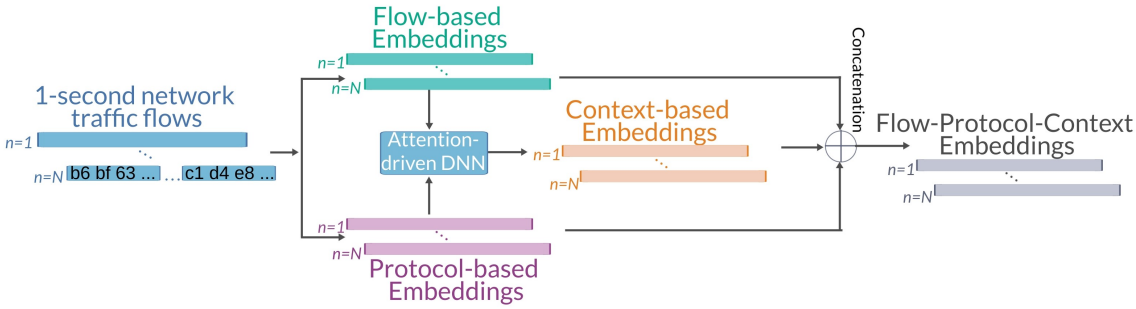

Figure 5: Concatenation process of flow-based, protocol-based, and context-based embeddings.

Finally, we evaluate the effectiveness of the OC-SVM classifiers in detecting anomaly 1-second network flows, as described in Algorithm 2.

Algorithm 2 Training and Testing Workflow

Require: PCAP files from Benign (B) and Malicious (M) IoMT scenarios

Ensure: Confusion Matrix of OC-SVM

Begin

Split B into B^{train} and B^{test}

Let E^{train} be the set of concatenated embeddings computed on B^{train} scenario.

Compute concatenated embeddings E^{test} on M and B^{test} scenarios.

Train OC-SVM on E^{train}

Test OC-SVM on E^{test}

Return TP, TN, FP, and FN outcomes

End

To assess our proposal's performance in detecting anomalies, we utilize standard metrics based on the True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN) values, such as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{19}$$

$$Precision = \frac{TP}{TP + FP} \tag{20}$$

$$Recall = \frac{TP}{TP + FN} \tag{21}$$

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{22}$$

Table 5 compares the anomaly detection performance of OC-SVM using the proposed concatenated embeddings and the pre-processed network traffic features provided by the works that developed the IoMT datasets.

Dataset	Feature Engineering	Accuracy	Precision	Recall	F1-score
CICIoMT	Ours	**84.41**	**84.43**	98.73	**91.02**
	Dadkhah et al. [52]	80.65	80.69	**99.88**	89.26
IoMT Traffic Data	Ours	**88.57**	**92.04**	94.85	**93.42**
	Areia et al. [53]	74.37	65.63	**99.64**	79.13

Table 3: Anomaly detection performance of OC-SVM using proposed feature engineering approach and pre-processed network traffic features.

Table 5 compare our proposal with current unsupervised DL-based anomaly detection methods evaluated in IoT-based environments, beyond IoMT settings, discussed in Section 3.3.

Dataset	Work	Accuracy	Precision	Recall	F1-score
CICIoMT	Ours	84.41	84.43	98.73	91.02
IoMT Traffic Data		88.57	92.04	94.85	93.42
Bot-IoT	Zixu et al. [84]	95.12	98.74	93.64	96.03
ToN-IoT	Alsaedi et al. [85]	-	70.59	90.01	79.13
IoTID20	Arifeen et al. [86]	89.89	93.31	96.07	-
MQTT-IoT-IDS2020	Boppana et al. [87]	80	86.80	80	81.40
RT-IoT2022	Sharmila et al. [88]	96.35	96.35	96.36	98.10
ToN-IoT	Vaisakhkrishnan et al. [89]	92	88	91	90

Table 4: Anomaly detection performance comparison with unsupervised DL-based models for IoT environments.

These initial findings suggest that our approach can improve the performance of the OC-SVM when compared to utilizing the pre-processed features given by the authors of the IoMT datasets. Moreover, our approach achieves comparable anomaly detection performance with unsupervised DL-based models, such as generative adversarial networks and autoencoders, proposed for IoT environments. The following step of our study will analyze different feature mapping methods for transforming classical data into quantum states for unsupervised anomaly detection in IoMT environments.

6 Conclusions

Unsupervised anomaly detection remains a significant challenge in the Internet of Medical Things. Motivated by the potential of quantum computing, this research proposal aims to develop a novel unsupervised anomaly detection method utilizing the principles of quantum machine learning. This proposal is envisioned to improve current methods in IoMT environments and contribute to future research on unsupervised anomaly detection.

This study offers several key contributions: an analysis of current anomaly detection methods for IoMT, including their feature engineering approaches; a review of unsupervised anomaly detection techniques for IoT applications; and a discussion of quantum machine learning-driven anomaly detection strategies, extending beyond both IoMT and IoT settings. Moreover, our preliminary achievements show a novel approach for unsupervised anomaly detection in IoMT that leverages natural language processing techniques, such as Word2vec and the Transformer architecture. These early findings suggest that there is still significant work to be done, especially considering the complex nature of IoMT environments. Moving forward, we will continue with the next steps of our methodology, refining our approach to address the proposed research problem.

References

[1] Pradyumna, G., Hegde, R. B., Bommegowda, K., Jan, T., & Naik, G. R. (2024). Empowering healthcare with iomt: Evolution, machine learning integration, security, and interoperability challenges. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3362239

[2] Stone, M. (2024). *A review of zero-day in-the-wild exploits in 2023* (tech. rep.). Google. https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/

[3] Alotaibi, A., & Barnawi, A. (2023). Securing massive iot in 6g: Recent solutions, architectures, future directions. *Internet of Things*, *22*, 100715. https://doi.org/https://doi.org/10.1016/j.iot.2023.100715

[4] Deloitte. (2024). *Global Future of Cyber Survey, 4th Edition* (tech. rep.). Deloitte. https://www.deloitte.com/global/en/services/risk-advisory/research/global-future-of-cyber.html

[5] Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., & Doulamis, N. (2024). Enhancing internet of medical things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine*, 108036. https://doi.org/https://doi.org/10.1016/j.compbiomed.2024.108036

[6] Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The role of ai in cyber security: Safeguarding digital identity. *Journal of Information Security*, *15*(02), 245–278. https://doi.org/https://doi.org/10.4236/jis.2024.152015

[7] Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for iomt security: A review of intrusion detection systems, attacks, datasets and cloud-fog-edge architectures. *Internet of Things*, *23*, 100887. https://doi.org/https://doi.org/10.1016/j.iot.2023.100887

[8] Liao, H., Murah, M. Z., Hasan, M. K., Aman, A. H. M., Fang, J., Hu, X., & Khan, A. U. R. (2024). A survey of deep learning technologies for intrusion detection in internet of things. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3349287

[9] Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2021). Unsupervised algorithms to detect zero-day attacks: Strategy and application. *Ieee Access*, *9*, 90603–90615. https://doi.org/10.1109/ACCESS.2021.3090957

[10] He, P., Huang, D., Wu, D., He, H., Wei, Y., Cui, Y., Wang, R., & Peng, L. (2024). A survey of internet of medical things: Technology, application and future directions. *Digital Communications and Networks*. https://doi.org/https://doi.org/10.1016/j.dcan.2024.11.013

[11] Zukaib, U., Cui, X., Zheng, C., Hassan, M., & Shen, Z. (2024). Meta-ids: Meta-learning based smart intrusion detection system for internet of medical things (iomt) network. *IEEE Internet of Things Journal*, 23080–23095. https://doi.org/10.1109/JIOT.2024.3387294

[12] Zubair, M., Ghubaish, A., Unal, D., Al-Ali, A., Reimann, T., Alinier, G., Hammoudeh, M., & Qadir, J. (2022). Secure bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system. *Sensors*, *22*(21), 8280. https://doi.org/https://doi.org/10.3390/s22218280

[13] Jawad, A. T., Maaloul, R., & Chaari, L. (2023). A comprehensive survey on 6g and beyond: Enabling technologies, opportunities of machine learning and challenges. *Computer Networks*, *237*, 110085. https://doi.org/https://doi.org/10.1016/j.comnet.2023.110085

[14] for Information Security, F. O. (2022). *Quantum Machine Learning – in the Context of IT Security* (tech. rep.). Federal Office for Information Security. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/QML/QML_Demonstrator.html

[15] Li, M., Zhang, H., Fan, L., & Han, Z. (2022). A quantum feature selection method for network intrusion detection. *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, 281–289. https://doi.org/10.1109/MASS56207.2022.00048

[16] Barletta, V. S., Caivano, D., De Vincentiis, M., Pal, A., & Scalera, M. (2024). Hybrid quantum architecture for smart city security. *The Journal of Systems Software*, *217*, 112161. https://doi.org/https://doi.org/10.1016/j.jss.2024.112161

[17] Laxminarayana, N., Mishra, N., Tiwari, P., Garg, S., Behera, B. K., & Farouk, A. (2022). Quantum-assisted activation for supervised learning in healthcare-based intrusion detection systems. *IEEE Transactions on Artificial Intelligence*, *5*(3), 977–984. https://doi.org/10.1109/TAI.2022.3187676

[18] Company, P. R. (2024). *Internet of Medical Things Market Size, Share, and Trends 2024 to 2034* (tech. rep.). Precedence Research Company. https://www.precedenceresearch.com/internet-of-medical-things-market

[19] Research, C. P. (2024). *Highest Increase of Global Cyber Attacks seen in last two years Report* (tech. rep.). Check Point Research. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/#:~:text=In%20Q2%202024%2C%20Check%20Point,(1%2C999%20attacks%20per%20week).

[20] IBM. (2024). *Cost of a data breach 2024* (tech. rep.). IBM. https://www.ibm.com/reports/data-breach

[21] Research, A., Consulting, & Advisory. (2022). *Artificial Intelligence in Cybersecurity Market Analysis - Global Industry Size, Share, Trends and Forecast 2022-2030* (tech. rep.). Acumen Research, Consulting, and Advisory. https://www.acumenresearchandconsulting.com/artificial-intelligence-in-cybersecurity-market

[22] Foundation, E. (2022). *2024 IoT Embedded Developer Survey Report* (tech. rep.). Eclipse Foundation. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/QML/QML_Demonstrator.html

[23] Kukliansky, A., Orescanin, M., Bollmann, C., & Huffmire, T. (2024). Network anomaly detection using quantum neural networks on noisy quantum computers. *IEEE Transactions on Quantum Engineering*, *5*, 1–11. https://doi.org/10.1109/TQE.2024.3359574

[24] Office, E. P. (2023). *Quantum computing: Insight report* (tech. rep.). European Patent Office. https://link.epo.org/web/epo_patent_insight_report-quantum_computing_en.pdf

[25] Markets & Markets. (2024). *Quantum Computing Market Size, Share, Statistics and Industry Growth Analysis Report* (tech. rep.). Markets and Markets. https://www.marketsandmarkets.com/Market-Reports/quantum-computing-market-144888301.html

[26] Nicesio, O. K., Leal, A. G., & Gava, V. L. (2023). Quantum machine learning for network intrusion detection systems, a systematic literature review. *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*, 1–6. https://doi.org/10.1109/ICAIC57335.2023.10044125

[27] Faker, O., & Cagiltay, N. E. (2023). Quantum machine learning in intrusion detection systems: A systematic mapping study. *International conference on WorldS4*, 99–113. https://doi.org/https://doi.org/10.1007/978-981-99-7886-1_9

[28] Corli, S., Moro, L., Dragoni, D., Dispenza, M., & Prati, E. (2024). Quantum machine learning algorithms for anomaly detection: A review. *Future Generation Computer Systems*, 107632. https://doi.org/https://doi.org/10.1016/j.future.2024.107632

[29] Vyas, S., & Bhargava, D. (2021). *Smart health systems: Emerging trends*. Springer Nature.

[30] Donta, P. K., Hazra, A., & Lovén, L. (2024). *Learning techniques for the internet of things*. Springer.

[31] Chakraborty, C., & Khosravi, M. R. (2022). *Intelligent healthcare: Infrastructure, algorithms and management*. Springer.

[32] Hemanth, D. J., Anitha, J., & Tsihrintzis, G. A. (2021). *Internet of medical things*. Springer.

[33] Househ, M., Borycki, E., & Kushniruk, A. W. (2021). *Multiple perspectives on artificial intelligence in healthcare: Opportunities and challenges*. Springer.

[34] Awad, M., & Khanna, R. (2015a). *Efficient learning machines: Theories, concepts, and applications for engineers and system designers*. Springer nature.

[35] Bauer, D. C., Wilson, L. O., & Twine, N. A. (2022). *Artificial intelligence in medicine: Applications, limitations and future directions*. Springer.

[36] Géron, A. (2022). *Hands-on machine learning with scikit-learn, keras, and tensorflow*. " O'Reilly Media, Inc.".

[37] Aggarwal, C. C., et al. (2018). *Neural networks and deep learning* (Vol. 10). Springer.

[38] Awad, M., & Khanna, R. (2015b). *Efficient learning machines: Theories, concepts, and applications for engineers and system designers*. Springer nature.

[39] Schneider, J., & Smalley, I. (2024). *What is a qubit?* (Tech. rep.). IBM. https://www.ibm.com/topics/qubit

[40] Manjunath, T., & Bhowmik, B. (2023). Quantum machine learning and recent advancements. *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, 206–211. https://doi.org/10.1109/AISC56616.2023.10085586

[41] Gouveia, A., & Correia, M. (2020). Towards quantum-enhanced machine learning for network intrusion detection. *2020 IEEE 19th international symposium on Network Computing and Applications (NCA)*, 1–8. https://doi.org/10.1109/NCA51143.2020.9306691

[42] Balamurugan, K., Sivakami, A., Mathankumar, M., Ahmad, I., et al. (2024). Quantum computing basics, applications and future perspectives. *Journal of Molecular Structure*, *1308*, 137917. https://doi.org/https://doi.org/10.1016/j.molstruc.2024.137917

[43] Jadhav, A., Rasool, A., & Gyanchandani, M. (2023). Quantum machine learning: Scope for real-world problems. *Procedia Computer Science*, *218*, 2612–2625. https://doi.org/https://doi.org/10.1016/j.procs.2023.01.235

[44] Payares, E., & Martínez-Santos, J. C. (2021). Quantum machine learning for intrusion detection of distributed denial of service attacks: A comparative overview.

Quantum Computing, Communication, and Simulation, *11699*, 35–43. https://doi.org/https://doi.org/10.1117/12.2593297

[45] Gong, C., Guan, W., Gani, A., & Qi, H. (2022). Network attack detection scheme based on variational quantum neural network. *The Journal of Supercomputing*, *78*(15), 16876–16897. https://doi.org/https://doi.org/10.1007/s11227-022-04542-z

[46] Alomari, A., & Kumar, S. A. (2023). Deqsvc: Dimensionality reduction and encoding technique for quantum support vector classifier approach to detect ddos attacks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3322723

[47] Abreu, D., Rothenberg, C. E., & Abelém, A. (2024). Qml-ids: Quantum machine learning intrusion detection system. *2024 IEEE Symposium on Computers and Communications (ISCC)*, 1–6. https://doi.org/10.1109/ISCC61673.2024.10733655

[48] Masum, M., Nazim, M., Faruk, M. J. H., Shahriar, H., Valero, M., Khan, M. A. H., Uddin, G., Barzanjeh, S., Saglamyurek, E., Rahman, A., et al. (2022). Quantum machine learning for software supply chain attacks: How far can we go? *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 530–538. https://doi.org/10.1109/COMPSAC54236.2022.00097

[49] Hady, A. A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, *8*, 106576–106584. https://doi.org/10.1109/ACCESS.2020.3000421

[50] Ahmed, M., Byreddy, S., Nutakki, A., Sikos, L. F., & Haskell-Dowland, P. (2021). Ecu-ioht: A dataset for analyzing cyberattacks in internet of health things. *Ad Hoc Networks*, *122*, 102621. https://doi.org/10.1016/j.adhoc.2021.102621

[51] Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., Garcia, N. M., & Zdravevski, E. (2021). A framework for malicious traffic detection in iot healthcare environment. *Sensors*, *21*(9), 3025. https://doi.org/10.3390/s21093025

[52] Dadkhah, S., Neto, E. C. P., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. A. (2024). Ciciomt2024: A benchmark dataset for multi-protocol security assessment in iomt. *Internet of Things*, *28*, 101351. https://doi.org/https://doi.org/10.1016/j.iot.2024.101351

[53] Areia, J., Bispo, I., Santos, L., & Costa, R. L. d. C. (2024). Iomt-trafficdata: Dataset and tools for benchmarking intrusion detection in internet of medical things. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3437214

[54] Fernandez Maimo, L., Huertas Celdran, A., Perales Gomez, A. L., Garcia Clemente, F. J., Weimer, J., & Lee, I. (2019). Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. *Sensors*, *19*(5), 1114. https://doi.org/https://doi.org/10.3390/s19051114

[55] Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. (2024). Explainable machine learning-based security and privacy protection framework for internet of medical things systems. *arXiv:2403.09752*. https://doi.org/10.48550/arXiv.2403.09752

[56] Alani, M. M., Mashatan, A., & Miri, A. (2023). Explainable ensemble-based detection of cyber attacks on internet of medical things. *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 0609–0614. https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361448

[57] Aljuhani, A., Alamri, A., Kumar, P., & Jolfaei, A. (2023). An intelligent and explainable saas-based intrusion detection system for resource-constrained iomt. *IEEE Internet of Things Journal*, *15*, 25454–25463. https://doi.org/10.1109/JIOT.2023.3327024

[58] Aversano, L., Bernardi, M. L., Cimitile, M., Montano, D., Pecori, R., & Veltri, L. (2024). Explainable anomaly detection of synthetic medical iot traffic using machine learning. *SN Computer Science*, *5*(488). https://doi.org/https://doi.org/10.1007/s42979-024-02830-4

[59] Gürbüz, E., Turgut, Ö., & Kök, İ. (2023). Explainable ai-based malicious traffic detection and monitoring system in next-gen iot healthcare. *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 1–6. https://doi.org/10.1109/SmartNets58706.2023.10215896

[60] Savanović, N., Toskovic, A., Petrovic, A., Zivkovic, M., Damaševičius, R., Jovanovic, L., Bacanin, N., & Nikolic, B. (2023). Intrusion detection in healthcare 4.0 internet of things systems via metaheuristics optimized machine learning. *Sustainability*, *15*(16), 12563. https://doi.org/https://doi.org/10.3390/su151612563

[61] Mosaiyebzadeh, F., Pouriyeh, S., Parizi, R. M., Han, M., & Batista, D. M. (2023). Intrusion detection system for ioht devices using federated learning. *IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 1–6. https://doi.org/10.1109/INFOCOMWKSHPS57453.2023.10225932

[62] Thapa, C., Karmakar, K. K., Celdran, A. H., Camtepe, S., Varadharajan, V., & Nepal, S. (2021). Feddice: A ransomware spread detection in a distributed inte-

grated clinical environment using federated learning and sdn based mitigation. *Quality, Reliability, Security and Robustness in Heterogeneous Systems: 17th EAI International Conference, QShine 2021, Virtual Event, November 29–30, 2021, Proceedings 17*, *302*, 3–24. https://doi.org/https://doi.org/10.1007/978-3-030-91424-0_1

[63] Akkal, M., Cherbal, S., Kharoubi, K., Annane, B., Gawanmeh, A., & Lakhlef, H. (2024). An intrusion detection system for detecting ddos attacks in blockchain-enabled iomt networks. *2024 7th International Conference on Signal Processing and Information Security (ICSPIS)*, 1–6. https://doi.org/10.1109/ICSPIS63676.2024.10812635

[64] Alzubaidi, L. H., Nijaguna, G., Pasha, S. N., Kotagi, V., & Kalaiselvi, K. (2024). Gaussian bare-bones butterfly optimization algorithm (gbboa) based support vector machine (svm) for cyberattack detection in healthcare. *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*, 1–5. https://doi.org/10.1109/ICICACS60521.2024.10498277

[65] Judith, A., Kathrine, G. J. W., & Silas, S. (2023). Efficient deep learning-based cyber-attack detection for internet of medical things devices. *Engineering Proceedings*, *59*(1), 139. https://doi.org/https://doi.org/10.3390/engproc2023059139

[66] Kilincer, I. F., Ertam, F., Sengur, A., Tan, R.-S., & Acharya, U. R. (2023). Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. *Biocybernetics and Biomedical Engineering*, *43*(1), 30–41. https://doi.org/https://doi.org/10.1016/j.bbe.2022.11.005

[67] Afroz, M., Nyakwende, E., & Goswami, B. (2024). A hybrid deep learning approach for accurate network intrusion detection using traffic flow analysis in iomt domain. *International Conference on Advances in Data-driven Computing and Intelligent Systems*, 369–385. https://doi.org/https://doi.org/10.1007/978-981-99-9518-9_27

[68] Alzahrani, A. (2023). A safeguard agent for intelligent health-care environments. *2023 International Conference on Smart Computing and Application (ICSCA)*, 1–6. https://doi.org/10.1109/ICSCA57840.2023.10087746

[69] Ramesh, K., Miller, N. C., Faridi, A., Aloul, F., Zualkernan, I., & Sajun, A. R. (2024). Efficient machine learning frameworks for strengthening cybersecurity in internet of medical things (iomt) ecosystems. *2024 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 92–98. https://doi.org/10.1109/IoTaIS64014.2024.10799438

[70] Hossain, M. T., Meem, S. M., Setu, J. H., Halder, N., Islam, A., & Alam, M. Z. (2024). Cyberattacks classification on internet of medical things using information gain feature selection and machine learning. *2024 Advances in Science and Engineering Technology International Conferences (ASET)*, 1–10. https://doi.org/10.1109/ASET60340.2024.10708692

[71] Tileutay, L., Chandroth, J., Lim, K.-W., Ko, Y.-B., & Roh, B.-H. (2024). Empirical distribution ranking based decision tree algorithm for building intrusion detection system in the internet of medical things. *2024 IEEE Annual Congress on Artificial Intelligence of Things (AIoT)*, 87–92. https://doi.org/10.1109/AIoT63253.2024.00027

[72] Lazrek, G., Chetioui, K., Balboul, Y., Mazer, S., et al. (2024). An rfe/ridge-ml/dl based anomaly intrusion detection approach for securing iomt system. *Results in Engineering*, *23*, 102659. https://doi.org/https://doi.org/10.1016/j.rineng.2024.102659

[73] Dhanya, L., & Chitra, R. (2023). An optimal differential evolution based xgb classifier for iomt malware classification. *2023 International Conference on Advances in Intelligent Computing and Applications (AICAPS).* https://doi.org/https://doi.org/10.1109/aicaps57044

[74] Dash, P. B., Senapati, M. R., Behera, H., Nayak, J., & Vimal, S. (2024). Self-adaptive memetic firefly algorithm and catboost-based security framework for iot healthcare environment. *Journal of Engineering Mathematics*, *144*(6). https://doi.org/https://doi.org/10.1007/s10665-023-10309-z

[75] Dhanya, L., & Chitra, R. (2024). A novel autoencoder based feature independent ga optimised xgboost classifier for iomt malware detection. *Expert Systems with Applications*, *237*, 121618. https://doi.org/https://doi.org/10.1016/j.eswa.2023.121618

[76] Alsalman, D. (2024). A comparative study of anomaly detection techniques for iot security using amot (adaptive machine learning for iot threats). *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2024.3359033

[77] Dina, A. S., Siddique, A., & Manivannan, D. (2023). A deep learning approach for intrusion detection in internet of things using focal loss function. *Internet of Things*, *22*, 100699. https://doi.org/https://doi.org/10.1016/j.iot.2023.100699

[78] Kumar, M., Kim, C., Son, Y., Singh, S. K., & Kim, S. (2024). Empowering cyberattack identification in ioht networks with neighborhood component-based improvised long short-term memory. *IEEE Internet of Things Journal*, *11*, 16638–16646. https://doi.org/10.1109/JIOT.2024.3354988

[79] Thulasi, T., & Sivamohan, K. (2023). Lso-csl: Light spectrum optimizer-based convolutional stacked long short term memory for attack detection in iot-based healthcare applications. *Expert Systems with Applications*, *232*, 120772. https://doi.org/https://doi.org/10.1016/j.eswa.2023.120772

[80] Ghourabi, A. (2022). A security model based on lightgbm and transformer to protect healthcare systems from cyberattacks. *IEEE Access*, *10*, 48890–48903. https://doi.org/10.1109/ACCESS.2022.3172432

[81] Gupta, B. B., Gaurav, A., Attar, R. W., Arya, V., Alhomoud, A., & Chui, K. T. (2024). A sustainable w-rlg model for attack detection in healthcare iot systems. *Sustainability*, *16*(8). https://doi.org/https://doi.org/10.3390/su16083103

[82] Al-Hawawreh, M., & Hossain, M. S. (2023). A privacy-aware framework for detecting cyber attacks on internet of medical things systems using data fusion and quantum deep learning. *Information Fusion*, *99*, 101889. https://doi.org/https://doi.org/10.1016/j.inffus.2023.101889

[83] Wagan, S. A., Koo, J., Siddiqui, I. F., Qureshi, N. M. F., Attique, M., & Shin, D. R. (2023). A fuzzy-based duo-secure multi-modal framework for iomt anomaly detection. *Journal of King Saud University-Computer and Information Sciences*, *35*(1), 131–144. https://doi.org/https://doi.org/10.1016/j.jksuci.2022.11.007

[84] Zixu, T., Liyanage, K. S. K., & Gurusamy, M. (2020). Generative adversarial network and auto encoder based anomaly detection in distributed iot networks. *GLOBECOM 2020-2020 IEEE Global Communications Conference*, 1–7. https://doi.org/10.1109/GLOBECOM42002.2020.9348244

[85] Alsaedi, A., Tari, Z., Mahmud, R., Moustafa, N., Mahmood, A., & Anwar, A. (2022). Usmd: Unsupervised misbehaviour detection for multi-sensor data. *IEEE Transactions on Dependable and Secure Computing*, *20*(1), 724–739. https://doi.org/10.1109/TDSC.2022.3143493

[86] Arifeen, M., Ghosh, T., Islam, R., Ashiquzzaman, A., Yoon, J., & Kim, J. (2022). Autoencoder based consensus mechanism for blockchain-enabled industrial internet of things. *Internet of Things*, *19*, 100575. https://doi.org/https://doi.org/10.1016/j.iot.2022.100575

[87] Boppana, T. K., & Bagade, P. (2023). Gan-ae: An unsupervised intrusion detection system for mqtt networks. *Engineering Applications of Artificial Intelligence*, *119*, 105805. https://doi.org/https://doi.org/10.1016/j.engappai.2022.105805

[88] Sharmila, B., & Nagapadma, R. (2023). Quantized autoencoder (qae) intrusion detection system for anomaly detection in resource-constrained iot devices using

rt-iot2022 dataset. *Cybersecurity*, *6*(1), 41. https://doi.org/https://doi.org/10.1186/s42400-023-00178-5

[89] Vaisakhkrishnan, K., Ashok, G., Mishra, P., & Kumar, T. G. (2024). Guarding digital health: Deep learning for attack detection in medical iot. *Procedia Computer Science*, *235*, 2498–2507. https://doi.org/https://doi.org/10.1016/j.procs.2024.04.235

[90] Huang, W., Zhang, J., Sun, H., Ma, H., & Cai, Z. (2017). An anomaly detection method based on normalized mutual information feature selection and quantum wavelet neural network. *Wireless Personal Communications*, *96*, 2693–2713. https://doi.org/https://doi.org/10.1007/s11277-017-4320-2

[91] Kalinin, M. O., & Krundyshev, V. M. (2021). Analysis of a huge amount of network traffic based on quantum machine learning. *Automatic Control and Computer Sciences*, *55*(8), 1165–1174. https://doi.org/https://doi.org/10.3103/S014641162108040X

[92] Zhang, M., Lv, B., & Liu, Z.-s. (2022). Network attack traffic recognition based on quantum neural network. *2022 7th International Conference on Computational Intelligence and Applications (ICCIA)*, 71–75. https://doi.org/10.1109/ICCIA55271.2022.9828461

[93] Kalinin, M., & Krundyshev, V. (2023). Security intrusion detection using quantum machine learning techniques. *Journal of Computer Virology and Hacking Techniques*, *19*(1), 125–136. https://doi.org/https://doi.org/10.1007/s11416-022-00435-0

[94] Rahman, M. A., Akter, M. S., Miller, E., Timofti, B., Shahriar, H., Masum, M., & Wu, F. (2024). Fine-tuned variational quantum classifiers for cyber attacks detection based on parameterized quantum circuits and optimizers. *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*, 1067–1072. https://doi.org/10.1109/COMPSAC61105.2024.00144

[95] Bhattacharya, P., Kumari, A., Tanwar, S., Budhiraja, I., Patel, S., & Rodrigues, J. J. (2024). Quant-jack: Quantum machine learning to detect cryptojacking attacks in iiot networks. *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*, 865–870. https://doi.org/10.1109/ICCWorkshops59551.2024.10615371

[96] Kumar, R., & Swarnkar, M. (2025). Quids: A quantum support vector machine-based intrusion detection system for iot networks. *Journal of Network and Computer Applications*, *234*, 104072. https://doi.org/https://doi.org/10.1016/j.jnca.2024.104072

[97] Chen, J., Qi, X., Chen, L., Chen, F., & Cheng, G. (2020). Quantum-inspired ant lion optimized hybrid k-means for cluster analysis and intrusion detection. *Knowledge-Based Systems*, *203*, 106167. https://doi.org/https://doi.org/10.1016/j.knosys.2020.106167

[98] Dong, Y., Hu, W., Zhang, J., Chen, M., Liao, W., & Chen, Z. (2022). Quantum beetle swarm algorithm optimized extreme learning machine for intrusion detection. *Quantum Information Processing*, *21*(1), 9. https://doi.org/https://doi.org/10.1007/s11128-021-03311-w

[99] Guo, M., Pan, S., Li, W., Gao, F., Qin, S., Yu, X., Zhang, X., & Wen, Q. (2023). Quantum algorithm for unsupervised anomaly detection. *Physica A: Statistical Mechanics and its Applications*, *625*, 129018. https://doi.org/https://doi.org/10.1016/j.physa.2023.129018

[100] Goodman, E. L., Zimmerman, C., & Hudson, C. (2020). Packet2vec: Utilizing word2vec for feature extraction in packet data. *arXiv:2004.14477*. https://doi.org/10.48550/arXiv.2004.14477

[101] Tan, M., Iacovazzi, A., Cheung, N.-M. M., & Elovici, Y. (2019). A neural attention model for real-time network intrusion detection. *2019 IEEE 44th conference on local computer networks (LCN)*, 291–299. https://doi.org/10.1109/LCN44214.2019.8990890

[102] Kheddar, H. (2024). Transformers and large language models for efficient intrusion detection systems: A comprehensive survey. *arXiv:2408.07583*. https://doi.org/10.48550/arXiv.2408.07583