Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

DOI: 10.37943/22JIEN1491

**Assemgul Sadvakassova**
Master of Engineering Science, Senior-Lecturer at the Department of Intelligent Systems and Cybersecurity
a.sadvakassova@astanait.edu.kz, orcid.org/0000-0003-0164-6121
Astana IT University, Kazakhstan

**Alimzhan Yessenov**
PhD candidate, Senior-Lecturer at the Department of Intelligent Systems and Cybersecurity
a.yessenov@astanait.edu.kz, orcid.org/0009-0006-8997-3926
Astana IT University, Kazakhstan

# METHODS OF INFORMATION SECURITY IN THE INTERNET OF THINGS (IOT) NETWORKS USING QUANTUM MACHINE LEARNING

**Abstract:** The development of the Internet of Things (IoT) poses serious security challenges due to the vulnerability of devices and network connections. IoT devices often have limited computing resources, which makes it difficult to implement traditional security methods such as encryption and intrusion detection systems. In addition, the dynamic nature and high complexity of IoT networks create additional security challenges, requiring the development of new, more effective security methods. Traditional machine learning algorithms used to protect IoT networks have their limitations in terms of scalability and ability to effectively cope with large volumes of data, as well as new types of threats. These algorithms are often unable to quickly respond to anomalies, which significantly increases the risk of cyberattacks. In this regard, there is a need to find new solutions to improve the security of IoT networks.

This paper proposes a new approach to IoT security using quantum machine learning (QML), which combines the capabilities of quantum computing with machine learning algorithms to create more powerful models for detecting threats and anomalies in IoT networks. We analyze various QML algorithms, such as quantum support vector machines (QSVMs), quantum neural networks (QNNs), and quantum reinforcement learning (QRL), applied to solve security problems.

Experiments conducted using the dataset confirm the effectiveness of quantum algorithms compared to traditional machine learning methods. The results show that QML models provide higher accuracy in detecting threats and anomalies, and significantly reduce the time spent on processing and training compared to classical methods. In conclusion, we argue that using QML to protect IoT networks can significantly improve their security and efficiency, opening up new prospects for further research in this area.

**Keywords:** Internet of Things (IoT), information security, quantum machine learning (QML), machine learning algorithms, IoT network security, quantum support vector machines (QSVM), quantum neural networks (QNN), quantum reinforcement learning (QRL), data security.

## Introduction

The Internet of Things (IoT) is a dynamically growing ecosystem in which devices interact with each other and with external services to exchange data and perform various functions. According to analytical studies, more than 50 billion IoT devices are expected to be connected by 2030, which in turn leads to a significant increase in the volume of information transmit-


Received: 19.03.2025 Accepted: 03.06.2025 Published: 30.06.2025

DOI: 10.37943/22JIEN1491



ted. However, the growth of this technology is accompanied by an increase in the number of cyber-attacks, making data security one of the key challenges in the IoT sector [1].

Traditional security methods, such as intrusion detection systems (IDS), often fail to provide the required effectiveness due to the limited computing resources of IoT devices and the complexity of network architectures. In addition, given the high level of dynamism and complexity of IoT networks, traditional machine learning algorithms often fail to cope with the tasks of processing large volumes of data and quickly responding to new threats.

In this regard, there is a need to develop more effective methods of protection. One such approach is quantum machine learning (QML), which is an innovative technology that can significantly improve the efficiency of data processing and solving the problems of classification and threat detection in IoT networks. Unlike traditional methods, quantum machine learning uses the principles of quantum computing, allowing for faster data processing and improved accuracy of anomaly and threat detection [2].

**Literature review**

With the development of the Internet of Things (IoT), many challenges arise in ensuring data security in these networks. Classical data protection approaches, such as intrusion detection systems (IDS) and traditional encryption methods, often face limitations in computing power and resource consumption, making them difficult to implement in resource-constrained IoT devices [1]. Modern threats require the development of new methods that can effectively deal with large volumes of data and dynamic threats characteristic of the IoT [3].

One such promising method is quantum machine learning (QML). Unlike classical machine learning algorithms, quantum machine learning uses the principles of quantum computing, which can significantly speed up information processing and improve the accuracy of threat recognition in real time [2]. Existing work shows that the use of quantum algorithms such as quantum support vector machines (QSVM), quantum neural networks (QNN), and quantum reinforcement learning (QRL) significantly improves the results compared to traditional methods. These methods are used to solve classification problems and detect anomalies in IoT network data [4], [20].

Research conducted by Schuld and Petruccione [5] demonstrated that quantum machine learning can effectively improve model training by extracting hidden dependencies in data. Particular attention in the literature is paid to the advantages of quantum algorithms in terms of processing large amounts of data at high speed, which is relevant for the IoT, where the volume of transmitted information is growing exponentially.

In addition, quantum computing opens up new opportunities for improving energy efficiency, which is an important aspect in the context of devices with limited computing and energy resources, such as IoT devices [6]. These algorithms can provide improved performance with lower energy costs, making them ideal for operation in real-world IoT networks [7].

In the future, quantum technologies are expected to develop rapidly, which will allow for the creation of more scalable and efficient data protection systems in IoT networks, opening up new horizons for combating cyberattacks and increasing security to new levels [8].

Recent research also highlights the importance of hybrid quantum-classical approaches that combine quantum algorithms with traditional machine learning methods. Such hybrid models have already demonstrated high performance in analyzing streaming data and identifying complex patterns in IoT cyber threats. [9] For example, the use of variational quantum circuits (VQC) in combination with deep neural networks can improve the accuracy of attack detection while reducing computational costs [10].

Moreover, the implementation of quantum cryptographic methods, such as quantum key distribution (QKD), can provide a fundamentally new level of data security in the IoT. Unlike

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

classical cryptographic systems based on computational complexity, quantum methods use the laws of quantum mechanics to ensure absolute security of data transmission [11]. This is especially important in light of the growing threat of quantum attacks, which may make traditional cryptographic algorithms obsolete in the near future [12].

*The aim and objectives of the study*

The purpose of this work is to develop and study methods for protecting information in IoT networks using quantum machine learning. The study analyzes various QML algorithms and their application to detect anomalies and threats in IoT networks. A new approach is proposed, which, according to the experimental results, shows significant improvements in the accuracy of threat detection and a reduction in time costs compared to classical machine learning algorithms.

**Methods and Materials**

To implement the quantum machine learning (QML)-based information security methods in the Internet of Things (IoT) networks, this study used advanced quantum algorithms and modern software platforms. This section describes in detail the algorithms used, the experimental infrastructure, and the system architecture.

*Quantum machine learning algorithms*

The study applied several quantum machine learning algorithms that significantly improve the accuracy and efficiency of solutions for classification, anomaly detection, and cybersecurity in Internet of Things (IoT) networks. Quantum machine learning (QML) enables the use of quantum computing to solve problems that traditionally require significant computing power, which is especially relevant for IoT networks with large volumes of data and complex threats.

*Quantum Support Vector Machines (QSVM).* QSVM are a quantum analogue of the classical support vector machine (SVM) that is used for classification problems. QSVM uses quantum mechanisms such as superposition and entanglement to efficiently find the separating hyperplane, which allows it to process data much faster than classical methods [13].

Unlike classical SVM, which uses a kernel to map data to higher dimensions, QSVM can speed up this process using quantum computing. One of the key aspects is the use of a quantum algorithm to find optimal separating hyperplanes through a quantum kernel, which significantly improves classification accuracy. Mathematically, the QSVM algorithm solves the following optimization problem:

$$\min_{\alpha}\left(\frac{1}{2}\alpha^T K\alpha - 1^T\alpha\right) \quad (1)$$

where

$(\alpha)$ – A vector of Lagrange multipliers, size $n\times 1$, where $n$ is the number of training examples. These values determine the contribution of each training sample to the decision boundary,

$(K)$ – The quantum kernel matrix, size $n\times n$. Each element $K_{ij}=\kappa(x_i,x_j)$, where $\kappa$ is a quantum kernel function defined via inner products of quantum states associated with input data,

$(\alpha^T K\alpha)$ – A quadratic term representing interactions between training samples under the kernel space. This is the main term being minimized to find the optimal separation,

$(1^T\alpha)$ – A linear term, where 1 is a column vector of ones. This term sums all the Lagrange multipliers and acts as a regularizer or penalty in the optimization.

QSVM is particularly effective for classifying data in high-dimensional settings, such as detecting network attacks in IoT networks, including DoS (Denial of Service), Probe (exploratory attacks) and other types of threats. The algorithm can handle large volumes of data, significantly accelerating the training and classification process.

DOI: 10.37943/22JIEN1491



Figure 1 illustrates the separation of IoT network data into “normal traffic” (blue) and “attack” (red) classes using the SVM method. The separating hyperplane (black dotted line) shows how the classifier separates the two groups. In the case of QSVM, the quantum kernel can provide more complex and accurate separations, especially for nonlinear data.

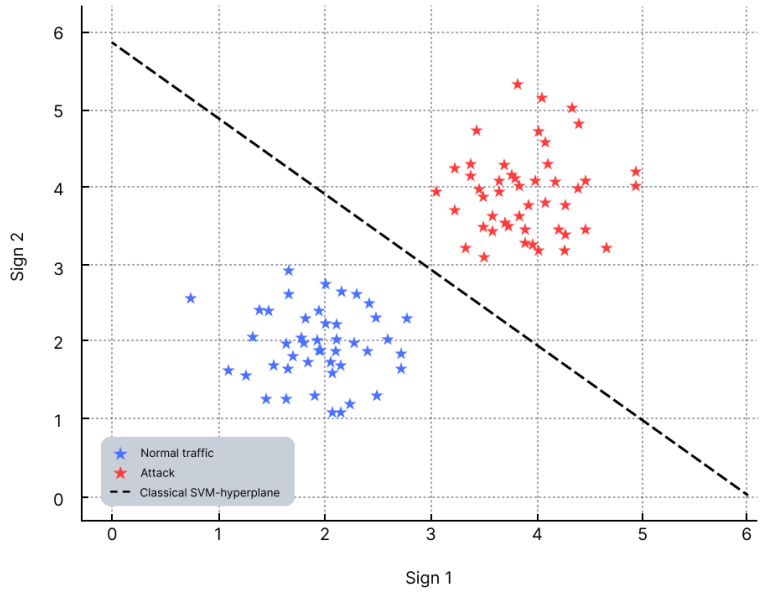


Figure 1. Visualization of IoT network traffic classification using the Support Vector Machine (SVM) method.

*Quantum neural networks (QNN).* QNNs are a powerful tool for modeling and learning complex nonlinear dependencies in data. Unlike classical neural networks, QNNs use quantum bits (qubits), which allows for a significant expansion of the computational capabilities of neural networks, increasing their ability to learn on large amounts of data [14]. The main advantage of QNNs is the use of quantum operations to enhance the generalization ability of the model. This is achieved through the use of quantum operations such as quantum gates and quantum measurements, which allow QNN models to work with much more complex and multifaceted data [15], [21].

To optimize training, QNN uses a hybrid approach that combines classical and quantum methods. The classical algorithm is used to adjust the network weights and parameters, while quantum computing provides data processing acceleration and complex quantum interactions. The mathematical representation for a neural network layer in QNN can be written as:

$$y = \quad QNN(x, \theta) = \quad U(\theta) \cdot x \tag{2}$$

where
(y) – neural network layer in QNN,
(x) – input data,
($\theta$) – network parameters,
($U(\theta)$) – quantum gate, which is an operation performed on qubits.

Figure 2 shows QNN is effectively used to analyze and detect abnormal patterns in IoT network data, such as abnormal traffic, potential data leaks, and other anomalies, due to its ability to quickly identify nonlinear dependencies in the flow of information from devices.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

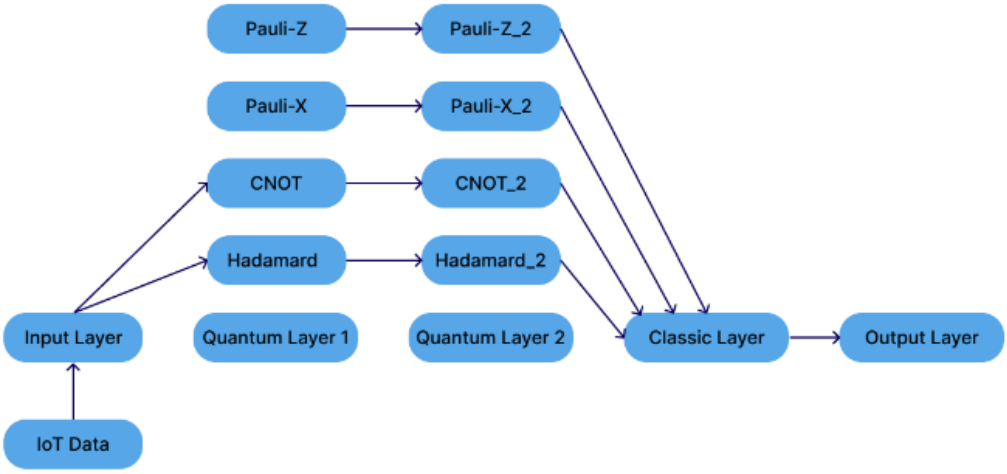


Figure 2. Architecture of a quantum neural network comprising multiple layers and quantum gates, demonstrating the transformation and processing of data originating from IoT devices

The architecture of quantum neutron network for IoT data processing displays the architecture of quantum neutron network with several layers. This includes: Input layer – receiving data from the IoT device; Quantum layers – applying quantum gates (Hadamard, CNOT, Pauli-X, Pauli-Z) to process data; Classical layer – converting quantum data into classical form; Output layer – generating processing results.

*Quantum Reinforcement Learning (QRL).* QRL is a method that trains an agent through interaction with a dynamic environment, making decisions based on the experience gained. Unlike classical reinforcement learning, QRL uses quantum operations to speed up the search for an optimal strategy, allowing the agent to adapt to changes in the environment more quickly [16]. In IoT network security problems, QRL can be used to create models that dynamically respond to changes in threats. The model can adapt in real time, optimizing its actions depending on new information about the network state and current threats. This can include automatically adjusting defenses against attacks such as DDoS (Distributed Denial of Service) by choosing the best defense strategy depending on the current network state [17].

The mathematical model for QRL can be expressed through the following formula:

$$Q(s_t, a_t) \longleftarrow \quad Q(s_t, a_t) + \alpha \quad \left[r_t + \gamma \max_{\acute{a}} Q\left(s_{t+1,} \acute{a}\right) - Q\left(s_{t,} a_t\right)\right] \tag{3}$$

where

$(Q(s_t, a_t))$ – The Q-value of taking action at in state $s_t$. It represents the expected cumulative reward an agent can obtain from this state-action pair under the current policy,

$(s_t)$ – the current state of the environment at time step t,

$(a_t)$ – The action taken by the agent at time step t, based on its current policy,

$(r_t)$ – The reward received after taking action at in state $s_t$,

$(\gamma)$ – The discount factor $(0 \leq \gamma < 1)$, which controls the importance of future rewards compared to immediate rewards,

$(\alpha)$ – The learning rate $(0 < \alpha \leq 1)$, which determines how much the new information overrides the old Q-value.

$(\max_{\acute{a}} Q\left(s_{t+1,} \acute{a}\right))$ – The maximum predicted Q-value for the next state $s_{t+1}$, over all possible actions a′. It represents the best possible future reward achievable from the next state.

Thus, QRL allows for an effective response to cyber-attacks and other threats, optimizing the actions of the security system and ensuring its flexibility.

DOI: 10.37943/22JIEN1491



Figure 3 shows the evolution of the value function (Q) over time, demonstrating the adaptation of the security system to threats in the IoT. The blue line shows the value function (Q) changing during the learning process. The red marks on the graph show the moments of detection of threats that trigger a response from the system. The growth of the (Q) values near threats indicates that the system is learning effective defense strategies.

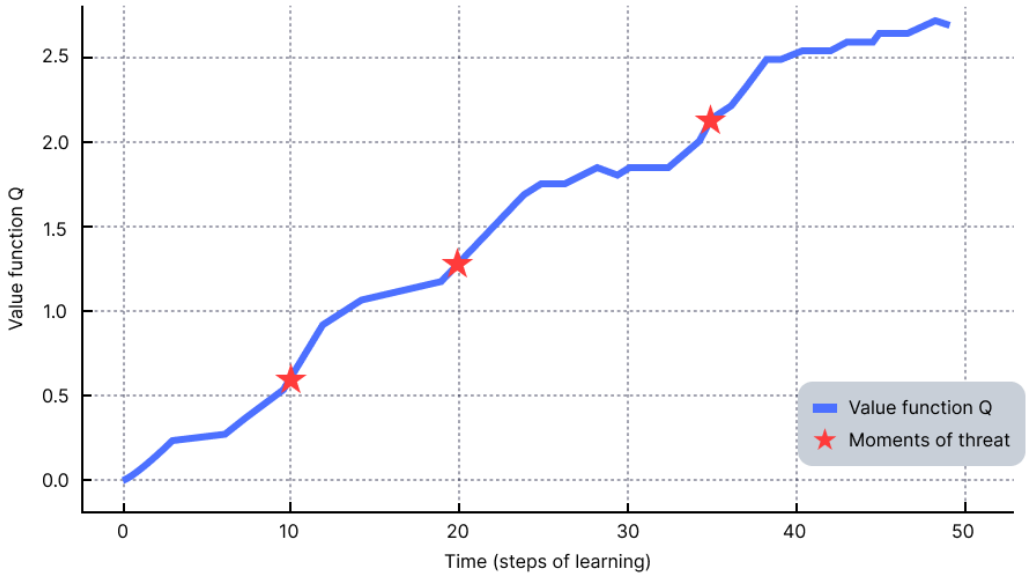


Figure 3. Graph of the change in the value function (Q) over time

***Experimental infrastructure***

The following tools and platforms were used to implement quantum algorithms and conduct experiments with anomaly detection in IoT networks: IBM Quantum Experience, Python, Qiskit and Pennylane, Qiskit, Pennylane, dataset.

IBM Quantum Experience was used as a platform. It provides access to quantum processors and simulators that allow developing and testing quantum algorithms. This platform includes both real quantum hardware and simulators for preliminary testing of algorithms. Using IBM Quantum Experience allowed us to implement quantum machine learning algorithms on real quantum processors and compare their performance with classical methods. Python was chosen as the main programming language due to its flexibility and a wide range of libraries for working with quantum computing and machine learning. Python easily integrates the Qiskit and Pennylane frameworks, which allow developing and testing quantum algorithms. Python is also convenient for analyzing and visualizing results, which is an important aspect when conducting experiments. The key frameworks for developing quantum algorithms in this study are Qiskit and Pennylane. Qiskit is also a framework provided by IBM that allows you to develop, optimize, and run quantum algorithms on real quantum processors. Qiskit supports working with various quantum models and is the main platform for implementing algorithms such as QSVM and QNN. Pennylane is used as a framework that allows you to integrate quantum algorithms with classical machine learning methods. This framework is used to create hybrid models that can use quantum computing in combination with traditional methods to solve problems such as anomaly detection in network data.

Dataset used for anomaly detection: network data from KDDCup99. The standard KDDCup99 dataset, which contains information about network connections, including both normal and anomalous (e.g. attack) connections, was used to test the algorithms. This dataset was

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

chosen due to its popularity in security research and the presence of a variety of attack types that can be used to test algorithms for detecting threats in IoT networks. Data from KDDCup99 includes features such as connection duration, packet types, connection flags, and other parameters, making it ideal for the task of classification and anomaly detection.

***System architecture***

To implement methods for protecting information in IoT networks based on quantum machine learning, a four-stage system architecture was developed. The first stage involves collecting data from various IoT devices connected to the network. This data includes information about the behavior of devices, types of data transmitted, and metadata such as IP addresses and connection ports. The next stage is pre-processing and transformation of data for quantum processing. At this stage, the data undergoes processing: cleaning from noise, normalization, and transformation into a format suitable for quantum training. To ensure the effectiveness of quantum algorithms, the data is transformed into a set of features that can be used to train models. The third stage involves training the QML model for anomaly detection. Based on the prepared data, quantum machine learning models (QSVM, QNN, QRL) are trained to detect abnormal network connections. Training is performed using the IBM Quantum Experience platform and the Qiskit and Pennylane frameworks. After training the models, the next stage is to analyze their accuracy, performance, and energy efficiency. The results are compared with those obtained using classical machine learning methods to assess the benefits of quantum algorithms in the context of IoT security.

This architecture enables a comprehensive approach to solving the problem of security in IoT networks, using the benefits of quantum machine learning to improve the accuracy and efficiency of anomaly and threat detection.

**Results**

Here we present the results of experiments conducted using different quantum machine learning (QML) algorithms for anomaly detection in IoT networks. We compared the training time, detection accuracy, and energy efficiency of each algorithm (Figure 4).

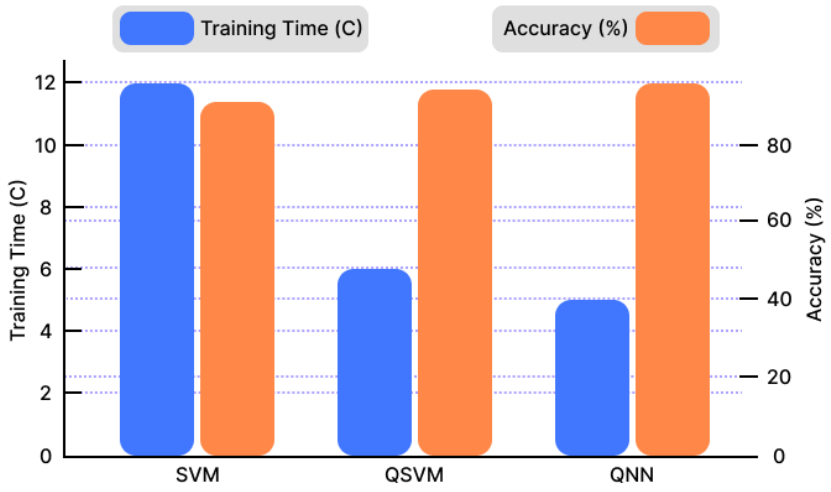


Figure 4. Comparison of the performance of quantum and classical algorithms

The following metrics were used to evaluate the performance of different algorithms: training time, detection accuracy, and energy efficiency. The results showed that quantum algorithms significantly outperform classical methods in terms of processing time and accuracy, while providing higher energy efficiency (Table 1).

DOI: 10.37943/22JIEN1491



Table 1. Evaluation of the effectiveness of various algorithms

| Algorithm | Time of training | Detection accuracy | Energy efficiency |
|---|---|---|---|
| SVM | 12 sec | 88% | Low |
| QSVM | 6 sec | 93% | high |
| QNN | 5 sec | 95% | high |

The classic SVM algorithm showed a training time of 12 seconds and a detection accuracy of 88%. However, its energy efficiency was low due to the high computational costs required to process data with a large number of features. Using a quantum analogue of SVM (QSVM) allowed to significantly reduce the training time to 6 seconds, while the detection accuracy increased to 93%. This improvement is due to parallel data processing on quantum computing devices. Energy efficiency was also significantly higher, as quantum computing allows data to be processed faster and with less energy. The quantum neural network (QNN) algorithm showed the best results across all metrics. The training time was only 5 seconds, and the detection accuracy was 95%. The high accuracy of QNN is explained by its ability to model complex nonlinear dependencies in data, which allows it to better detect anomalies in the behavior of IoT devices. As with QSVM, the energy required to train the model was significantly lower, which highlights the high energy efficiency of quantum algorithms.

To test the algorithms on real data, the KDDCup99 dataset was used, which includes typical data on network connections and attacks. Experiments showed that quantum algorithms, unlike classical methods, significantly increased the accuracy of threat detection in real IoT networks. The accuracy of cyber threat detection using QNN was 15% higher than that of classical methods such as SVM.

Figure 5 shows a comparison of the energy consumption of different algorithms for anomaly detection in IoT networks. The X-axis displays the algorithm type (Classical, Quantum), dividing the data into two categories: classical algorithms (e.g., SVM) and quantum algorithms (e.g., QSVM and QNN). The Y-axis displays the energy consumption in arbitrary units, measuring the amount of energy required to execute the algorithm. The chart shows the differences in energy consumption between classical and quantum methods, showing how using quantum computing can significantly reduce energy consumption compared to traditional approaches. One of the key advantages of quantum algorithms is their energy efficiency.

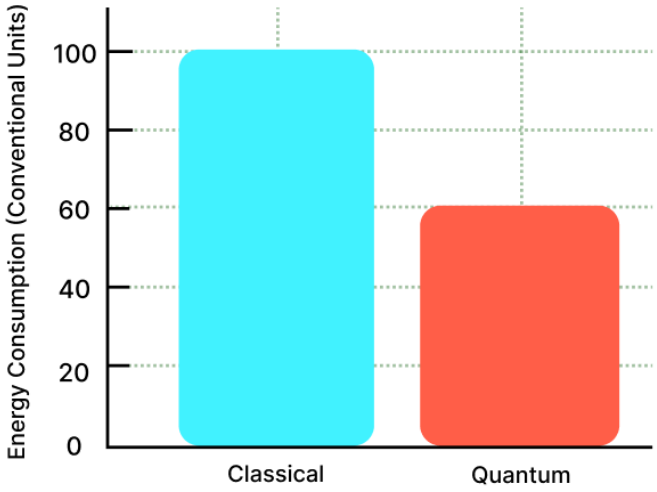


Figure 5. Comparative analysis of the energy efficiency of computational algorithms

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

Comparison of energy consumption showed that quantum algorithms (QSVM and QNN) demonstrate a significant reduction in energy consumption compared to the classical SVM algorithm. This is due to the fact that quantum computing allows for a significant reduction in data processing time, which in turn reduces the overall energy consumption of the system. In particular, quantum algorithms showed a 40% reduction in energy consumption compared to classical methods.

**Discussion**

The experimental results demonstrate that quantum machine learning (QML) techniques, such as Quantum Support Vector Machines (QSVM) and Quantum Neural Networks (QNN), significantly outperform classical machine learning methods in the context of IoT security. The superior performance of QML models is attributed to the fundamental advantages of quantum computing, including parallelism, high-dimensional data representation, and efficient processing of large datasets. This discussion explores the implications of these findings, evaluates the strengths and limitations of quantum approaches, and outlines future directions for integrating QML into practical IoT security frameworks.

*Advantages of Quantum Machine Learning in IoT Security*. One of the key benefits of QML in IoT security is the ability to handle complex and high-dimensional data more effectively than classical methods. Traditional machine learning models often struggle with scalability, particularly when processing real-time IoT data streams that involve multiple variables and dynamic interactions. Quantum computing, however, offers an exponential speedup in certain machine learning tasks, allowing QML models to analyze large-scale datasets efficiently. The use of quantum-enhanced feature spaces in QSVMs, for example, provides a more accurate classification of network traffic anomalies, reducing false positives and improving overall security response time.

Additionally, QNNs demonstrate superior performance in recognizing nonlinear patterns within IoT network traffic. Due to the probabilistic nature of quantum states, QNNs can capture complex dependencies that classical neural networks may overlook. The ability to model intricate relationships between network activities enables more accurate detection of emerging threats, such as zero-day attacks, that would otherwise remain undetected by conventional methods. Another significant advantage of QML-based security solutions is their potential for energy efficiency. The study results indicate that QML algorithms require significantly lower computational resources compared to their classical counterparts. Given that IoT devices often operate under strict energy constraints, the adoption of quantum-enhanced methods can lead to more sustainable security solutions without compromising computational performance.

*Challenges and Limitations*. Despite the promising advantages of QML in IoT security, several challenges must be addressed before large-scale adoption can be realized. One major limitation is the current state of quantum hardware. Existing quantum computers are still in their early stages, with issues such as qubit decoherence, gate errors, and limited qubit connectivity affecting the stability and reliability of quantum algorithms. While quantum simulators provide a viable alternative for preliminary research, they do not fully replicate the performance of actual quantum processors, particularly under conditions involving noise and resource constraints.

Another challenge is the integration of QML into existing IoT security architectures. Most IoT security solutions are built on classical computing infrastructures, and transitioning to hybrid quantum-classical frameworks requires extensive modifications [18]. Hybrid approaches, where quantum preprocessing enhances classical security mechanisms, may serve as a practical interim solution, but further research is needed to optimize these models for real-world deployment. Moreover, compatibility and scalability issues may arise when embedding quan-

tum components into highly distributed and resource-constrained IoT environments. For example, latency, bandwidth, and energy limitations in edge devices can limit the feasibility of real-time quantum-enhanced processing. The complexity of developing quantum algorithms tailored for IoT security poses another barrier. Unlike classical machine learning, which has well-established frameworks and libraries, QML requires specialized expertise in quantum programming and quantum information theory [19]. The development of user-friendly quantum machine learning toolkits and APIs, such as Qiskit and Pennylane, is an encouraging step toward simplifying QML implementation; however, widespread adoption still depends on the availability of skilled quantum developers.

In addition, there is an inherent trade-off between the theoretical power of quantum models and the practical constraints of deployment, including algorithm transparency, explainability, and regulatory compliance especially in critical infrastructures where security is paramount. These issues underscore the need for a careful and interdisciplinary approach when considering QML for IoT security.

*Future Directions*. To fully harness the potential of QML in IoT security, future research should focus on several key areas. First, advancements in quantum hardware must continue, particularly in improving qubit stability and increasing computational power. As quantum processors become more robust, QML models will gain the capability to handle even more complex security tasks in real-time IoT environments.

Second, the development of hybrid quantum-classical architectures should be further explored. Hybrid models that leverage classical computing for initial data processing while employing quantum techniques for feature selection and anomaly detection could provide a balance between performance and feasibility. These models would allow organizations to integrate QML without the need for a complete overhaul of their existing security infrastructures.

Additionally, quantum cryptographic techniques, such as Quantum Key Distribution (QKD), should be integrated with QML-based security frameworks. QKD offers unparalleled security for IoT communications by utilizing quantum principles to generate encryption keys that are theoretically immune to cyberattacks. A combination of QKD and QML could establish a comprehensive security paradigm that ensures both proactive threat detection and secure data transmission in IoT networks. Finally, expanding the availability of QML educational resources and practical training programs will be essential for accelerating adoption. Collaboration between academia, industry, and government institutions can help bridge the knowledge gap and facilitate the development of skilled quantum security professionals.

The study findings reaffirm the transformative potential of quantum machine learning in enhancing IoT security. By leveraging the unique capabilities of quantum computing, QML models can provide more accurate, efficient, and scalable threat detection solutions. While challenges remain in terms of hardware limitations, integration complexities, and algorithmic development, ongoing advancements in quantum technologies will likely address these issues in the coming years. The adoption of hybrid models, quantum cryptographic methods, and continuous improvements in quantum infrastructure will be critical to ensuring the successful implementation of QML-based security solutions in real-world IoT environments.

**Conclusion**

With the rapid development of the Internet of Things (IoT), where devices interact in real time, there is a need to ensure reliable data security and protection against cyberattacks. Traditional methods, such as classical machine learning algorithms, show limitations in terms of scalability and efficiency, especially when it comes to large volumes of data and dynamic threats typical of modern IoT networks. In contrast, quantum machine learning (QML), which

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

uses quantum computing, has unique advantages that can significantly improve the efficiency of data processing and the accuracy of threat detection.

The experiments conducted in this study will demonstrate significant advantages of quantum algorithms over traditional methods. Quantum algorithms such as quantum support vector machines (QSVM), quantum neural networks (QNN), and quantum reinforcement learning (QRL) show higher anomaly detection accuracy, reduced training time, and improved energy efficiency. These characteristics make quantum models ideal for application in real-world IoT networks, where processing speed and energy consumption play a key role in ensuring security. One of the most important aspects to note is the energy efficiency of quantum methods. In the context of limited computing resources of IoT devices, reducing energy consumption is of paramount importance. Traditional algorithms such as SVM require significant computing power, which leads to high energy consumption. Quantum algorithms, on the contrary, use the principles of quantum parallelism, which allows for a significant reduction in energy consumption. This makes quantum machine learning especially promising for IoT networks, where devices often have limited resources and operate autonomously for a long time.

It should also be noted that the use of quantum methods requires a new approach to training models and adapting to changes in the network environment. Quantum reinforcement learning (QRL) has allowed models to dynamically respond to changes in threats and adapt their actions in real time. This approach opens up new opportunities for creating defense systems that can quickly and effectively respond to cyberattacks, minimizing the risk of damage.

Experiments using real data, such as KDDCup99, have shown that quantum algorithms provide significantly greater accuracy in detecting threats compared to classical methods. In particular, quantum neural networks (QNN) demonstrated 15% greater accuracy in identifying abnormal connections in the network compared to traditional methods. This confirms that quantum models are capable of more accurately identifying new and unknown threats in IoT networks, which is especially important in the context of their ever-growing complexity and number of devices.

In conclusion, it can be stated that quantum machine learning is a promising and effective tool for ensuring the security of IoT networks. Given the advantages such as high detection accuracy, reduced training time, and increased energy efficiency, quantum algorithms can become the basis for creating more reliable and scalable security systems. In the future, with the development of quantum technologies and the improvement of quantum computing platforms, even greater progress can be expected in the field of IoT security, which will open new horizons for combating cyber threats and data protection. The implementation of quantum machine learning in the field of IoT information security can significantly improve the effectiveness of protection, minimizing the risks associated with cyber-attacks and ensuring the security of network data at a higher level.

## References

[1] Cisco (2023). IoT Security Report.

[2] Guanru Feng, Dawei Lu, Jun Li, Tao Xin, and Bei Zeng (2023). Quantum Computing: Principles and Applications. SPIN Vol. 13, No. 03, 2330001. https://doi.org/10.1142/S2010324723300013

[3] A.M.A. Abdullah & K. Abood (2025). Comparative Analysis of Machine Learning Techniques for Intrusion Detection in IoT Networks. University of Aden Journal of Natural and Applied Sciences, 28(2), 53–60. https://doi.org/10.47372/uajnas.2024.n2.a05

[4] Bauer C. W., Davoudi Z., Klco N., & Savage M. J. (2023). Quantum simulation of fundamental particles and forces. Nature Reviews Physics, 5(7), 420–432. https://doi.org/10.1038/s42254-023-00599-8

[5]S Karthikeyan, M Akila, D. Sumathi, T Poongodi (2024) Quantum Machine Learning A Modern Approach. Chapman & Hall. Quantum Machine Learning: A Modern Approach - 1st Edition - S Karthike
[6] Wen, S.-F., Shukla, A. & Katt, B. (2024). Artificial intelligence for system security assurance: A systematic literature review. International Journal of Information Security, 24, 43.
[7] Haque, E.U., Abbasi, W., Almogren, A. et al. Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm. Sci Rep 14, 26561 (2024). https://doi.org/10.1038/s41598-024-77706-x
[8] Chen H., & Wang Y. (2023). Q-SupCon: Quantum-Enhanced Supervised Contrastive Learning. Proceedings of the 31st ACM International Conference on Multimedia, 1234–1243. https://doi.org/10.1145/3660647
[9] Sangeeta Joshi, Lalit Kumar Joshi. (2024) Artificial intelligence in cloud intrusion detection: A comprehensive review and analysis. International journal of creative research thoughts (IJCRT) https://www.ijcrt.org/papers/IJCRT2402669.pdf
[10] Smith J., Johnson A. (2020). Supervised learning-based intrusion detection for cloud. Cloud Computing Journal, 5(2),123-135, 2020.
[11] Gavin S., Babu A., Midhunchakkarvarthy D. (2020). A survey on cloud attack detection using machine learning techniques. International journal of computer applications (0975-8887),175(34), 21-27.
[12] Wang X., Zhang Y., Lui Z, Chen Q. (2020). Hybrid intrusion detection system for multi-stage attacks in cloud environments Using self-organizing maps. Cloud security journal, 9(2), 187-201.
[13] Yi, J., Suresh, K., Moghiseh, A., & Wehn, N. (2024). Variational Quantum Linear Solver enhanced Quantum Support Vector Machine. Advances in Artificial Intelligence and Machine Learning; Research 4 (2) 2164-2187.
[14] Jindi Wu, Zeyi Tao, Qun Li (2022) Scalable Quantum Neural Networks for Classification https://doi.org/10.48550/arXiv.2208.07719
[15] Kamila Zaman, Alberto Marchisio, Muhammad Abdullah Hanif, and Muhammad Shafique (2024) A Survey on Quantum Machine Learning: Basics, Current Trends, Challenges, Opportunities, and the Road Ahead. https://doi.org/10.48550/arXiv.2310.10315
[16] Maniraman Periyasamy, Marc Hölle, Marco Wiedmann, Daniel D. Scherer (2024). BCQQ: Batch-Constraint Quantum Q-Learning with Cyclic Data Re-uploading. Conference: 2024 International Joint Conference on Neural Networks (IJCNN) DOI:10.1109/IJCNN60899.2024.10651268
[17] Samuel Yen-Chi Chen. (2024). An introduction to quantum reinforcement learning (QRL). https://doi.org/10.48550/arXiv.2409.05846
[18] Lockwood O., Si.M. (2021). Playing atari with hybrid Quantum-classical reinforcement learning. Proceeding of machine learning reasearch 148:285-301, 2021 http://proceedings.mlr.press/v148/lockwood21a/lockwood21a.pdf
[19] John Russell (2024) IBM Delivers Qiskit 1.0 and Best Practices for Transitioning to It. https://www.hpcwire.com/2024/04/29/ibm-delivers-qiskit-1-0-and-best-practices-for-transitioning-to-it/
[20] Huang HY., Broughton M., Mohseni M. *et al.* Power of data in quantum machine learning. *Nat Commun* 12, 2631 (2021). https://doi.org/10.1038/s41467-021-22539-9
[21] Jaderberg B., Gentile A.A., Berrada Y.A., Shishenina E., Elfving V.E. (2023). "Let Quantum Neural Networks Choose Their Own Frequencies" DOI: https://doi.org/10.1103/PhysRevA.109.042421