future internet

Article

Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT)

Anand Singh Rajawat [1], S. B. Goyal [2], Pradeep Bedi [3], Tony Jan [4], Md Whaiduzzaman [5] and Mukesh Prasad [6,*]

[1] School of Computer Sciences & Engineering, Sandip University, Nashik 422213, India
[2] Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia
[3] School of Computing Science and Engineering, Galgotias University, Greater Noida 203201, India
[4] Centre for Artificial Intelligence Research and Optimization, Design and Creative Technology Vertical, Torrens University, Sydney 2007, Australia
[5] School of Information Technology, Torrens University, Brisbane 4006, Australia
[6] School of Computer Science, Faculty of Engineering and IT (FEIT), University of Technology Sydney, Sydney 2007, Australia
* Correspondence: mukesh.prasad@uts.edu.au

Abstract: Internet of Medical Things (IoMT) is an ecosystem composed of connected electronic items such as small sensors/actuators and other cyber-physical devices (CPDs) in medical services. When these devices are linked together, they can support patients through medical monitoring, analysis, and reporting in more autonomous and intelligent ways. The IoMT devices; however, often do not have sufficient computing resources onboard for service and security assurance while the medical services handle large quantities of sensitive and private health-related data. This leads to several research problems on how to improve security in IoMT systems. This paper focuses on quantum machine learning to assess security vulnerabilities in IoMT systems. This paper provides a comprehensive review of both traditional and quantum machine learning techniques in IoMT vulnerability assessment. This paper also proposes an innovative fused semi-supervised learning model, which is compared to the state-of-the-art traditional and quantum machine learning in an extensive experiment. The experiment shows the competitive performance of the proposed model against the state-of-the-art models and also highlights the usefulness of quantum machine learning in IoMT security assessments and its future applications.

Keywords: vulnerability prediction; Internet of Things; quantum machine learning; Internet of Medical Things

check for updates

Citation: Rajawat, A.S.; Goyal, S.B.; Bedi, P.; Jan, T.; Whaiduzzaman, M.; Prasad, M. Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT). *Future Internet* **2023**, *15*, 271. https://doi.org/10.3390/fi15080271

Academic Editor: Matthew Pediaditis

Received: 13 July 2023
Revised: 8 August 2023
Accepted: 13 August 2023
Published: 15 August 2023

1. Introduction

Smart devices can be used to improve a wide range of services in ubiquitous computing. The gadgets that make up the “things” in the Internet of Things (IoT) can exist in any household, company, and city. The services based on IoT bring benefits but also security vulnerabilities in the form of blind spots and increased attack surfaces [1]. Smart devices with security vulnerabilities can allow malicious users to infiltrate private computing networks. Most IoT devices are vulnerable to cyber-attacks because they are not equipped with sufficient security features. These IoT networks are vulnerable to several factors, such as technological limitations and the users associated with the IoT applications [2].

Firstly, there are security vulnerabilities in IoT devices on the market because of their hardware limitations. IoT devices can only perform so much processing; their specific purpose is to provide minimized computing power (and constrained energy usage). Therefore, there are limited options for stronger data protection and security reinforcement. Secondly, diversity in the IoT device types brings challenges in establishing security protocols applicable to all IoT devices [3,4].

Most importantly, the lack of user control in IoT automation provides severe challenges to IoT security assurance [5]. As IoT applications are applied to various fields, including medical services (e.g., monitoring patients) where security is of paramount importance, proactive and preventative security assurance is vital in future applications of Internet of Medical Things (IoMTs) [6].

The purpose of this study is to identify practical solutions to these IoT security vulnerabilities. This paper focuses on the Internet of Medical Things (IoMT) [7] because the IoT devices in this sector can have significant impacts on human lives and their well-being, and IoMT often lacks the most fundamental security assurance [8]. In this article, IoMT security is first discussed. We describe several actual attacks carried out against commercial IoMT devices [9,10]. We review the processors, communication protocols, and cryptographic hardware/software used in commercial IoMT applications. It is absolutely necessary, in order to ensure the safety of IoMT devices, that ethical and privacy concerns be taken into account during the process of developing the IoMT. IoMT devices manage an astounding quantity of private and sensitive health information for their users. As a direct consequence of this, maintaining the secrecy of this information is of the utmost significance.

Patients, healthcare professionals, and regulators should all have complete access to and an understanding of IoMT and its operations because it is crucial from an ethical standpoint that they do. It is imperative that the specific data being used, the manner in which it is being processed, and the potential repercussions of improper data use all be made transparent. The likelihood of data bias, which could lead to unequal treatment for some patients, is another consideration that IoMT needs to take into account.

Concerns regarding the privacy of patients revolve around the necessity of preventing unauthorized access to sensitive information and maintaining compliance with legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) of the European Union. A number of potential remedies include using robust data encryption, stringent access limits, and anonymizing patient data whenever it is practicable to do so. There is also the possibility that IoMT networks will inadvertently divulge sensitive information. Additionally, there is the possibility that unauthorized access will be gained and data will be misused. Because of this, it is absolutely necessary to design and implement IoMT and its operation through (quantum) machine learning that includes tight protections, comprehensive testing, and regular monitoring, so that any possible issues may be located and resolved as soon as they appear.

This paper discusses various conventional machine learning models in IoMT and then considers quantum machine learning (QML) to overcome some of the limitations of conventional machine learning approaches in IoMT (due to its inherent complexity, heterogeneity, and data velocity). This paper proposes the framework for using a QML in IoMT vulnerability assessment. Some aspects of quantum physics, such as quantum entanglement, quantum superposition, and wide parallelism, are reviewed to discuss practical applications of QML [11]. This paper also presents a detailed experimental analysis of vulnerability assessment in IoMT of the proposed QML model against the other state-of-the-art machine learning models. This paper further provides insight into the benefits and further challenges of QML in IoMT security. The contributions of this research work are as follows:

1. This research investigates and assesses the viability of using quantum machine learning to detect security flaws in IoMT systems.
2. This research provides an in-depth analysis of classical and quantum machine learning methods, with an emphasis on their use in assessing the security of IoMT.
3. This research proposes, develops, and evaluates a unique fused semi-supervised learning model for IoMT security and compares its efficacy to that of conventional and quantum machine learning techniques.

In the remainder of the paper, Section 2 provides a comprehensive review of IoMT advances and its vulnerabilities, followed by an introduction to quantum machine learning. Section 3 presents the proposed model utilizing innovative quantum machine learning in

IoMT, followed by experimental analysis in Section 3.7. The paper concludes in Section 4 with further insight for future work.

2. Background

2.1. Review of IoT Applications

There are many new “smart” services and goods available, such as “smart” appliances, “smart” homes, “smart” watches, and “smart” TVs. These new “smart” services and products all contribute to the rapid proliferation and increasing ubiquity of Internet of Things (IoT) devices. The disclosure of sensitive personal data to a service provider is frequently required in exchange for smarter and more flexible service alternatives (which may at times be private information) [12]. This indicates that developing each product or service related to IoT should primarily emphasize protecting consumers’ personal information. Unfortunately, this is not the case with many commercially available Internet of Things (IoT) devices. In recent years, there has been an increase in the amount of scrutiny placed on the risks associated with using simple IoT devices in services that have access to sensitive information or important controls [13]. Examples of these services include a video recording of private environments, real-time personal location, health monitoring, building access control, industrial processes, and traffic lights. The recording of private areas through video, real-time monitoring of individuals, monitoring of health data, and monitoring of production lines are all services that fall under this category. Recent security breaches in media that target consumer IoT devices have heightened the public’s awareness of the risks that are inherently associated with the Internet of Things (IoT) ecosystem. Protecting commercial IoT devices from cyberattacks calls for first-principles design considerations [14]. However, because many different types of devices are connected to the IoT, it is difficult to create reliable security-by-design solutions. The capacity of many IoT devices to use electricity, transmit and receive data, and store information is severely limited. This makes things even more complicated than they already are. Owing to these difficulties, conventional and Internet-connected equipment cannot execute standard security measures similarly. Meanwhile, we must come up with creative responses and think beyond the box. A culture of cybersecurity is required by all parties involved in the Internet of Things (IoT), notably product designers and end users. This goes beyond technological factors that need to be considered. Many creators of IoT devices have been motivated to innovate by the demand for inexpensive sensors and actuators (e.g., home automation, light control, video surveillance, etc.). Because no other people utilize the system in remote locations where these devices are employed, the risk of security breaches is considerably reduced. This is because no other people use this system. As a consequence, many organizations have a poor understanding of cybersecurity and may remain naïve to the dangers posed by devices connected to the Internet [13].

Items connected to the Internet of Things have been brought to the market, even though their security was either disregarded or treated as an afterthought. This is because there is a lack of information, no production strategy, and a requirement to minimize both production costs and the amount of time it takes to enter the market. Additionally, most people do not alter the factory-set password on their devices, which is one of the most fundamental steps to increase safety. Consequently, a large amount of electrical hardware has been rendered useless. If a person is not given adequate credit to defend themselves and their own equipment, the user’s risk of being attacked increases. To assist readers in developing a deeper comprehension of the threats posed by Internet-connected devices, this paper offers an up-to-date analysis of the current cybersecurity status of the Internet of Things (IoT).

2.2. Security Flaws in IoMT Devices

Many events, both in the real world and in academic research, have shown how serious IoT security flaws are and their potential consequences. The Open Web Application Security Project (OWASP), a group that works to improve software, publishes an annual list of the most dangerous security holes of IoT. Below are some examples of each of these mistakes. This flaw is often encountered in new malware. For example, we found a version of Mirai called Mukashi that used brute-force attacks with default credentials to get into Zyxel NAS systems by exploiting CVE-2020-9054. Mukashi was able to do so because it used a loophole. As part of our research into complex IoMT ecosystems, we found the medical platforms were exposed to security risks while connecting and operating various devices. The server for the home automation system was not locked down, so sensitive information, such as the geolocation of the homes and hard-coded passwords, was exposed. The effects of a compromised automation platform are further discussed in this research.

The service providers with insecure networks aim to identify security flaws in products. The study showed that sensitive user information was leaked because the device had open ports that allowed it to connect to the Internet. It is not difficult to find examples of how people and networks have been compromised by device flaws, and more such cases are likely to occur in the future. The users need to know about these common flaws to protect themselves.

Threat actors can use vulnerable devices to move laterally, which allows them to move closer to important targets. Attackers can use vulnerabilities to take over specific devices, convert them into weapons for use in larger campaigns, or even use them to spread malware across an entire network. IoT botnets are an example of how dangerous device vulnerabilities can be and how sophisticated cybercriminals' methods are in taking advantage of them. One of the most well-known types of IoT botnet malware is headlines, which use a network of thousands of infected home IoT devices to launch a distributed denial of service (DDoS) attack against a number of well-known websites [15]. There is no clear line between the security needs of businesses and homes. IoT devices, primarily when used for remote work, make that line even less clear. This is particularly true when people work in the same office. Bringing IoT devices into the home can increase the number of possible entry points for hackers. This could put the company's network and employees in danger. This is a major concern for bring-your-own-device rules and arrangements allowing people to work from home. In addition, attackers can use weak Internet of Things (IoT) devices to enter internal networks. The growing list of threats includes new attacks that use side channels, such as infrared laser beam attacks on smart devices in homes and businesses and domain name service (DNS) rebinding attacks that can collect and send information from within networks.

The heterogeneity, velocity, and massivity in IoMT data communications pose serious challenges to traditional security solutions, as presented in Section 2.3.

2.3. Machine Learning Models in IoMT

In vulnerability prediction in IoMT-based applications, machine learning is used to analyze risks and find security vulnerabilities. It identifies and evaluates threats based on patterns in the network traffic generated by IoMT devices. It uses the features of dynamically updated threats to determine and assess them. The "vulnerability" of a system is a flaw that an attacker can take advantage of because it is built into the system. Most of the time, vulnerabilities can be found and possibly used, because they are common knowledge. On the other hand, risks consider not only the environment, configuration, behavior, and security policy but also one or more underlying weaknesses. Some risks can change how serious IoT Security [16] thinks a vulnerability is, but they only appear on the device details page and not on the vulnerability page. Specifically, IoT Security calls a vulnerability "possible" when it affects a specific device type, model, and version number. At least one device fits this type, but the model and version number are unknown. A device is vulnerable if it can be broken. If a flaw is only found in devices with a specific serial number, there are devices with unknown serial numbers that fit the description of the flaw; then the flaw is still a possibility. The vulnerability has not yet been used in this situation. The IoT has the potential to simultaneously improve patient care and lower healthcare costs at the same time. However, most IoT devices can be hacked, raising cybersecurity concerns that could hurt both patient care and business finances [17,18].

Ban et al. [19] summarized the typical research methods used in IoT security. Every study that finds a hole in the Internet of Things (IoT) infrastructure was carefully examined using a standard research method. Both the problems that needed to be solved and the tasks that needed to be performed were discussed.

Meneghello et al. [20] provided a thorough discussion of the security issues that plagued the Internet of Things (IoT) sector and looked at some of the ways that these issues were dealt with in the past. The authors provided a high-level overview of security in the IoT and then went into more detail about the specific security features built into the most popular IoT communication protocols. Next, the authors reported some of the attacks on real IoT devices in the literature. This was performed to show the importance of building security in IoT systems and the security problems common in commercial IoT solutions.

Zhao et al. [21] examined how safe MQ Telemetry Transport (MQTT) servers were to see whether vendors and users took safety measures. Their research showed that not all MQTT servers required a password to connect to the network. Their results provided an excellent way to investigate the safety of IoT devices and encouraged the creation of a more secure ecosystem for IoT systems.

Meidan et al. [22] obtained a lot of information about network activity from a wide range of commercial IoT devices and ran a series of tests to compare different ways of classifying security concerns. Their research showed that (a) the light gradient-boosting machine (LGBM) algorithm provided very accurate detection results, and (b) their flow-based approach was robust and could handle situations in which the other ways of identifying NAT devices could not (such as encrypted, non-TCP, or non-DNS traffics). The LGBM algorithm yielded outstanding results in terms of finding things. Other methods to find NAT-hidden devices had their limitations, but their flow-based method could work in these situations.

Al-Boghdady et al. [23] used machine learning to create a tool called iDetect that can detect security flaws in the C/C++ code of IoT operating systems (ML). With the help of the Software Assurance Reference Dataset (SARD) and the source code of 16 different releases of IoT operating systems, a tagged dataset of vulnerable and safe codes was created. This dataset was based on Common Weakness Enumeration (CWE), which was a list of flaws in IoT operating systems. Studies have shown that the C/C++ source code of low-end IoT operating systems had a minimal number of standard security holes and openings (CWEs).

Zeng et al. [24] used semi-supervised learning algorithms based on convolutional neural networks (CNNs) to find hidden features. Semi-supervised CNNs could learn from both labeled and unlabeled datasets. They could also learn from raw sensor data to use three different real-world datasets to show that their CNNs perform better than both supervised and standard semi-supervised learning methods by a mean F1-score margin of up to 18%.

Ramezani et al. [25] provided an overview of what we knew about using machine learning (ML) in quantum computing (QC). It also examined the benefits of using quantum machines in terms of speed and complexity.

Qu et al. [26] considered quantum blockchain to secure the IoMT network. Zanbouri et al. [27] studied how quantum computing may be used to secure IoMT data transmission with comparable success. Quantum computing brings significant improvements in future security computing, as discussed in Section 2.4.

2.4. Quantum Computing

Based on Boolean logic, traditional computing can only process data in one of two states. There is either "on" or "off" in these states. In a quantum computer, the numbers 0 and 1 can be represented by different fundamental particles, such as electrons or photons, depending on how they are charged or polarized. In the context of quantum computing, each of these particles is called a quantum bit or qubit [28].

Quantum entanglement and superposition of states are the two concepts in quantum physics that are thought to be the most important. Owing to quantum entanglement, qubits can talk to each other even if they are physically far apart (not restricted to the speed of light). Even if the connected particles are far apart, they are bound to each other. When quantum superposition and interposition are used together, they significantly affect the amount of computing power required. Traditional computers can only store one of four possible binary configurations (00, 01, 10, or 11) at any given time. However, a 2-qubit registry can store all four qubits simultaneously because each qubit represents two integers. However, traditional computers can store only one of four possible binary configurations. When more qubits are used, the capacity increases in a manner proportional to the square of the number of qubits [28].

Even though quantum machine learning (QML) has a lot of promise to make IoMT more secure, it is important to be aware of the challenges and limitations that will always come up during its implementation. First of all, smaller and medium-sized hospitals have a hard time buying and acquiring quantum computing technology because it is rare and expensive. Secondly, the settings for making and running QML algorithms are still in their early stages, just like quantum technology itself. There is a high entry barrier because the learning curve is steep and there are not any standard tools or guidelines. This is partially because of how hard quantum computing is to learn.

Lastly, we need to deal with how private and safe our data is. Quantum cryptography gives a higher level of protection, but it is not completely foolproof. If it is not kept in good shape, sensitive information about patients could be leaked, which would violate the patient's right to privacy and could have legal consequences. When integrating quantum-based systems with traditional computer platforms, there may be problems with how well they work together. If QML is going to be used successfully for IoMT security, then future studies will have to focus on finding solutions to these problems.

In quantum physics, a "photon" is the smallest amount of light that can behave in a certain manner. Therefore, someone cannot listen in on a conversation, obtain one-half of a photon, and then use that photon to figure out how much it is worth before letting it keep going. The two people in QKD who are honest with each other devise a plan to throw off an eavesdropper by making mistakes in their conversation, thought to have started the field or created it, was the first person to suggest and show that quantum mechanical properties could be used in communication if information bits could be physically specified [29]. Information can be encoded and sent using the spin of an electron, the manner in which a photon scatters, or a combination of these and other quantum properties.

Table 1 provides a summary of the literature review and their research gaps. Quantum computing is considered a futuristic solution to IoT security using its significantly improved computational capacity and speeds—analyzing the detailed attack surface of the IoMT network, providing useful vulnerability assessments to IoMT applications. Quantum machine learning is of significant importance to IoMT [30] and we consider its usage in vulnerability assessments of the complex and large network of IoMT devices in the following section.

Table 1. Summary of Literature Review and Research Gaps.

Ref. No.	Citation	Methods	Advantages	Disadvantages	Research Gaps
1	Jammula et al. (2023) [1]	A Very Lightweight Protocol for Communicating in an AI Framework	Predicts attacks on the Internet of Things with minimal network overhead.	Due to its lightweight nature, it may not be able to withstand complicated attacks.	Protocol Improvements for Countering Advanced Attacks.
2	Hussein et al. (2022) [2]	IoT Security Evaluation Using MQTT	Identifies flaws in the ZigBee protocol used to control smart lights.	Only works with ZigBee networks and the MQTT protocol; might not operate in other Internet of Things settings.	Exploring more protocols and configurations for the Internet of Things.
3	Ramadan et al. (2022) [3]	Literature Review	Offers an in-depth analysis of the risks associated with the Internet of Things.	Insufficient experimental confirmation or real-world application.	Investigations into the discovered weaknesses through experimentation.
4	Hasan et al. (2022) [5]	Hybrid Deep Learning Approach Successful in preventing botnet attacks in the IIoT.	The application of deep learning may necessitate a lot of computing power.	The proposed approach has lower computational needs.	
5	Koutras et al. (2020) [6]	Literature Survey Presents a thorough evaluation of security measures for IoMT transmissions.	Not enough effort has been put into actual use or testing.	There have to be experiments performed on the surveyed IoMT security techniques.	
6	Razdan et al. (2022) [7]	Overview and Case Studies	IoMT Case Studies and Emerging Technologies Discussion.	It is possible that there isn't enough technical depth or proposed solutions to the problems.	Formulation of approaches to resolving the problem at hand.
7	Yaacoub et al. (2020) [8]	Literature Review and Recommendations.	Describes the challenges of safeguarding IoMT systems and offers solutions.	The suggestions might not have been tested or validated in practice.	Testing and implementation of the suggested changes.
8	Bouriche et al. (2022) [9]	Systematic Review	Pinpoints security holes to stop IoMT attacks.	It is possible that there are no workable fixes for the detected flaws.	Creating workable fixes for the reported flaws.

3. Proposed Model and Research Framework

In this section, the proposed model using an innovative quantum deep learning algorithm is introduced alongside the other state-of-the-art machine learning models (both traditional and quantum). The proposed model is evaluated against the other machine learning model in detecting security vulnerabilities in IoMT applications. Due to the massivity, heterogeneity, and high velocity, IoMT security is considered challenging and the experimental analysis shows that the proposed quantum machine learning model can attain favorable security assessments.

The suggested system, which combines quantum computing with machine learning for the purpose of IoMT security evaluation, has several primary goals, the most important of which are optimizing data processing, boosting the accuracy of prediction, and beefing up security measures. The following constitute the primary components of the framework: Data Collection and Preprocessing: During this phase, data is collected from a wide variety of IoMT devices and then transmitted to a hub server. The readings from sensors, data from gadgets, and medical records are some examples of the types of information that could come under this category. Quantum techniques are utilized in order to clean and prepare the data. One of the most important characteristics of quantum computing is its capacity to process enormous volumes of data simultaneously.

Feature Extraction and Selection: After the data has been preprocessed, techniques based on quantum mechanics are employed to extract relevant characteristics from the data. The Quantum Feature Selection (QFS) method makes use of quantum bits (qubits) as an optimization tool for the purpose of selecting the features that are the most significant, decreasing the complexity of the problem, and improving the performance of the computation.

Security Vulnerability Assessment: This feature does security risk analysis with the use of a quantum machine learning (QML) model. The chosen attributes are used to teach the model how to identify dangers and weaknesses. Utilizing the increased processing capacity and greater pattern recognition capabilities of quantum computing, QSVMs, and QNNs can be employed for this purpose.

Threat Prediction and Classification: As soon as the QML model has been properly educated, it will be able to recognize and classify vulnerabilities and threats to the IoMT infrastructure. It is able to forecast future attacks by gaining knowledge from previous ones and by continuously monitoring data in real time. Response and Mitigation: The final component of the framework is taking action in response to the hazards that have been recognized. Quantum algorithms can, in a relatively short period of time, determine the best possible courses of action to adopt. Warnings may be issued by the system, compromised devices may be isolated, and additional precautions may be taken if the system deems it necessary.

Continuous Learning and Adaptation: The proposed method uses a feedback loop to continuously refine and update the QML model based on new data and threat trends. This makes the strategy still useful and effective as threats evolve over time. A novel architecture that is based on quantum machine learning has been designed in order to keep up with the constantly shifting nature of the IoMT security landscape. It makes use of quantum computing in order to manage the huge amount of data and the challenging nature of the security challenges linked to IoMT. This strategy makes it possible to recognize potential dangers early on and to respond quickly to mitigate them. As a result, it can potentially prevent catastrophic losses or interruptions to essential medical services.

In the remainder of Section 3, the concepts of semi-supervised reinforced learning (RL) (Section 3.1), Deep Q neural network (Section 3.2), and semi-supervised Convolution Neural Network (CNN) (Section 3.3) are presented, followed by the introduction to quantum machine learning (Section 3.4), quantum semi-supervised reinforced learning (Section 3.5) and the proposed model of quantum deep learning in altered form (Section 3.6). The extensive experimental analysis is provided in Section 3.7.

3.1. Semi-Supervised Reinforcement Learning (RL)

Semi-supervised RL is similar to the traditional proposed RL, but it has two types of episodes instead of just one: “Labeled” episodes are the same as “normal” episodes, but “unlabeled” attacks make it difficult for the agent to see how their actions help. We aim to find a strategy that provides a significant advantage at the end of each episode [31]. There are two types of semi-supervised RL: a random label is assigned to each attack, and the label has a certain chance of being right. The agent learns by asking how it performed after each attack. The total amount of time spent on training and the number of feedback sessions required should be kept as low as possible. We filtered out events that were not annotated using a standard RL algorithm on the semi-supervised data. Most of the time, this means that people learn slowly. An interesting question is how to learn the most useful things from having no limits on what you can do. Semi-supervised RL is not only a key part of AI control, but also a major problem in the field of RL that needs to be studied. However, even if AI control is not considered, semi-supervised RL remains a significant challenge for the RL community. This gives us a new way to look at the success of RL algorithms and a different way to measure the progress of learning that is more "human-like." The methods used for semi-supervised reinforcement learning are expected to be useful when dealing with the more general problems of a few and changing the reward signals. Even if we only consider RL issues under full monitoring, these are still major problems. Putting possible solutions in a clear setting will help us to better understand them. When AI is used for commands, this makes our tasks easier. It would be beneficial to use an experimental method to study counterfactual oversight and bootstrapping. Both methods require the optimization of costly ground truth, making it difficult to perform large-scale experiments on good semi-supervised RL.

Figure 1 provides an overview of Q-process learning. In the case of semi-supervised RL, there are some problems with data analysis, such as observing how the environment changes. If an agent learns to perform a new type of action in a different environment, the previous benefit estimates may no longer be accurate. To perform well in active semi-supervised RL, an agent must be taught to anticipate changes and ask for feedback in response to those changes. How can uncertain rewards be dealt with? A semi-supervised RL agent will ll not be very useful if it cannot perform well even when it has a rough idea of the reward function. There are times when the model of the dynamics of the environment is much better and more stable than the reward function. This topic is much more interesting when we track performance during training, instead of simply looking at how long it takes to converge. Obtaining information [32] and talking to people. In different situations, one may need to act strategically to obtain a hidden reward. For example, if an agent wants to know what a human supervisor would find after a thorough inspection, they can ask the supervisor a series of questions. Thus, the supervisor can make quick, correct decisions, and it is important for the agent to be able to explain what he or she is thinking. This is how aligned the AI systems must act.

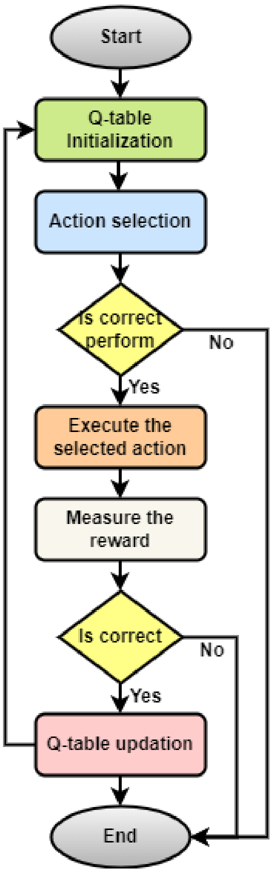


Figure 1. Actions by the state that is good for the state (SARSA).

3.2. Deep Q Neural Network (DQNN)

Q-learning [33] can be used as an off-policy RL technique in temporal-difference learning for prediction in IoMT-based applications [34]. Temporal difference learning techniques can be used to compare the accuracy of the predictions made at different times.

The value function Q (S, a) is then learned. This function shows the value of performing a specific action (a) in a specific state (S) (s).

State action reward state action (SARSA) is an example of an on-policy temporal difference learning system for vulnerability prediction in IoMT-based applications. The on-policy control technique [35] selects the best way to implement a policy in each state while the policy is being learned. The goal of the SARSA program is to calculate Q (s, a) for the selected policy and for all the permutations of s and a. (s-a) (s-a). The most significant difference between the SARSA and Q-learning algorithms is that in SARSA, the Q-value in the table does not need to be changed by knowing what the highest reward will be for the next state. SARSA decides what the next step and reward will be based on the same policy that determines the first action. This maintains consistency. The quintuple Q (s, a, r, s′, a′) used by the algorithm is, where the term SARSA is derived from. Where

s: the starting point a: The initial action taken r: what people hope to get out of following the rules The letters s and a represent a new combination of a state and an action.

DQN describes "Q-learning through Neural networks". Defining and maintaining a Q-table in an environment with a vast state space is a difficult and time-consuming task owing to the complexity of the domain. When we use the DQN method, we can find an answer to this problem. In this example, the neural network approximatively calculates the Q-values for each action and state, rather than specifying a Q-table.

Q-learning is a popular model-free reinforcement-learning algorithm based on the Bellman equation. The goal of Q-major learning is to learn the policy that tells the agent what to do and when to do it to obtain the highest reward. This is an unofficial RL that tries to determine the best thing to do right now. In Q-learning, the agent's goal is to make Q's value as high as possible. With the help of the Bellman equation, you can figure out the value of the Q-learning algorithm. The Bellman equation is as follows:

$$V(s) = \max\{R(s,a) + \gamma\Sigma_{s'}P)V(s')\} \tag{1}$$

Equation (1) has several variables, such as the reward, discount factor (), probability, and end states (s′). However, it does not consider the Q-value; therefore, we start with the image above.

The letter V represents a variable with values s1, s2, or V. (s3). Because this is a Markov Decision Process, the agent only cares about the current state and what will happen in the future. The agent is free to go wherever he wants, so he has to choose between three possible routes to reach his destination as quickly as possible. Here, the agent acts based on the odds, which causes the system's state to change. However, we will have to make some changes to the Q-value if we want our maneuvers to be accurate. Q is a way to determine how well the steps taken in the situation work. Therefore, instead of using a value at each stage, we used the letter Q to represent a set of states and actions (s, a). The agent decides what to do next by looking at the Q-value, which shows which action is more lubricating than the others. The Bellman equation was used to determine the Q-value.

When the agent performs an action, he either receives a reward of type R(s, a) or moves to a different state. Therefore, for the Q-value, we can write the following equation:

$$Q(S,a) = R(s,a) + \gamma\Sigma_{s'}P(s,a,s^{'})V\left(s^{'}\right) \tag{2}$$

Hence, we can say that, $V(s) = \max[Q(s,a)]$

$$Q(S,a) = R(s,a) + \gamma\Sigma_{s'}(P\left(s,a,s^{'}\right)maxQ\left(s^{'},a^{'}\right)) \tag{3}$$

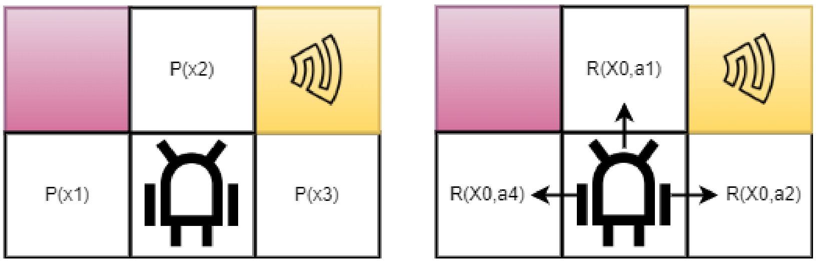
3.3. Semi-Supervised Convolutional Neural Networks

We combined the supervised CNN and CNN-encoder decoder models to obtain semi-supervised learning for vulnerability prediction in IoMT-based applications. Semi-supervised learning [36] uses a set of labeled pairs (xi, ti) |1 I N along with unlabeled data xi |N+1 I N+M to train a classifier. This information was used to teach the classifier. In a semi-supervised CNN-encoder-decoder setup, labeled and unlabeled data can be processed in one of three ways: the clean encoder, noisy encoder, or decoder. The clean encoder path was used to determine the intermediate layer hidden variables, which are marked by z l I. This route is used for both labeled and unlabeled clean data. In the noisy encoder path, both labeled and unlabeled data are exposed to Gaussian noise before the noisy encoder converts them into a more abstract representation. The letters z, l, and I represent this representation, respectively. We used the cross-entropy cost to make predictions with the best softmax classifier for the has been labeled data (x I 1 I N). In the labeled dataset, the values of x range from 1 to N. Let us assume that the letters y I stand for the expected label. The decoder attempts to return the original, clean input from the noisy, unlabeled data (x i, N + 1 I N + M) (xi). The square error is used to measure the size of the reconstruction error. The clean encoder path and noisy encoder path both use the same parameters [37]. The only difference is in the inputs, as shown in Figure 1. (The CNN-Ladder shown in Figure 2 can be simplified to a CNN-Encoder-Decoder structure by only looking at the vertical connections and the cost on the side). The cost function for the CNN-encoder decoder includes both the supervised cross-entropy cost from the labeled data in the supervised CNN and the unsupervised denoising square error cost between the clean input and its noisy reconstruction output. Supervised CNN must pay these two extra costs. This figure shows the cost function.

$$z_i^{(1)}, \ldots\ldots, z_i^{(L)} = Encoder_{clean}(x_i) \tag{4}$$

$$\underline{x}_i, \underline{z}_i^{(1)}, \ldots, \underline{z}_i^{(L)} = Encoder_{noisy}(x_i) \tag{5}$$

$$\hat{x}_i = Decoder(\underline{z}_i^{(L)}) \tag{6}$$



(**a**) (**b**)

Figure 2. (**a**) Markov decision process for *P* component. (**b**) Markov decision process for *R* component.

Given the input x_i, the average cross-entropy of the noisy output y I that meets goal t_i is equal to supervised cost Cs. The average squared error between the reconstructed output xi and original input xi can be considered as the unsupervised cost Cr. If we use a CNN-encoder–decoder that is only partially supervised, we can train both the network and the features simultaneously from the data, as described in Figure 3.

$$C_e = C_s + \lambda C_r^{(0)} = -\frac{1}{N}\sum_{i=1}^{N} \log\log P(x_i) + \frac{\lambda}{M}\sum_{i=N+1}^{N+M} ||\underline{x}_i - x_i||_2^2 \tag{7}$$

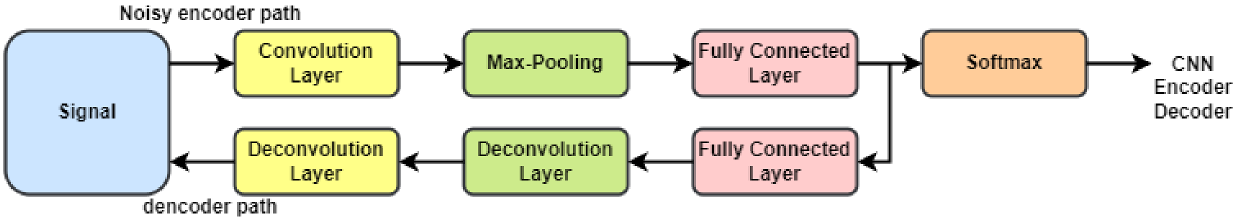


Figure 3. Vulnerability prediction in IoMT-based application uses both a (CNN) Encoder-Decoder.

There are two kinds of ties in CNN-Ladder. This kind of connection is shown by the reconstructed cost function C (l) r and the lateral connection g (l). A vertical link is the other kind of link that can be used.

3.4. *Quantum Machine Learning*

"Quantum-enhanced machine learning" means using quantum algorithms to solve problems in machine learning. This makes traditional machine-learning techniques [38] more effective and, in many cases, speeds up the process [39–42]. When giving a classical dataset to a quantum computer for use, it is often encrypted for use in quantum information processing. The quantum computing results can be retrieved once the state of the quantum system is measured. For example, after an operation, the state of the qubit can be used to determine the results of a binary classification task. Many quantum machine-learning algorithms are still in the theoretical stage and can only be tested on a full-scale universal quantum computer. However, some quantum machine-learning algorithms have already been used for small-scale or purpose-built quantum devices. Quantum machine learning is a field of study that investigates how well quantum computing and machine learning work together. We would like to examine whether a quantum computer can evaluate [38] and train a machine learning model faster than traditional methods. However, it is possible that machine learning can be used to find quantum error-correcting algorithms, evaluate the properties of quantum systems, and develop new quantum algorithms. The scientific community is currently facing several problems that cannot be solved using traditional methods of computing because they are too complicated or take too long to solve.

However, quantum systems today do not have enough qubits and cannot handle mistakes well enough to do these things. On the other hand, quantum computing could be useful in fields such as machine learning and biology with existing hardware. Most of the algorithms that have been found to date are quantum versions of traditional machine learning algorithms, such as support vector machines, and traditional deep learning methods, such as quantum neural networks. In a wide range of articles, the use of quantum devices and methods is considered a way to solve problems that are currently being solved by classical machine learning. Quantum machine learning has a long way to go before it can fully live up to its promise [26], even though new research is encouraging. To realize the full promise of quantum computing, advances in quantum hardware are necessary because existing quantum computers lack the essential quality, speed, and scalability.

3.5. *Quantum Semi-Supervised Reinforcement Learning (RL)*

Quantum control involves making a series of choices in a certain order. To run a quantum system, the agent is a piece of software that must be installed and run on a regular workstation. The agent is part of a quantum environment composed of a quantum harmonic oscillator, which is the electromagnetic mode of a superconducting resonator, and an ancilla qubit, which is the two lowest energy levels of a transom. Both parts are brought to life as electromagnetic modes in the superconducting resonator. In quantum physics, "environment" means a dissipative bath that is connected to a quantum system. However, in Vulnerability prediction in IoMT-based applications, "environment" means the quantum system itself, which is the agent's environment. Therefore, the word is used differently. A good way to save time is to use a circuit model of quantum control instead of learning the details of the control gear. This operational definition demonstrates how an agent interacts with its environment. This is performed by performing a parameterized control circuit in a series of discrete steps. To prepare for the next phase, the agent converts the observations into an action vector that is used to change the settings of the control circuit. An episode consists of T steps, in which the agent talks to their surroundings. depicts the pipeline for implementing classical RL in a quantum-observable setting. The agent (yellow box), which is a piece of software that runs on a classical computer and manages the quantum system, follows a policy defined in terms of a neural network. The quantum environment of an agent consists of a harmonic oscillator and its ancilla qubit. The agent's goal [43] is to move the oscillator from its initial state j0i to the target state jtargeti after a certain number of time steps T. The agent can only learn about its surroundings by making projective measurements of the ancilla qubit, which gives binary results, and not by directly observing the quantum state of its surroundings. This is because the agent cannot know what is going on in the quantum world.

3.6. Q-Deep Learning Model

To determine whether a cluster state is "excited," you must first prepare the state and then train a quantum classifier. Even if the cluster state is highly complicated, it may still be possible to deal with it using a traditional approach. structures of traditional CNN to operate in quantum systems. When a quantum physics problem written in many-body Hilbert space is moved to a traditional computing environment [44], the size of the data increases with the size of the system [45]. Therefore, it cannot be used to find good answers to problems. Because data can be described with qubits in a quantum environment, this problem can be solved by providing a quantum computer with a CNN structure. This makes it possible to solve this problem. Once everything has been settled, we can look at what is inside the Q-deep CNN model.

Q-Deep CNN: For this classification of vulnerability prediction in IoMT-based applications, to make a Q-Deep CNN architecture:

1. A cluster state on a ring is also independent of translation, just like the Q-Deep CNN.
2. Also, the cluster state is very complicated.

A mixture model with only one quantum filter. After performing one layer of quantum convolution and reading all the bits, a neural network with many connections is used as presented in Figure 4.

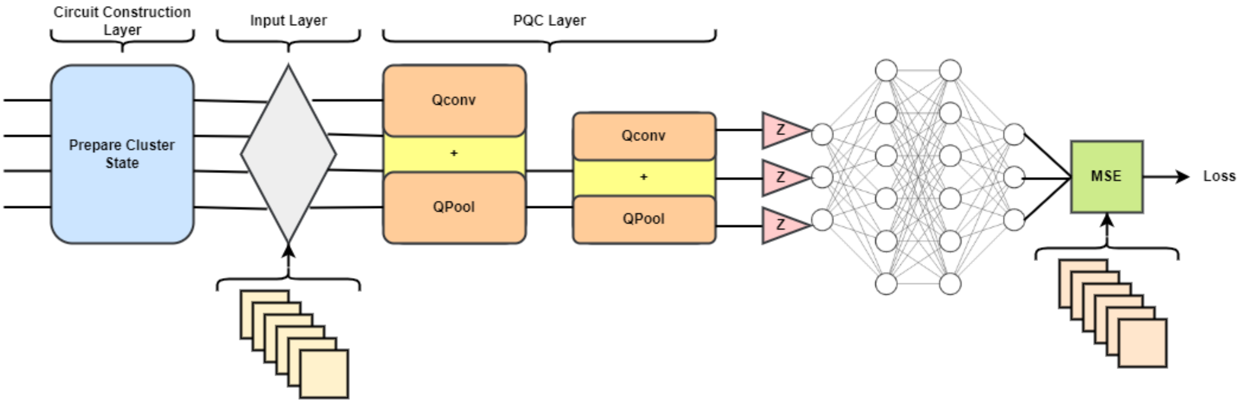


Figure 4. In a convolutional hybridization process, more than one quantum filter is used.

Let us attempt a method that combines the results of many quantum convolutions with a classical neural network, as presented in Figure 5.

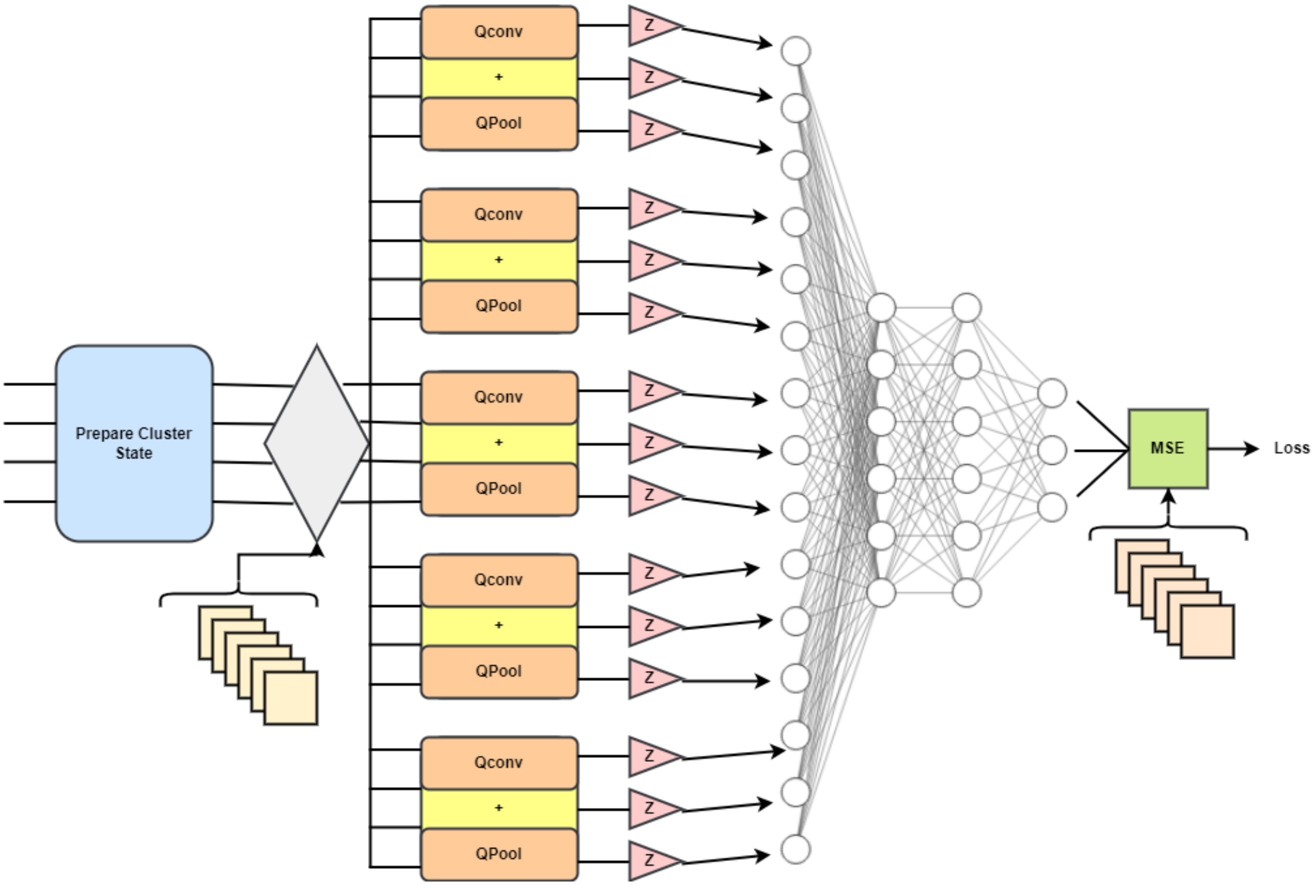


Figure 5. Combination of the results of many quantum convolutions with a classical neural network.

The Q-deep CNN model changes the core parts of the CNN, such as the convolution layer and pooling layer, so that they can be used with quantum computing. When multiple qubit gates are used on nearby qubits in the convolution circuit, a hidden state is observed. The pooling circuit can make the quantum system smaller in two ways: by keeping an eye on the qubit fraction or by using CNOT gates for only two-qubit gates, it leads to a size reduction in the quantum system that is exponentially smaller than the size of the data that enters it.

IoMT security evaluation carried out by means of quantum machine learning (QML) has demonstrated a significant amount of promise. The capabilities of its quantum-based system allow the analysis of data at scales that are unreachable to traditional computers. However, overfitting is a significant problem that needs to be considered before releasing QML models. When a model learns too much from its training data, it becomes overfit and is unable to generalize successfully to new data. This is because it has become overfit. This happens as a result of the model's incorporation of noise or other random fluctuations that are present in the training data. As a result, it is not possible to generalize its findings, which leads to incorrect predictions when applied to new information. When QML is utilized for IoMT, overfitting presents a number of challenges for a variety of different reasons. Privacy of Information: IoMT data is frequently personal and sensitive due to the fact that it connects to the health of individuals. Inaccurate security vulnerability assessments may be the result of models that have been overfitted, which leaves a door open for possible security breaches and threats.

Environments that make use of the IoMTs are notoriously difficult to navigate due to the sheer number of devices that are involved. The utilization of an overfitted model that does not take into consideration the nuanced complexity of the context in an effective manner may lead to inaccurate judgments. The danger landscape in IoMT is in a state of perpetual flux as a result of the emergence of new threats and the evolution of existing risks. Models that have been overfitted, meaning that they are overly specialized to the training data, have difficulty coping with new dangers.

There are a few different avenues that can be pursued in order to cut down on the possibility of overfitting occurring in QML for IoMT:

1. Regularization approaches such as L1 and L2 are able to prevent overfitting by employing a penalty based on the complexity of the model.
2. The creation of fictional data points is a kind of data augmentation, which is performed with the intention of enhancing the ability of the model to generalize.
3. By utilizing cross-validation to fine-tune the model's hyperparameters for optimal bias and variance, overfitting can be avoided. This allows for optimal bias and variance.
4. It is possible to prevent a model from picking up on random oscillations in the data by terminating the training phase of the process early.

Last, but not least, it is absolutely necessary to carry out routine audits of the models in order to guarantee that they will continue to be accurate and that they will be able to withstand any new security threats that arise within the IoMT ecosystem. Monitoring how well the model performs on a validation set is an excellent approach to identifying overfitting in its early stages and making the necessary adjustments to fix it.

3.7. Experimental Comparisons

We experimented with several machine-learning models. These models were constructed using Python 3.7.0, TensorFlow 1.10.0, and the Keras library on the web-based interactive computing platform Jupyter Notebook, version 5.6.0. The ML models were then separated using multi-class and binary-class methods. This resulted in two copies of the final labeled dataset as presented in Table 2.

Table 2. Datasets and Threat Information.

No.	IoT Device	IoMT Device Type	Network Type	Data Transmission Rate	Quantum Machine Learning Used	Detected Security Threats	Threat Severity	Correct Detection (Yes or No)
1	Heart Rate Monitor	Biometric	ZigBee	100 Kbps	Quantum SVM	Data Tampering	High	Yes
2	Insulin Pump	Therapeutic	Wi-Fi	11 Mbps	Quantum Neural Network	Denial of Service	Medium	Yes
3	Smart Inhaler	Therapeutic	Bluetooth	2 Mbps	Quantum Decision Tree	No Threat	N/A	Yes
4	Pacemaker	Implantable	Cellular	1 Mbps	Quantum SVM	Eavesdropping	High	No
5	Fitness Tracker	Biometric	Bluetooth	3 Mbps	Quantum Neural Network	No Threat	N/A	Yes

The following is a list of all of the parameters for the fields:

1. IoMT devices are what the name "IoMT Device" refers to in its most specific form.
2. The IoMT Device Type indicates the broad category that the device belongs to in its entirety (i.e., biometric, therapeutic, implantable, etc.)
3. Network Type: The configuration of the device's network at the present time (i.e., ZigBee, Wi-Fi, Bluetooth, Cellular, etc.)
4. The speed in megabits per second (Mbps) at which the device can send and receive data.
5. Implementation of the Quantum ML Method: When assessing the safety of a network, specialists frequently use quantum machine learning techniques such as Quantum Support Vector Machine (SVM), Quantum Neural Network, Quantum Decision Tree, and a variety of other approaches.
6. Type of Security Threat Identified: Specifies the type of security threat, if any, that was determined to have been identified (i.e., Data Tampering, Denial of Service, Eavesdropping, No Threat, etc.)
7. The level of danger that the threat poses can be characterized as "High", "Medium", "Low", or "Not Applicable".
8. This metric will read "Correct Detection" (Yes/No) depending on whether the quantum ML algorithm accurately identified the threat or the absence of such a threat.

This dataset may be given with real or simulated data, depending on the resources that are available and the ethical considerations that must be taken into account.

The first one for testing is the quantum machine learning multi-class. The labels indicate whether the code is a security risk or not. There are some reasons you might want to use Quantum Machine learning (QML) classification. It is easier for the developer to keep up with vulnerable code if it is first put into the QML. This makes sense because QML has already been used as a standard for identifying vulnerabilities. We used binary classification to compare our experimental outcomes with those of other studies in the field that used the same method.

An experiment under controlled conditions was carried out, using data gathered from IoMT devices already in operation. It was determined whether or not the proposed Quantum-Deep Learning (Q-Deep Learning) model was capable of efficiently locating vulnerabilities in the IoMT infrastructure by putting it through its paces in a series of tests. For the purpose of this inquiry, data was gathered from a diverse assortment of medical devices and computer systems located in several different types of healthcare facilities.

IBM's quantum machine learning capabilities were utilized throughout the tests. The quantum-enhanced model was trained and tested using the real-world dataset that was provided. The success of the model was evaluated based on how accurately it identified areas of data protection that needed improvement. Standard statistical methods were utilized in order to evaluate the performance of the model.

The well-respected quantum machine learning technology developed by IBM allowed the Q-Deep Learning model to execute complex calculations both more quickly and accurately than traditional machine learning approaches. The findings that were collected provided evidence that the method that was recommended was both useful and reliable in detecting security weaknesses in operational Internet of Things (IoMT) infrastructure. These findings illustrate the value of merging quantum computing with deep learning for the purpose of protecting applications used in the healthcare industry.

After Q-Deep QC was trained and verified, a set of measures was used to determine the best one. Our deep-learning model was built to make accurate predictions. The confusion matrix and classification model assessment metrics were used to determine whether the traffic on an IoMT network is harmful. Accuracy, precision, recall, and F1-score were also used to evaluate the classification Q-Deep QC models. Some of the measures considered were as follows:

$$\text{Accuracy} = \frac{\text{TP + TN}}{\text{TP + FP + TN + FN}} \tag{8}$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP + TN}} \tag{9}$$

$$\text{Precison} = \frac{\text{TP}}{\text{TP + FP}} \tag{10}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP + FN}} \tag{11}$$

$$\text{F1 score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision + Recall}} \tag{12}$$

Chaos in the Confusion Matrix Model (CMM) is used to determine how well the True Positives (TP), False Positives (FP), False Negatives (FN), and True Negatives (TN) work (TN). The CMM is also used to explain why the results of the classifier model make sense when they are applied to test data whose actual values are known. Table 3 shows how we used the confusion matrix to estimate what might be dangerous and what might be safe to interact with.

Table 3. Confusion matrix.

Confusion Matrix	Predicted Class (Benign)	Predicted Class (Malicious)
Actual Class (Benign)	TP	FN
Actual Class (Malicious)	FP	TN

The ROC curve, which stands for Receiver Operating Characteristic (ROC) curve, was used to show how clinical sensitivity and specificity trade-off against each other. The x-axis shows the number of false positives and the y-axis shows the number of true positives. ROC curve analysis uses measurements such as the Area Under the Curve (AUC) and the Area Between the Curves (ABC). The model can determine the difference between true positives and false positives if the area under the receiver operating characteristic curve (AUC) is greater than or equal to 0.70.

$$\text{Sensitivity} = \frac{\text{TP}}{(\text{TP} + \text{FN})} \tag{13}$$

$$\text{Specificity} = \frac{\text{TN}}{(\text{TN} + \text{FP})} \tag{14}$$

Experiments show how well different supervised machine-learning classification methods can predict whether IoT network traffic is harmful. So we can make sense of the test results, this is what will be carried out. Four main types of malicious software, namely Distributed Denial of Service (DDoS), Command and Control (C&C), Mirai, and Okiru were predicted for each category. Several different metrics, such as accuracy, precision, recall, and the F1-score, were used to judge the performance of a model. Before using it with a machine learning model, the IoT dataset was divided into thirds: 70% for training, 30% for testing, and 10% for 10-fold cross-validation. In the experiments, different ML classification methods were used, such as RL, BPNN, MLNN, CNN, QNN Q-Deep Learning model, and the proposed model. The IoT dataset was used to obtain the features used in these methods. This research also compares the evaluation criteria for the prediction models of the proposed technique with those of previous studies to predict whether IoT network traffic is malicious or harmless. Python was used to build the machine learning model and to put data mining strategies into action. IoT traffic can be both bad and good. Four measurements were used to determine the performance score: accuracy, precision, recall, and the F1 score.

Table 4 information is visualised in Figure 6. The proposed model performed well as shown in Figure 6.

Table 4. Results of several ML algorithms.

Model	Precision	Recall	F1	Accuracy
RL	0.7943	0.73431	0.73432	0.81323
BPNN	0.80235	0.75345	0.73456	0.82344
MLNN	0.8278	0.7767	0.7473	0.86765
CNN	0.8454	0.8334	0.8123	0.87347
Q-Deep Learning model	0.9145	0.8934	0.7934	0.92234
Proposed Model	0.9934	0.90345	0.80345	0.9934

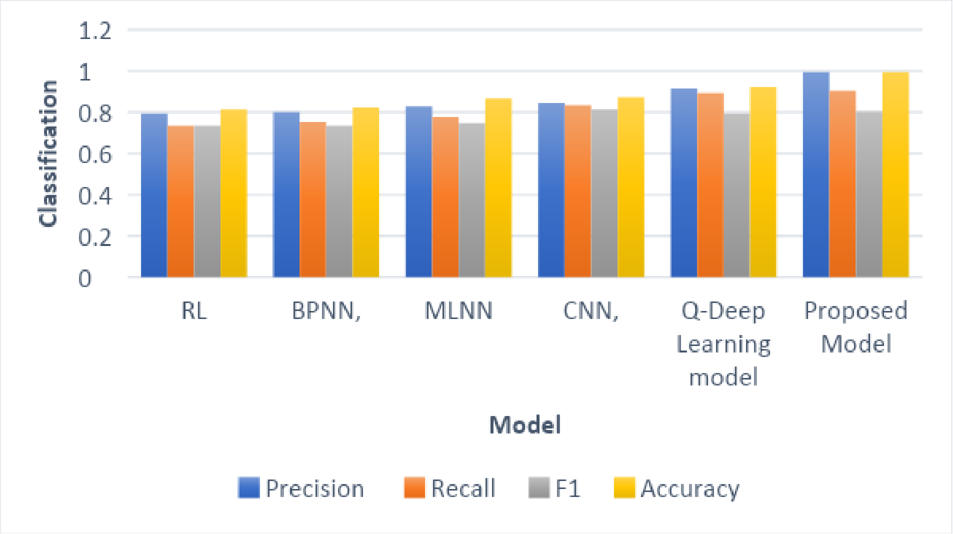


Figure 6. Comparative analysis different machine learning model.

The precision of each experimental model is also compared in Figure 7 with the proposed model outperforming the other models.

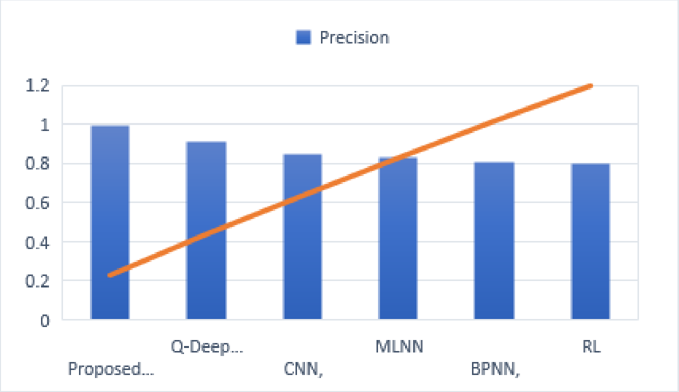


Figure 7. Comparative analysis of different machine learning models in terms of precision.

Vulnerability prediction in IoMT-based application in Figure 8 shows a comparison of the machine-learning algorithms based on the behavior of IoT devices using an existing dataset.

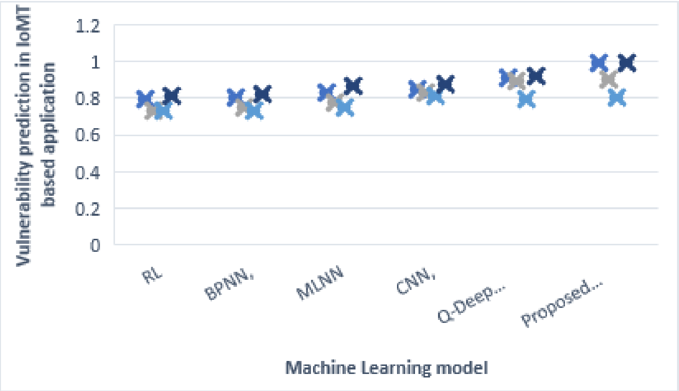


Figure 8. Vulnerability prediction in IoMT-based application.

Quantum machine learning (QML) exhibits promising results when evaluating the security of IoMT devices when compared to more typical machine learning techniques.

Quantum computing makes possible the rapid processing and analysis of massive IoMT datasets, which QML leverages to substantially cut down the amount of time spent on challenging computations and pattern discovery.

Using typical approaches to machine learning could be proven challenging due to the vast dimensionality, interconnection, and highly sensitive nature of the data in an IoMT environment. On the other hand, the fact that QML is able to manage high-dimensional data fields makes it an effective instrument for locating security vulnerabilities in IoMT systems. In addition to this, it is capable of doing many calculations concurrently, which significantly accelerates the process of vulnerability assessment. QML has the ability to increase prediction and generalization as a result of its status as a probabilistic language that is capable of modeling complex quantum states. This increases the accuracy with which vulnerabilities are found and categorized, which in turn contributes to an improvement in the dependability of IoMT security. The quantum advantage has taken on new significance in light of the increasing intricacy of cyberattacks and the critical importance of maintaining data privacy in the medical industry. We might be able to entirely rethink the way in which we evaluate the safety of IoMT systems by utilizing quantum computing, which would contribute to the systems becoming more reliable and secure.

4. Conclusions

In this study, we used machine learning classification algorithms to predict which vulnerability predictions in IoMT-based applications in IoT network traffic were malicious and which were not and to ensure that our predictions were correct. In this study, different types of malware and IoT botnets were examined and used to make predictions. This included DDoS, C&C, and a number of IoT botnets such as Mirai and Okiru. In terms of the accuracy rate and other parameters, this study was compared to others that used the same IoT dataset. We used a method called " Quantum Machine Learning" to find the most important parts of the dataset and compared our results with those of other studies that used the same dataset. Because of our work, machine learning methods such as RL, BPNN, MLNN, CNN, QNN Q-Deep Learning model, and the proposed model have become better at classifying objects. This was performed to create a model for explaining the difference between harmful and harmless IoT communications. With the help of the RL, BPNN, MLNN, and CNN algorithms, the most accurate model for making predictions was obtained. After the current scheme is completed, researchers will know a lot about how different types of malware attacks work in IoT. We will also examine the different types and sizes of malware attacks on IDS systems that use machine learning. We also test the IDS to see if it can find and stop programs that could be harmful from being sent over the network.

Author Contributions: Conceptualization, A.S.R.; Methodology, A.S.R. and S.B.G.; Software, A.S.R.; Validation, P.B., T.J. and M.P.; Formal analysis, S.B.G., P.B., T.J. and M.W.; Resources, S.B.G., T.J. and M.P.; Data curation, P.B.; Writing—original draft, A.S.R.; Writing—review & editing, A.S.R., S.B.G., P.B., T.J., M.W. and M.P.; Visualization, M.W.; Supervision, S.B.G.; Project administration, M.W.; Funding acquisition, T.J. and M.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jammula, M.; Vakamulla, V.M.; Kondoju, S.K. Artificial intelligence framework-based ultra-lightweight communication protocol for prediction of attacks in Internet of Things environment. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4680. [CrossRef]
2. Hussein, N.; Nhlabatsi, A. Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control. *IoT* **2022**, *3*, 450–472. [CrossRef]
3. Ramadan, R. Internet of Things (iot) Security Vulnerabilities: A Review. Available online: https://plomscience.com/journals/index.php/PLOMSAI/article/view/14 (accessed on 12 August 2023).

4. Puthal, D.; Wilson, S.; Nanda, A.; Liu, M.; Swain, S.; Sahoo, B.P.; Yelamarthi, K.; Pillai, P.; El-Sayed, H.; Prasad, M. Decision tree based user-centric security solution for critical IoT infrastructure. *Comput. Electr. Eng.* **2022**, *99*, 107754. [CrossRef]
5. Hasan, T.; Malik, J.; Bibi, I.; Khan, W.U.; Al-Wesabi, F.N.; Dev, K.; Huang, G. Securing industrial internet of things against botnet attacks using hybrid deep learning approach. *IEEE Trans. Netw. Sci. Eng.* **2022**. [CrossRef]
6. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT communications: A survey. *Sensors* **2020**, *20*, 4828. [CrossRef]
7. Razdan, S.; Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Tech. Rev.* **2022**, *39*, 775–788. [CrossRef]
8. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
9. Bouriche, A.; Bouriche, S. A systematic review on security vulnerabilities to preveny types of attacks in iomt. *Int. J. Comput. Inf. Manuf.* **2022**, *2*. [CrossRef]
10. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A.; Yelamarthi, K. Prospect of internet of medical things: A review on security requirements and solutions. *Sensors* **2022**, *22*, 5517. [CrossRef] [PubMed]
11. Koudia, S.; Cacciapuoti, A.S.; Simonov, K.; Caleffi, M. How deep the theory of quantum communications goes: Superadditivity, superactivation and causal activation. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1926–1956. [CrossRef]
12. Mishra, M.; Lourenço, P.B.; Ramana, G.V. Structural health monitoring of civil engineering structures by using the internet of things: A review. *J. Build. Eng.* **2022**, *48*, 103954. [CrossRef]
13. Jeon, H.; Lee, C. Internet of Things Technology: Balancing privacy concerns with convenience. *Telemat. Inform.* **2022**, *70*, 101816. [CrossRef]
14. Janani, K.; Ramamoorthy, S. Threat analysis model to control IoT network routing attacks through deep learning approach. *Connect. Sci.* **2022**, *34*, 2714–2754. [CrossRef]
15. Ali, I.; Ahmed, A.I.A.; Almogren, A.; Raza, M.A.; Shah, S.A.; Khan, A.; Gani, A. Systematic literature review on IoT-based botnet attack. *IEEE Access* **2020**, *8*, 212220–212232. [CrossRef]
16. Schuld, M.; Petruccione, F. *Supervised Learning with Quantum Computers*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 17. [CrossRef]
17. Joshi, S.; Sharma, M.; Das, R.P.; Rosak-Szyrocka, J.; Żywiołek, J.; Muduli, K.; Prasad, M. Modeling Conceptual Framework for Implementing Barriers of AI in Public Healthcare for Improving Operational Excellence: Experiences from Developing Countries. *Sustainability* **2022**, *14*, 11698. [CrossRef]
18. Singh, P.; Manjunatha, A.S.; Baig, A.; Dhopeshwar, P.; Huo, H.; Bharathy, G.; Prasad, M. Application of Artificial Intelligence in Healthcare by Industries in Australia: Opportunities and Challenges. In *Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021), Sur, Oman, 3–4 October 2021*; Sharma, H., Vyas, V.K., Pandey, R.K., Prasad, M., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 568–580.
19. Ban, X.; Ding, M.; Liu, S.; Chen, C.; Zhang, J. A Survey on IoT Vulnerability Discovery. In Proceedings of the Network and System Security: 16th International Conference, NSS 2022, Denarau Island, Fiji, 9–12 December 2022; Springer: Cham, Switzerland, 2022; pp. 267–282. [CrossRef]
20. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
21. Zhao, B.; Ji, S.; Lee, W.H.; Lin, C.; Weng, H.; Wu, J.; Zhou, P.; Fang, L.; Beyah, R. A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1826–1840. [CrossRef]
22. Meidan, Y.; Sachidananda, V.; Peng, H.; Sagron, R.; Elovici, Y.; Shabtai, A. A novel approach for detecting vulnerable IoT devices connected behind a home NAT. *Comput. Secur.* **2020**, *97*, 101968. [CrossRef]
23. Al-Boghdady, A.; El-Ramly, M.; Wassif, K. iDetect for vulnerability detection in internet of things operating systems using machine learning. *Sci. Rep.* **2022**, *12*, 17086. [CrossRef]
24. Zeng, M.; Yu, T.; Wang, X.; Nguyen, L.T.; Mengshoel, O.J.; Lane, I. Semi-supervised convolutional neural networks for human activity recognition. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 522–529. [CrossRef]
25. Ramezani, S.B.; Sommers, A.; Manchukonda, H.K.; Rahimi, S.; Amirlatifi, A. Machine learning algorithms in quantum computing: A survey. In Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 19–24 July 2020; pp. 1–8. [CrossRef]
26. Qu, Z.; Meng, Y.; Liu, B.; Muhammad, G.; Tiwari, P. QB-IMD: A secure medical data processing system with privacy protection based on quantum blockchain for IoMT. *IEEE Internet Things J.* **2023**. [CrossRef]
27. Zanbouri, K.; Al-Khafaji, H.M.R.; Navimipour, N.J.; Yalçın, Ş. A new fog-based transmission scheduler on the Internet of multimedia things using a fuzzy-based quantum genetic algorithm. *IEEE MultiMedia* **2023**, 1–12. [CrossRef]
28. Vajner, D.A.; Rickert, L.; Gao, T.; Kaymazlar, K.; Heindel, T. Quantum communication using semiconductor quantum dots. *Adv. Quantum Technol.* **2022**, *5*, 2100116. [CrossRef]
29. Bharathi, M.; Amsaveni, A. Machine Learning with IoMT: Opportunities and Research Challenges. In *Internet of Medical Things: Remote Healthcare Systems and Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 235–252.

30. Al-Hawawreh, M.; Hossain, M.S. A privacy-aware framework for detecting cyber attacks on internet of medical things systems using data fusion and quantum deep learning. *Inf. Fusion* **2023**, *99*, 101889. [CrossRef]
31. Rahmani, A.M.; Hosseini Mirmahaleh, S.Y. Flexible-Clustering Based on Application Priority to Improve IoMT Efficiency and Dependability. *Sustainability* **2022**, *14*, 10666. [CrossRef]
32. Anitha Kumari, K.; Padmashani, R.; Varsha, R.; Upadhayay, V. Securing Internet of Medical Things (IoMT) using private blockchain network. In *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 305–326.
33. Watkins, C.J.; Dayan, P. Q-learning. *Mach. Learn.* **1992**, *8*, 279–292. [CrossRef]
34. Zikria, Y.B.; Afzal, M.K.; Kim, S.W. Internet of multimedia things (IoMT): Opportunities, challenges and solutions. *Sensors* **2020**, *20*, 2334. [CrossRef]
35. Fiaidhi, J.; Mohammed, S. Security and vulnerability of extreme automation systems: The IoMT and IoA case studies. *IT Prof.* **2019**, *21*, 48–55. [CrossRef]
36. Geng, J.; Luo, P. A novel vulnerability prediction model to predict vulnerability loss based on probit regression. *Wuhan Univ. J. Nat. Sci.* **2016**, *21*, 214–220. [CrossRef]
37. Imran, M.; Zaman, U.; Imran; Imtiaz, J.; Fayaz, M.; Gwak, J. Comprehensive survey of iot, machine learning, and blockchain for health care applications: A topical assessment for pandemic preparedness, challenges, and solutions. *Electronics* **2021**, *10* 2501. [CrossRef]
38. Manickam, P.; Mariappan, S.A.; Murugesan, S.M.; Hansda, S.; Kaushik, A.; Shinde, R.; Thipperudraswamy, S. Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare. *Biosensors* **2022**, *12*, 562. [CrossRef]
39. Patel, O.P.; Bharill, N.; Tiwari, A.; Patel, V.; Gupta, O.; Cao, J.; Li, J.; Prasad, M. Advanced Quantum Based Neural Network Classifier and Its Application for Objectionable Web Content Filtering. *IEEE Access* **2019**, *7*, 98069–98082. [CrossRef]
40. Patel, O.P.; Tiwari, A.; Chaudhary, R.; Nuthalapati, S.V.; Bharill, N.; Prasad, M.; Hussain, F.K.; Hussain, O.K. Enhanced quantum-based neural network learning and its application to signature verification. *Soft Comput.* **2019**, *23*, 3067–3080. [CrossRef]
41. Patel, O.P.; Bharill, N.; Tiwari, A.; Prasad, M. A Novel Quantum-Inspired Fuzzy Based Neural Network for Data Classification. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1031–1044. [CrossRef]
42. Bharill, N.; Patel, O.P.; Tiwari, A.; Mu, L.; Li, D.L.; Mohanty, M.; Kaiwartya, O.; Prasad, M. A Generalized Enhanced Quantum Fuzzy Approach for Efficient Data Clustering. *IEEE Access* **2019**, *7*, 50347–50361. [CrossRef]
43. Chaganti, R.; Mourade, A.; Ravi, V.; Vemprala, N.; Dua, A.; Bhushan, B. A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. *Sustainability* **2022**, *14*, 12828. [CrossRef]
44. Rahman, A.; Hossain, M.S.; Muhammad, G.; Kundu, D.; Debnath, T.; Rahman, M.; Khan, M.S.I.; Tiwari, P.; Band, S.S. Federated learning-based AI approaches in smart healthcare: Concepts, taxonomies, challenges and open issues. *Clust. Comput.* **2022**, *26*, 2271–2311. [CrossRef]
45. Hussien, H.M.; Yasin, S.M.; Udzir, S.; Zaidan, A.A.; Zaidan, B.B. A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *J. Med. Syst.* **2019**, *43*, 1–35. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.