Journal of Computer Science

Original Research Paper

Quantum-Enhanced IoT-Cloud Security: Integrating SHAP and Variational Quantum Classifiers

[1,2]Veena Antony and [3]Nainan Thangarasu

[1]*Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India*
[2]*Department of CyberSecurity and Applied Computing, St. Teresa's College (Autonomous), Ernakulam, India*
[3]*Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India*

Article history
Received: 29-09-2024
Revised: 14-11-2024
Accepted: 23-11-2024

Corresponding Author:
Veena Antony
Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
Email: veenaantony22@gmail.com

Abstract: In the current Internet era, there are now trillions of gadgets online, and the Internet of Things is becoming a necessary part of daily life. IoT devices are connected, but this also makes them vulnerable to cyberattacks. Cyberattacks targeting Internet of Things (IoT) systems have increased dramatically in both volume and sophistication in the last year. Determining the importance and explainability of significant feature selection is not done in conventional feature selection, which acts as a black box method. Classical machine learning suffers from overload and class imbalance issues in IoT-based cloud security which is the major issue that results in botnet attack detection. To overcome these two issues, this study developed a model of a feature map to encode conventional data to a quantum feature space and then utilize the newly created quantum data in the cognitive circuit, which motivates to development of Quantum Shapley Additive Explanation with Variational Quantum Classifier (QSHAP-VQC) is implemented. This makes it possible to employ classical data in a quantum circuit. To minimize a cost function, a VQC employs hybrid quantum-classical techniques that involve parameterized circuits and gates whose parameters are improved via a classically based optimization loop. A quantum-classical hybrid loop consisting of these steps is eventually broken when the classical optimization finds the ideal parameters. For training data, the usual cost function is a comparison of the actual and expected outputs. The proposed QSHAP-VQC achieves the highest rate of accuracy in the detection of attacks in an IoT cloud environment.

Keywords: Quantum Cryptography, Parameter Optimization, Shapley Additive Explanation, Variational Quantum Classifier, IoT, Cloud Security, Botnet

Introduction

The Internet of Things integrated systems are currently proliferating and encompassing many geographically dispersed networks of diverse equipment functioning in an insecure environment (Ali *et al*., 2020). These devices use core and secondary cloud services to facilitate communication and business tasks while interacting locally. IoT devices are often used without the owners' knowledge as instruments in cyberattacks. These gadgets have the potential to be taken over and added to a "botnet," or collection of compromised devices. These botnets, which are networks of individual computers controlled collectively and contaminated with malware, are frequently employed in cyber security attacks especially botnet attacks (Alshamkhany *et al*., 2020). Because these devices frequently have insufficient security measures, the involvement of IoT in these botnets is becoming more and more concerning.

Four kinds of botnet architecture are distinguished: Hierarchical, random, multiple-server, and star topologies (Ragunthar *et al*., 2021). As illustrated in Fig. (1), the centralized botnet, sometimes referred to as star topology, is the most widely used and swiftly spreading kind of botnet. The control-and-command server announces a command to all the bots when a bot master publishes it, starting an attack (Wazzan *et al*., 2021). As soon as the bots get the order, they will launch the attack using the strategy that the bot manager has prepared. A web host or researcher can discover and use the control-and-command system, which is the foundation of this architecture, to successfully take down a botnet.

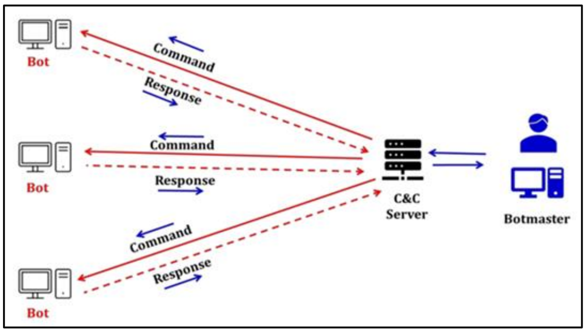

Fig. 1: Star topology of botnet attack in IoT

The assault will not be successful if the connection among the control-and-command servers is interrupted because the bots cannot get commands from the bot master. The total count of servers varies from the star topology in many server architectures. Because of how easily things might go wrong, many server topologies modify the setup of the control-and-command servers. Every control-and-command server in the network is set up to send out commands. The botnet will continue to operate as planned even if any of the servers is discovered and malfunctions; a substitute server is going to take its place. According to the bot master, the attack will go on regardless of whether each of the servers is up and running.

IoT networks typically have several entry points that could be used by hostile actors to compromise the devices. These access points can be found remotely via wireless communication protocols, the Internet, or cloud infrastructure, or they can be found inside the network's communication boundary (Kumar and Lim, 2020). Such networks are particularly susceptible to several kinds of harmful impacts because of this situation.

The dynamic aspect of IoT cloud functioning that includes the capacity to alter the devices' composition, location, settings, data, profiles, user behavior features, and data flow structure is a crucial component of the technology. This is specifically caused by the organizational and technological difficulties involved in upgrading such devices, which frequently entails performing manual maintenance on the device and upgrading the firmware to fix vulnerabilities. All these calls for the creation of specialized methods for guaranteeing the information confidentiality of IoT clouds, methods that would take into consideration their characteristics and enable the successful detection and reaction to threats in addition to the prevention of potential assaults.

The ability to collect and analyze data from numerous similar or distinct IoT clouds using the cloud's virtually limitless computational resources negates the need to implement computationally demanding protection algorithms. This is one of the main benefits when employing the cloud and its offerings to guarantee the confidentiality of IoT clouds. Apart from examining Big Data and recognizing diverse trends that impact IoT cloud maintenance and user requirements, cloud infrastructure also enables the identification of dispersed coordinated attacks (Darshan and Divyanka, 2023).

These assaults can take the shape of intricate multi-step schemes and botnets, involving tens of thousands of devices from various IoT clouds and employing techniques like SYN port flooding, port sweeping, and scanning. It appears that identifying such assaults locally within the hardware of each unique IoT network would be very challenging, if not impossible.

However, there are inherent drawbacks to these cloud services for information security. Specifically, they are the practical impossibility of supplying the entirety of network security data transferred to the cloud, as well as the inherent communication constraints of network communication routes. It results in the requirement to extract, compile, and transfer to the cloud only the bare minimum of required data. Furthermore, the ability to transfer any user data, or even small portions of it, to the cloud is restricted by law and marketing due to privacy concerns. Specifically, providing entirely anonymized user data may result in legitimate legal inquiries to the provider as well as harm to the company's reputation from a lack of end-user awareness (Mijwil *et al*., 2023).

Thus, decentralizing security measures and attack detection methods is thought to be a potential strategy for managing the security of an IoT network. This proposed work contributes a novel quantum theory with the SHAP method to select the potential features and improve the computation complexity while detecting attacks in IoT clouds.

A unique collection of features from different attacks is extracted and constructed by analyzing the original traffic to generate each model.

The proposed methodology’s approach is novel as represented below:

- Uses the types of network attacks that have been chosen as an essential component of intricate, multi-step actions
- Creates and extracts feature sets for these attacks based on the properties of TCP/IP traffic in Internet of Things clouds
- Combines specific, machine learning-based adaptations of widely used classification techniques. Furthermore, in contrast to previous analogs, the concurrent examination of several facets of TCP/IP information in IoT clouds enables the identification of an assault as well as its primary attributes
- The significance of the proposed methodology is demonstrated by an improvement in recognizing indicators of quality, which is validated through experimental means

Literature Review

Muñoz and Valiente (2023) focused on aspects of network traffic that may indicate cybersecurity risks to the Internet of Things networks and impacted network nodes. Using the components that were obtained on each IoT console, particular attribute vectors were also produced. To manage cyberattacks in real-time communication, such good prediction is required. The model may be used to predict cyberattacks in real-time, even in large-scale IoT deployments, due to its efficiency and scalability. Its ability to compute efficiently enables it to produce precise predictions quickly, enabling timely detection and intervention.

Intrusion Detection Systems (IDSs) fall into one of two primary categories as discussed by the authors (Khraisat *et al*., 2019) look for previously identified patterns in data sent over the network, sadly, the efficacy of these systems is declining. It uses machine learning techniques to identify variations in the network's learned behavior. To avoid being discovered, attackers need to be aware of typical behavior.

Kumar *et al*. (2022) utilized Autocorrelation Function based tests to identify individual bots after classifying aggregate traffic using supervised machine learning techniques. A policy engine, a feature extractor, a traffic parser, and a malware traffic database are further components of the EDIMA architecture.

This study explored by Azam *et al*. (2023) the security features, procedures, risks, and practical applications of security-related technologies for cloud computing and Internet of Things services. We also examine the effects of cloud computing and Internet of Things security services, including their advantages, drawbacks, and prospects. To give readers a basic knowledge of these technologies, we describe cloud computing and the Internet of Things (IoT) in our exploration. Subsequently, we explore their practical uses, emphasizing their pertinence and abundance across several fields.

In the article (Joseph and Jayapandian, 2022), the authors describe many kinds of security risks that impact cloud computing and the Internet of Things. Machine learning is used to categorize these threats. Applications' runtime behavior can be exploited to identify malware using supervised learning methods. The malware is identified by its unusual behavior, which is discovered through network traffic. After the malware has been identified, application data is kept in a database that has been educated using an ML classifier like KNN or Random Forest. The model can more accurately identify malicious programs with more training.

The work of (Priyatharsini *et al*., 2022) covers the secure online verification of IoT device settings to offer further value-added services. Provide a Cloud-based architecture that permits communication between IoT devices and several federated Cloud services after reviewing the safe self-configuration restrictions placed on IoT and Cloud technologies. Talk about two specific scenarios, one in which federated cloud infrastructure, and a cloud environment interact with IoT devices and address special problems. Furthermore, it offers a plethora of operational design elements that consider the existing hardware and software products that are truly open.

A unique hybrid honeynet driven by artificial intelligence AI and cloud computing CC for improved IoT botnet detection rates in the work (Memos and Psannis, 2020). This new security feature predicts the possible existence of a botnet by utilizing Machine Learning such as Logistic Regression, Naïve Bayes (Shang, 2024), etc.

To detect and stop harmful attacks in an environment involving cloud computing, Arunkumar and Kumar (2023) developed an innovative combination of support vector machine-extreme learning machine techniques based on the Gannet Optimization Algorithm. It is utilized to minimize information loss and choose the best characteristics. The GOA method optimizes the variables of the combined SVM-ELM model.

To reduce the DDoS threat, a DDoS detection technique based on Random Forest Classifier and Grey Wolf Optimization algorithms was created in this study (Savita and Taran, 2023). Botnet attacks can be identified using the staked boosted LSTM encoder method. Offering an improved detection system to recognize impending threats is the study's main goal. The solution offers excellent accuracy by combining deep learning and machine learning with proactive security (Aruna and Prayla, 2024).

Materials and Methods

The experiment was conducted in a cloud-based environment using Google Cloud IoT platform. To detect Botnet attacks public dataset UNSW-NB15 is used to provide labeled data for training and testing. Raw traffic data was preprocessed to extract features such as: Packet size, flow duration, source/destination IP, protocol type, and port usage.

The proposed work architecture is depicted in Fig. (2), the main objective of this newly developed Quantum SHAP model with enhanced Variational Quantum classifier is to prevent botnet attacks from occurring in the IoT clouds. The IoT clouds are used for cost-effective resource storage, but the attackers find a high chance of possible attacks that could be done with botnets to affect the service to the cloud users. Hence in this study to detect botnet attacks in the IoT cloud, a novel quantum theory-based feature selection using SHAP value and classification of legitimate and abnormal attacks are discovered by the variational quantum optimizer by optimizing the parameters of a classifier to produce a high detection rate. The dataset used for attack detection is collected from the UNSW-NB15 dataset with 2,57,673 records (Moustafa and Slay, 2015).

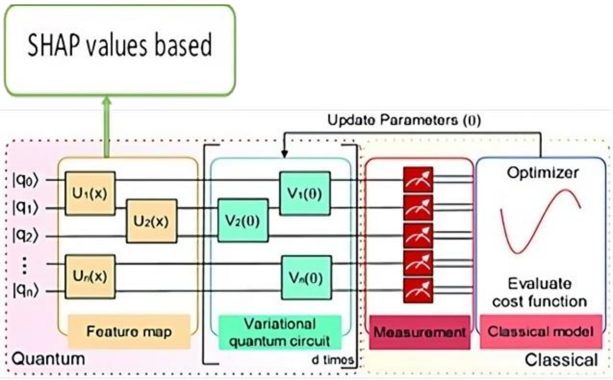

Fig. 2: Proposed model: Integrating SHAP and variational quantum classifiers

As illustrated in Fig. (2), the proposed model of the IoT cloud botnet attack data is initially encoded into a quantum state by VQCs. A feature map, a type of quantum circuit that receives data as input and outputs a quantum state, is used to do this. A variational quantum circuit, or a quantum circuit that is parameterizable, receives the quantum state after that. Next, a classical machine learning technique is used to optimize the variational quantum circuit's parameters to minimize a loss function. The effectiveness of the VQC in classifying the data is indicated by the loss function. New instances can be classified using the variational Quantum Circuit (VCCR) once its parameters have been optimized. In order to accomplish this, the feature map is used to encode the data point into a quantum state, which is subsequently sent to the VCCR. Next, over the various classes, VCCR generates a probability distribution. Next, the type of data point is projected to be the one with the highest likelihood.

Feature Selection Based on the SHAP Model

Shapley additive explanation (SHAP) has been a well-liked technique for deciphering predictions from machine learning models. SHAP offers information about how each attribute contributes to particular predictions by using strategies from Game Theory (Schuld *et al*., 2015; Sheoran and Yadav, 2024). It's one of a category of model-independent additive feature attribution approaches that may be used with a wide range of deep learning and machine learning models. These methods assist in gaining a deeper comprehension of the behavior of the model by assigning significance to specific input features.

The mean absolute ratings for each feature are then determined by computing SHAP values for each instance and averaging these values over the whole dataset. This technique makes the calculation of SHAP values computationally hard. The absolute SHAP score reflects the significance of a feature regardless of its tendency (negative or positive), but the average SHAP score shows the average influence of each feature on predicted models over the whole dataset. Higher SHAP features are recognized as having a greater influence on the model's predictions by ranking the features according to their mean relative SHAP values in order of decreasing importance.

Preamble of Quantum Machine Learning

Classification tasks play a significant role in the broad field of machine learning. An algorithm is trained to identify labeled subsets within provided data in a supervised training circumstance (Farhi and Neven, 2020). After it has been trained, this structure can be utilized for organizing unlabeled data since it learns the characteristics that collectively define each label. Additionally, ongoing efforts are being undertaken to identify situations in which quantum solutions are preferable to conventional, standard methods. The goal of this effort is to find quantum algorithms that are either exponentially more efficient or substantially quicker than their digital equivalents. If a breakthrough of this sort were made, let us discuss the merits of using the quantum concept.

A new multidisciplinary research field that blends ML with quantum physics is called Quantum Machine Learning (QML). Using QML enhances QC's performance and expedites the data processing process.

Data Normalization

In this study, the min-max normalization is applied to convert the different range of values in each attribute of the botnet dataset to convert to a common range of values using the formula:

$$X = (X - min) / (max - min) \tag{1}$$

where, *X* is the attribute value *min* and *max* are the minimum and maximum range of values of a particular attribute.

State Preparation

In order to prepare data for processing, state preparation is required in QML. In supervised learning, for instance, a common function classification involves computing the function f to map the input data (*x*) and the output labels (*z*) to become $z = f(x)$. Enhancing prediction model accuracy is the main objective of classification. The binary classification $Z = \{d_1, d_2, \dots. d_n\}$ where *Z* is the target variable and a collection of data in the training phase in such a way that the conventional machine learning domain can describe it as:

$$C = \{(x_1, y_1), (x_i, y_i), \dots (x_n, y_n)\} \tag{2}$$

where, features (n) are denoted as x_i on the properties of the order of instance I and y_i is the related instance. In binary classification $y_i \epsilon (L_1, \ L_2)$.

To illustrate the same framework in the quantum machine learning domain, the initial process is to convert the classical data to quantum data as denoted in training data as shown in the equation below:

$$E_n = \{((\langle\psi_1\rangle, z_1), \dots ((\langle\psi_i\rangle, z_i), \dots ((\langle\psi_n\rangle, z_n) \tag{3}$$

where, the quantum state of E_n is denoted as $\langle\psi_1\rangle$ and $z_i \in L_1,\ L_2$.

To transform classical data to quantum data, in this study basic encoding is used. Using the following equation, this method establishes a connection between n-bit classical data points and the computational foundation of n-qubit data points, like classical information (1001) enciphered to four qubits |1001> quantum data:

$$|C\rangle = \frac{1}{\sqrt{P}} \sum_{p=1}^{P} |x^p\rangle \tag{4}$$

where, C is the classical data, $\{\, C = x^1, x^2 \ldots., x^p \,\}$ produce a binary vector, $x^p = \{d_1^p, d_2^p, \ldots, d_N^p\}$, $d_i^p \in \{0,1\}, i \in \{1,2, \ldots, P\}$ and P refers to a number of features in the dataset.

Variational Quantum Classifier

Mainly used for supervised QML classification applications, the Variational Quantum Classifier (VQC) is an important algorithm for classifying quantum events that are relevant to environmental events. It provides a classification of the complexity involved in approximating the Ising and Tutte partition functions with complex parameters and investigates their connections to quantum computation. (Havlíček *et al.*, 2019; Saxena and Nigam, 2022, Goldberg and Guo (2017).).

Iterative device measurements are used to generate the cost function, which reduces mistakes by incorporating noisy data into the optimization calculations. This quantum technique, which is based on quantum circuits that are challenging to replicate conventionally, maps conventional input data to an expanding quantum feature space. In VQC, classical data is embedded into quantum computing through a variety of feature mapping approaches. This process begins with the preliminary preparation of QML issues. The variational circuit has the same dimensions and number of measurements. Lastly, a circuit receives the measured value as feedback to enhance the trainable parameters of the variational circuit as depicted in Fig. (3).

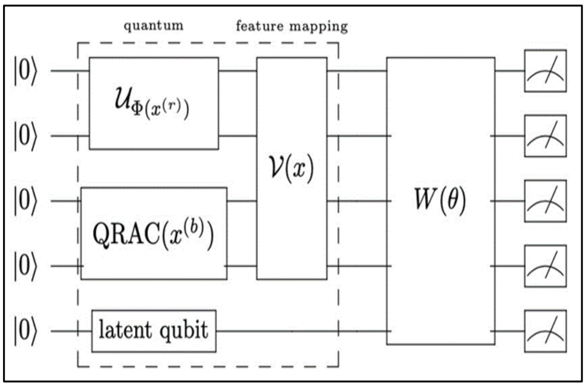

Fig. 3: Process of variational quantum classifier

The standard machine learning kernel technique, which maps a dataset non-linearly into a higher-dimensional space to identify a hyperplane that classifies non-linear data, is the source of the fundamental idea behind quantum feature mappings.

Our feature space (Fi) has now increased in dimension due to the unitary operation applied to the starting state and our classifier's job is to locate a separating hyperplane in this enlarged space. Which include the depth (dp) of the circuit and the layer of Hadamard gates (H) sandwiched between entangling blocks encoding the classical data. The quantity of qubits needed depends on the data's dimension. Unitary gates are used to encode the data. When non-traditionally generated quantum feature maps are used instead of characteristic maps that can be modeled on classical computers, the quantum advantage becomes apparent.

This method's fundamental principle is to optimize the parameters by following the guidance of an objective function. Variational quantum circuits have two unique phases: The quantum phase and the classical phase. State preparation in the variational quantum circuit parameterized input depending on the number of parameters and measurements included in that procedure. The learning algorithm, the objective function, and the circuit's output comprise the classical phase. The VQC is estimated via optimization approaches such as restricted optimization by linear approximations.

The assessment stage, which comes next, uses a definitive measurement to evaluate the class possibilities. It is equivalent to computing the average value of several samples taken from a distribution of possible computational base states. The aim of training is to find the parameter values that will optimize a specific loss function. Like how we can optimize a traditional neural network, we can also optimize a quantum model. Calculate the loss function by running the model forward in both scenarios. The gradient-based optimization techniques update our trainable parameters as loss functions fluctuate during training because the gradient of a quantum circuit can be determined. This technique allows us to calculate the loss function value, which represents the difference between our estimates and the actual data. When the measurements are prepared, an optimization procedure is used to update the parameter values of the VQC. Our parameters are trained using the classical loop until the value of the cost function drops.

Experimental Results and Discussion

This section discusses in detail the performance of the proposed Quantum Shapely Additive Explanation Model with Variational Quantum Classifier (QSHAP-VQC) deployed using Python software to detect botnet attacks in the IoT cloud environment. To detect botnet attacks, the training dataset comprised 1,75,341 records and the testing dataset is 82,332 records. The python software is used to develop the proposed QSHAP-VQC Model.

The confusion matrix to measure the efficiency model is depicted in Table (1).

In Table (2), the botnet and normal attacks correctly predicted are 26,312 and 55,850 respectively. The process of the quantum SHAP model with Variational Quantum Classifier effectively detects the botnet attacks more prominently.

The proposed QSHAP-VQC performance is compared with a conventional support vector classifier [Arunkumar, M., & Kumar, K], Random Forest [Savita, D., & Taran], and conventional variational quantum classifier [Saxena, N., & Nigam]. The metrics used for analysis are accuracy, precision, recall, and mean square error.

Table (3) explores the comparative analysis of four different IoT botnet security attack detection models in cloud computing. The result shows that the performance of the newly devised quantum SHAP model as feature selection and Variation quantum classifier to detect the normal and abnormal packets entering inside the IoT network in the cloud environment achieves the highest accuracy rate of 98.1% compared with other existing models.

The proposed model QSHAP-VQC has a much more balanced distribution of the feature's importance, with significant features selected by the quantum SHAP model. The computation of the contribution of each feature played a vital role in improving the detection rate effectively compared with the other machine learning models, which work as a black box to produce output. It is difficult to find what makes the misclassification rate. Hence, in this proposed work quantum Shapley feature selection is used to determine the contribution of each feature, and a variational Quantum classifier is used to determine the patterns of the input data and the corresponding output generated based on the cost function during the training phase it achieves higher rate of accuracy is depicted in Fig. (4).

Table 1: Confusion matrix

		True label	
		Botnet	Normal
Predicted label	Botnet	True positive	False positive
	Normal	False-negative	True negative

Table 2: Result of proposed model confusion matrix

		True label	
		Botnet	Normal
Predicted label	Botnet	26,312	20
	Normal	150	55,850

Table 3: Performance result

Prediction Models	Accuracy	Precision	Recall	MSE
SVC	80.8	82.3	83.5	0.48
VQC	85.2	87.2	88.1	0.37
Random Forest	89.9	90	90.1	0.22
QSHAP-VQC	98.1	98.3	98.4	0.1

When comparing the proposed framework QSHAP-VQC to the existing techniques for cloud-based IoT botnet attack detection, the latter achieves the highest rate of precision. In order to improve cloud computing's security measures for IoT botnet attack detection, novel perspectives into the algorithm are provided by the notion of quantum theory and the SHAP approach, which uncovers unanticipated correlations between input characteristics and the target variable. Thus, in Fig. (5), QSHAP-VQC achieves a precision rate of 98.1%, while SVC, QSVC, and Random Forest produce 79.4%, 86.7%, and 89.6% respectively.

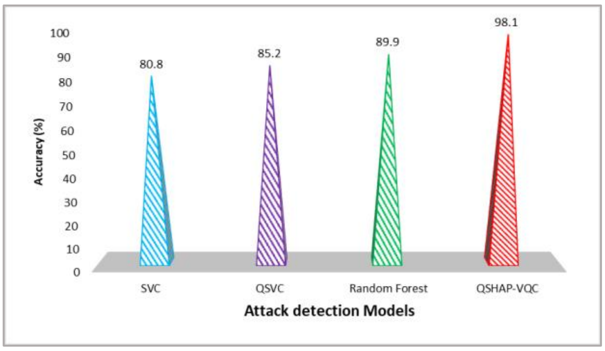

Fig. 4: Rate of accuracy

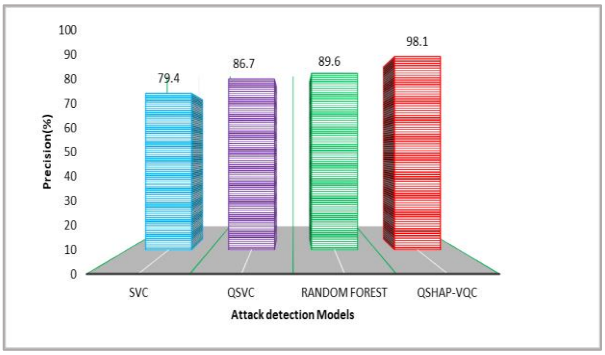

Fig. 5: Precision rate

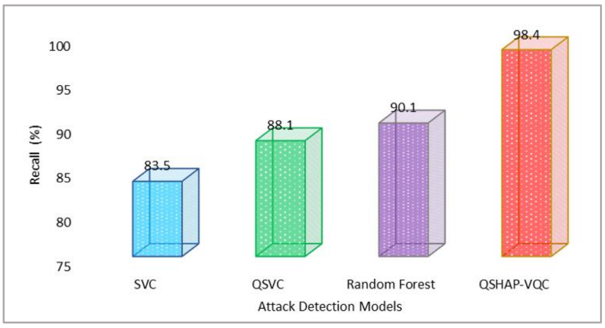

Fig. 6: Recall rate

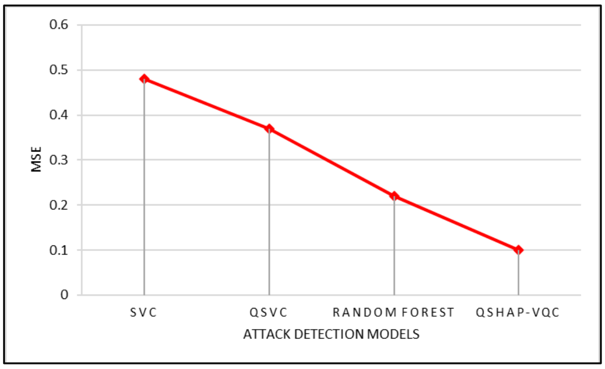

Fig. 7: Mean square error rate

The recall value obtained by the four IoT botnet attack detection models is depicted in Fig. (6). The results show that QSHAP-VQC with the reduced feature subset selection using Quantum Shapley values and using Variational Quantum Classifier achieves better performance of recall value compared to other standard classification models. This method compares the predictions made by a model with and without a feature, assigning a relevance value to each one for a given prediction. Because the computation considers all potential feature combinations and takes the effects of interaction between features into account, it guarantees equitable imputation. In Fig. (6), the recall rate of QSHAP-VQC is higher than the other existing models as it attains a value of 98.4%.

As shown in Fig. (7), the suggested QSHAP-VQC has a much lower mean square error rate when compared to the existing algorithms for IoT botnet attack detection in the cloud. The proposed QSHAP-VQC algorithm achieves the lowest error rate compared to other advanced algorithms due to its utilization of the quantum concept in machine learning. The anticipated VQC attained during the training process has a fundamentally different approach to feature importance compared to the conventional approaches for the prediction of botnet attacks in cloud-based IoT.

Discussion

The SHAP-integrated Gradient Boosting Model outperformed baseline approaches such as.

SVC: Accuracy of 80.8%, lower due to oversimplification of feature relationships:

- VQC: Accuracy of 85.2%, limited by higher false-positive rates
- Random Forest: While achieving comparable accuracy (89.9%), lacked interpretability compared to QSHAP-VQC based explanations

Conclusion

Although this study provides an overview of current developments in quantum machine learning research, it is important to note that it is not an exhaustive analysis. It is crucial to have a thorough understanding of both machine learning and quantum information processing before exploring their interaction. Most of the research in quantum machine learning so far has come from specialists in quantum information processing and classical machine learning and this successful multidisciplinary collaboration has produced a lot of positive results. Hence, in this proposed work a novel Quantum SHAP-based feature selection and Variational Quantum Classifier is developed to predict the botnet attacks in IoT clouds. First, it makes use of quantum computing's high parallelism to improve machine learning's capacity for managing, interpreting, and mining massive amounts of data. Second, it encourages innovation and the creation of fresh machine-learning algorithms by taking inspiration from the ideas of quantum physics. Thirdly, it draws inspiration from conventional machine learning methods to suggest novel study directions that will propel quantum mechanics research forward. The simulation results proved quantum machine learning is the most promising area in the field of IoT cloud-based cybersecurity. In the future, we will improve the efficiency and dependability of quantum machine learning in our next work with the goal of contributing significantly to the resolution of challenging issues, the improvement of algorithms, and the achievement of more useful applications and scientific advances.

Acknowledgment

The authors express their gratitude to Karpagam Academy of Higher Education for their recommendations and unwavering support during the experimental work.

Funding Information

This research received no external funding.

Author’s Contributions

Veena Antony: Proposed methodology, experimental results, and discussion, Reviewing and edited.

Nainan Thangarasu: Identifying the security issues in IoT, literature review, designed the research plan.

Ethics

This article does not contain any studies with animals performed by any of the authors.

Data Availability Statement

The authors declare that all data supporting this study's findings are available within the article.

Conflicts of Interest

The author declares no potential conflict of interest.

References

Ali, I., Ahmed, A. I. A., Almogren, A., Raza, M. A., Shah, S. A., Khan, A., & Gani, A. (2020). Systematic Literature Review on IoT-Based Botnet Attack. *IEEE Access*, *8*, 212220–212232. https://doi.org/10.1109/access.2020.3039985

Alshamkhany, M., Alshamkhany, W., Mansour, M., Khan, M., Dhou, S., & Aloul, F. (2020). Botnet Attack Detection using Machine Learning. *2020 14th International Conference on Innovations in Information Technology (IIT)*, 203–208. https://doi.org/10.1109/iit50501.2020.9299061

Aruna, J., & S. Prayla, S. (2024). Botnet Attack Detection in the Network with SBLSTM Classification. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(20s), 331–337.

Arunkumar, M., & Kumar, K. A. (2023). GOSVM: Gannet Optimization Based Support Vector Machine for Malicious Attack Detection in Cloud Environment. *International Journal of Information Technology*, *15*(3), 1653–1660. https://doi.org/10.1007/s41870-023-01192-z

Azam, H., Tajwar, M. A., Mayhialagan, S., Davis, A. J., Yik, C. J., Ali, D., & Sindiramutty, S. R. (2023). Innovations in Security: A Study of Cloud Computing and IoT. *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, *2*(1), 1–29. https://doi.org/10.54938/ijemdcsai.2023.02.1.252

Darshan, I., & Divyanka, I. (2023). An Enhanced Blockchain Based Security and Attack Detection Using Transformer in IOT-Cloud Network. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *31*(2), 142–156. https://doi.org/10.37934/araset.31.2.142156

Farhi, E., & Neven, H. (2020). Classification with Quantum Neural Networks on Near Term Processors. *ArXiv*, *2*, 1–21. https://doi.org/10.48550/arXiv.1802.06002

Goldberg, L. A., & Guo, H. (2017). The Complexity of Approximating Complex-Valued Ising and Tutte Partition Functions. *Computational Complexity*, *26*(4), 765–833. https://doi.org/10.1007/s00037-017-0162-2

Havlíček, V., Córcoles, A. D., Temme, K., Harrow, A. W., Kandala, A., Chow, J. M., & Gambetta, J. M. (2019). Supervised Learning with Quantum-Enhanced Feature Spaces. *Nature*, *567*(7747), 209–212. https://doi.org/10.1038/s41586-019-0980-2

Joseph, T. A., & Jayapandian, N. (2022). Detection of Various Security Threats in IoT and Cloud Computing using Machine Learning. *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 996–1001. https://doi.org/10.1109/icscds53736.2022.9760791

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges. *Cybersecurity*, *2*(1), 20. https://doi.org/10.1186/s42400-019-0038-7

Kumar, A., & Lim, T. J. (2020). Early Detection of Mirai-Like IoT Bots in Large-Scale Networks Through Sub-Sampled Packet Traffic Analysis. In K. Arai & R. Bhatia (Eds.), *Advances in Information and Communication* (Vol. 70, pp. 847–867). Springer International Publishing. ISBN-10: 978-3-030-12385-7. https://doi.org/10.1007/978-3-030-12385-7_58

Kumar, A., Shridhar, M., Swaminathan, S., & Lim, T. J. (2022). Machine Learning-Based Early Detection of IoT Botnets Using Network-Edge Traffic. *Computers and Security*, *117*, 102693. https://doi.org/10.1016/j.cose.2022.102693

Memos, V. A., & Psannis, K. E. (2020). AI-Powered Honeypots for Enhanced IoT Botnet Detection. *2020 3rd World Symposium on Communication Engineering (WSCE)*, 64–68. https://doi.org/10.1109/wsce51339.2020.9275581

Mijwil, M. M., Salem, I. E., & Ismaeel, M. M. (2023). The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review. *Iraqi Journal for Computer Science and Mathematics*, *4*(1), 87–101. https://doi.org/10.52866/ijcsm.2023.01.01.008

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). *2015 Military Communications and Information Systems Conference (MilCIS)*, 1–6. https://doi.org/10.1109/milcis.2015.7348942

Muñoz, D. C., & Valiente, A. del-Corte. (2023). A Novel Botnet Attack Detection for IoT Networks Based on Communication Graphs. *Cybersecurity*, *6*(1), 33. https://doi.org/10.1186/s42400-023-00169-6

Priyatharsini, G. S., Babu, A. J., Kiran, M. G., Sathish Kumar, P. J., Nelson Kennedy Babu, C., & Ali, A. (2022). Self Secured Model for Cloud Based IOT Systems. *Measurement: Sensors*, *24*, 100490. https://doi.org/10.1016/j.measen.2022.100490

Ragunthar, T., Ashok, P., Gopinath, N., & Subashini, M. (2021). A Strong Reinforcement Parallel Implementation of K-Means Algorithm using Message Passing Interface. *Materials Today: Proceedings*, *46*, 3799–3802. https://doi.org/10.1016/j.matpr.2021.02.032

Savita, D., & Taran, S. B. (2023). Ensemble Approach for DDoS Attack Detection in Cloud Computing Using Random Forest and GWO. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(11), 347–357. https://doi.org/10.17762/ijritcc.v11i11.9653

Saxena, N., & Nigam, A. (2022). Performance Evaluation of a Variational Quantum Classifier. *2022 IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 1–5. https://doi.org/10.1109/upcon56432.2022.9986421

Shang, Y. (2024). Prevention and Detection of DDOS Attack in Virtual Cloud Computing Environment Using Naive Bayes Algorithm of Machine Learning. *Measurement: Sensors*, *31*, 100991. https://doi.org/10.1016/j.measen.2023.100991

Schuld, M., Sinayskiy, I., & Petruccione, F. (2015). An Introduction to Quantum Machine Learning. *Contemporary Physics*, *56*(2), 172–185. https://doi.org/10.1080/00107514.2014.964942

Sheoran, S. K., & Yadav, V. (2024). Comparative Analysis of Classification Efficiency of Quantum Machine Learning Algorithms. *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, 1818–1823. https://doi.org/10.1109/ic2pct60090.2024.10486763

Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research. *Applied Sciences*, *11*(12), 5713. https://doi.org/10.3390/app11125713