# Fine-tuned Variational Quantum Classifiers for Cyber Attacks Detection based on Parameterized Quantum Circuits and Optimizers

Md Abdur Rahman
*Department of Intelligent Systems and Robotics*
*University of West Florida*
*Pensacola, FL, USA*
*mr252@students.uwf.edu*

Emily Miller
*Department of Computer Science*
*University of West Florida*
*Pensacola, FL, USA*
*eam61@students.uwf.edu*

Bogdan Timofti
*Department of Computer Science*
*University of West Florida*
*Pensacola, FL, USA*
*bt56@students.uwf.edu*

Hossain Shahriar
*Center for Cybersecurity*
*University of West Florida*
*Pensacola, FL, USA*
*hshahriar@uwf.edu*

Mohammad Masum
*Department of Applied Data Science*
*San Jose State University*
*San Jose, CA, USA*
*mohammad.masum@sjsu.edu*

Fan Wu
*Department of Computer Science*
*Tuskegee University*
*Tuskegee, AL, USA*
*fwu@tuskegee.edu*

***Abstract*—Recent investigations into Quantum Machine Learning (QML) techniques have unveiled methodologies that accelerate training in established machine learning models to provide an alternative for capturing complex patterns. This study focuses on implementing a practical QML Algorithm, Variational Quantum Classification (VQC) for cybersecurity dataset so that detecting anomalies can be improved and faster by reducing number of attributes $\log_2 M$ while training the model using Qiskit. Also, we study quantum algorithms to understand how it impacts on cyber datasets to detect anomalies in a improved way as it follows logarithms in the dimensionality reduction of quantum states which opens new horizons to quantum big data applications. Most importantly, we aim to also investigate the impact of various parameterized quantum circuits on VQC using quantum data as quantum states encoded by the cyber security dataset, NSL-KDD. In this research, we train VQC with various structures and parameters of quantum circuits as well as optimizers to adjust parameters of quantum circuits (ansatz) to minimize the objective function values so as to improve accuracy of the model in which quantum circuit, EfficientSU2, along with optimizer, COBYLA, outperforms the accuracy than other circuits and optimizers which shows great potential for improving cybersecurity systems. The research could effectively bridge in the gap between theory and implementation based quantum machine learning on cybersecurity systems.**

***Index Terms*—quantum machine learning, variational quantum classifier, parameterized quantum circuit, optimizer**

## I. Introduction

Quantum computing (QC) has driven significant progress in diverse fields as it shows impressive potential with exponential acceleration to address traditionally unsolvable problems with improved effectiveness and velocity. In other words, quantum computing has caught huge attention in recent years, because it can solve complex problems using special features like superposition and entanglement, which regular computers can not handle [1-6]. Quantum devices are being made to do these jobs much faster than normal computers. For example, they can search through a bunch of data super fast, like finding something in a messy pile, but even quicker [7].

When quantum computing and machine learning come together, it forms a new area called quantum machine learning (QML). Scientists have created quantum versions of popular machine learning models, such as quantum support vector machines, quantum reinforcement learning, and quantum variational autoencoders [8-11].

Meanwhile, research papers on machine learning and network security are looking at different ways to spot and stop Distributed Denial of Service (DDoS) attacks, which make networks crash. They are also working on making sure important data gets sent quickly and smoothly over industrial wireless networks. They are focusing on making the rules for how devices communicate really good to support important jobs in factories and other industrial places [12-13]. Hossain et al., (2012) underscore the importance of addressing program security vulnerabilities, highlighting various approaches and challenges [14]. Additionally, Hossain et al., (2014) emphasize the significance of effectively detecting vulnerable and malicious browser extensions, contributing to enhanced computer security measures [15].

Also, one work used difefernt machine learning approaches for the prediction of risk factor for elements of cryptocurrency market [16]. Moreover, Rahman used K-means clustering to make the dataset as clustered input to the Random Forest classifier for big data distributed systems for detecting in a high accuracy using big data processing because it was introduced to use computing capabilities across clusters of machines in the case of huge amount of data [17]. Therefore, they focused to enhance this work to address the imbalanced dataset problem using GANs by generating dataset for specific


DOI 10.1109/COMPSAC61105.2024.00144

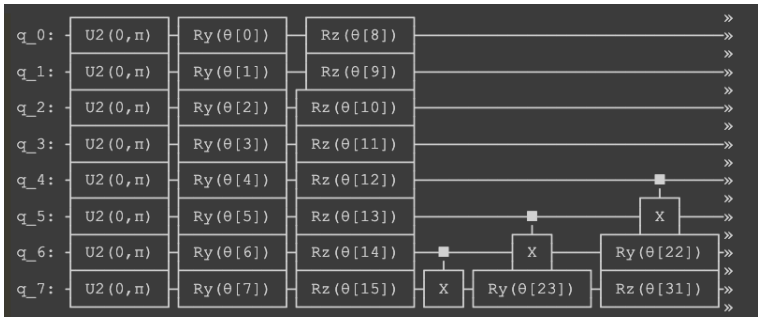



Fig. 1. A schematic representation of a typical quantum circuit, illustrating the flow of quantum information within a quantum computing system.

classes so that the imbalanced dataset issues can be resolved for IDS in distributed computing using PySpark.

Even though there is been significant progress in quantum computing, it is still facing numerous problems, especially in the NISQ stage [18]. Right now, quantum computers only use a few qubits because the hardware is not good enough yet. This means we can not make a quantum computer that doesn't make mistakes. However, the emergence of VQA [19] is proving helpful in tackling current quantum tasks. With VQA, we construct different quantum setups and methodologies to improve the detection of anomalies using NSL-KDD dataset. Some common VQA include VQE, which aids in finding molecule energies, dynamical quantum simulation, and QAOA [20-23], as well as QML [24-26]. However, VQA still encounters numerous challenges. Presently, it operates within a simulated quantum environment created by regular computers. This simulated environment introduces a significant amount of errors, especially in NISQ phase quantum machines, where qubits and quantum gates frequently make mistakes [25-26]. Additionally, due to the limited number of qubits, we can not develop very complex algorithms, which impacts their effectiveness.

Quantum computing faces challenges in handling cybersecurity datasets NSL-KDD due to limited resources, algorithmic complexity, and security implications [27-28]. Current quantum devices suffer from high error rates and noise, impacting data accuracy [29]. Moreover, the potential vulnerability of traditional cryptographic protocols heightens security concerns [30]. Developing quantum-safe cryptography is crucial [31] amidst the evolving landscape of cybersecurity threats [32] and quantum technologies [33].

In this work, Section 2 discusses the basic background of Variation Quantum Classifier (VQC) in quantum machine learning (QML). Section 3 and Section 4 presents the dataset and methods respectively. Section 5 describes results and discussion and finally, we conclude with summary of our works.

## II. Variational Quantum Classifier (VQC)

The Variation Quantum Classifier (VQC) is a novel approach in realm of quantum computing that has garnered attention for potential applications in various domains, including cybersecurity. When it comes to detecting intrusions in cyber security datasets like NSL-KDD, VQC presents a promising arena with worth exploring. An overview of VQC and its potential in intrusion detection is described below:

### A. Quantum Computing and VQC

The Variation Quantum Classifier (VQC) is an innovative application of quantum computing, which represents a groundbreaking shift in computational paradigms by harnessing the fundamental principles of quantum mechanics. Unlike conventional classical computers that depend on binary bits, which can only exist as either 0 or 1, quantum computers utilize quantum bits, commonly referred to as qubits. The unique property of qubits is their ability to exist in a superposition of states, allowing them to represent multiple values simultaneously. For each quantum states as data points, the parameters are assigned to the feature map and the variational circuit shown in Fig. 1.

### B. Features of VQC

- Variational Circuits: VQC uses special quantum circuits called variational quantum circuits. These circuits have settings that can be adjusted to do certain jobs better.
- Quantum-Classical Hybrid: VQC combines quantum and classical components, where classical algorithms are used to optimize the quantum circuit's parameters.
- Feature Mapping: In the context of intrusion detection, VQC can be used to map input data (such as network traffic logs) into a quantum state, effectively encoding features in a quantum format.

### C. Framework of VQC algorithm

Fig. 2 shows the framework of VQC algorithm which illustrates to compute cost function with various features, quantum circuits and optimizers. It combines quantum circuitry and neural networks to create a robust classifier. By employing variational techniques, it interprets measured bitstrings as classification outputs. Labels can be provided for attacks as a one-dimensional array. The VQC also supports one-hot encoded labels, transforming them into binary representation. Its training process consistently utilizes one-hot labels, ensuring effective and accurate learning. This flexibility in label formats

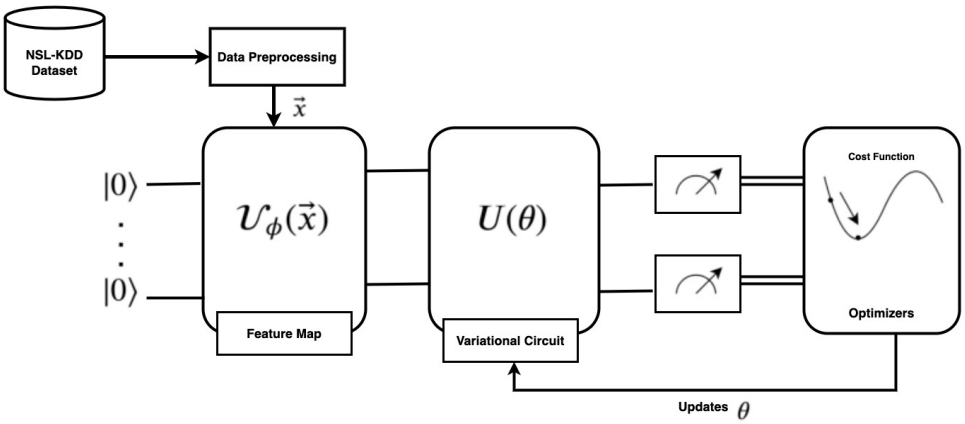



Fig. 2. A framework of VQC algorithm to compute cost function with various features, quantum circuits and optimizers.

enhances the versatility and practicality of the VQC algorithm, making it suitable for various classification tasks.

### D. Potential Benefits for Intrusion Detection

- Enhanced Data Representation: VQC's ability to transform data into quantum states may capture intricate patterns and relationships in cyber threats that are challenging to discern with classical techniques.
- Quantum Parallelism: Quantum computers can potentially explore multiple data patterns simultaneously, which might speed up the detection process.
- Complex Pattern Detection: Cyber threats often involve complex, evolving patterns. VQC's capacity to handle high-dimensional data could improve the detection of sophisticated intrusions.

### E. Challenges and Considerations:

- Quantum Hardware: As of my last knowledge update in September 2021, practical quantum hardware is still in its infancy and may not be readily available for widespread use.
- Algorithm Development: Developing quantum algorithms, including VQC, requires expertise in both quantum physics and computer science, making it a specialized field.

## III. Dataset

Within the NSL-KDD dataset, the training subset comprises 125,973 records, however there are 22,544 records in the test subset. For this work, we extracted the features for this supervised model: protocol_type, service, src_bytes, dst_bytes, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, and dst_host_same_src_port_rate. The attribute 'attack' is chosen for target variables. It has 4 four types of attacks as well as nornal value. We study to understtod how protocol type connects the attack types. These attacks fall into four primary categories, as described below:

- Denial-of-Service (DoS): This category includes attacks like syn flood, aiming to overwhelm and disrupt services, making them inaccessible to legitimate users.
- Unauthorized Remote Access (R2L): Attacks in this category involve unauthorized access attempts from remote machines, often employing techniques like password guessing to breach security barriers.
- Unauthorized Local Access (U2R): This category entails attacks seeking unauthorized access to local superuser (root) privileges, using techniques like "buffer overflow" attacks to exploit vulnerabilities and elevate privileges.
- Probing: Attacks in this category involve surveillance and probing activities, such as port scanning, where attackers try to gather information about potential system vulnerabilities.

The categorization and visualization of these attacks provide valuable insights for researchers and cybersecurity experts, enabling the development of robust defense mechanisms against various intrusion attempts. Leveraging these datasets and their analyses contributes significantly to enhancing our collective knowledge and understanding of network security, ultimately fortifying digital infrastructures against potential cyber threats.

## IV. Methods

In our method, we initially employ the ZZFeatureMap technique for encoding data within the classification circuit. A dedicated function is developed to encode the extracted features of NSL-KDD dataset into the feature map by setting variational parameters within the quantum circuit. It is crucial to ensure that the correct parameters within the circuit are associated with the appropriate quantities. Subsequently, after training the Variational Quantum Classifier (VQC) with both data and parameters, the parameters are set within both the feature map and the variational circuit.

To classify our data, we devise a function that takes in data and parameters. For each data point in the dataset, the parameters are assigned to the feature map and the variational circuit. Once the quantum circuit is stored, the system undergoes a transformation. This crucial step enables the execution of circuits. After running these circuits, the system computes probabilities based on both the bit string and the assigned class labels for each circuit, providing valuable insights into the outcomes. During the training phase, the objective function

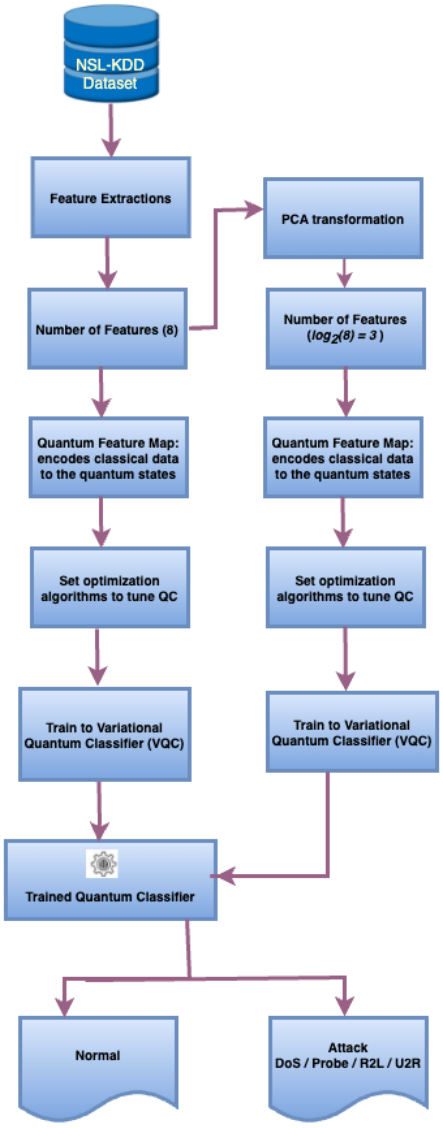



Fig. 3. The flowchart to illustrate steps to train the VQC with various features.

value serves as the cost function or loss function. Classical optimizers, specifically COBYLA, and AQSD are utilized to initialize quantum circuit parameters for reproducibility, optimizing our cost function across 100 training epochs. This optimization process adjusts the variational circuit parameters based on the output of the cost function.

The performance of the trained VQC classifier is evaluated using a testing dataset. It is expected that the training optimization process may require significant time, potentially leading to convergence to a local minimum rather than a global minimum. The whole steps are described in the flowchart (Fig. 3).

## V. Results and Discussions

We implemented this work in the Google Colab environment using the Qiskit tool (IBM) since we lack access to quantum computers for quantum computing in our laboratory, thus encountering significant challenges. However, we can still explore quantum algorithms and concepts through simulation on classical computers. While these simulations may not provide the same speed-up as actual quantum computers, they allow us to understand quantum principles and develop algorithms that could be used in the future when quantum computing technology becomes more accessible. This approach enables us to stay engaged with quantum computing research and prepares us for advancements in the field.

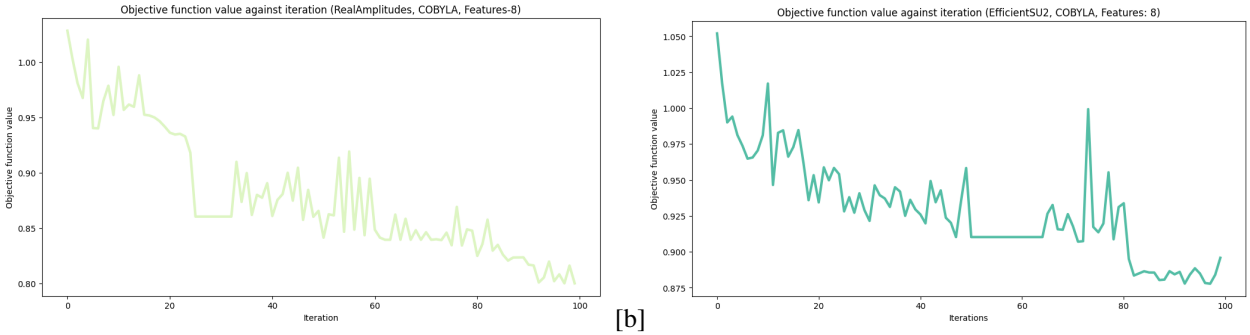
Firstly, we extracted 8 important features of NSL-KDD datasets to improve the intrusion detection systems using VQC. Through this implementations, we have made plots for the objective function values for quantum circuits, optimizers, and various features so that we can measures how well the model predicts anomalies. VQC adjusts its parameters by making this function as small as possible to improve accuracy. It is used like a scorecard for evaluating how good the model is at classifying anomalies in training and testing observations.

In fact, the objective function value reflects the alignment between predicted and actual labels which guides model optimization. While setting up EfficientSU2 and COBYLA with 3 features after applying PCA, objective function values minimization correlates with heightened accuracy compared to configurations with 8 features of dataset. Moreover, this value tends to be lower in EfficientSU2 and COBYLA setups than in RealAmplitudes and COBYLA configurations. This clearly indicates that EfficientSU2 has superior performance in accurately classifying attacks from normal observations.

Moreover, EfficientSU2 with reduced features exhibits superior performance than RealAmplitudes due to its more flexible representation of quantum states as it employs a combination of single-qubit rotations and entangling gates which allow it to more efficiently explore complex quantum feature spaces. This flexibility enables EfficientSU2 to capture intricate attack patterns from normal data instances effectively. Consequently, it results in enhanced classification accuracy. However, RealAmplitudes tends to converge faster and it is also observed that RealAmplitudes is required little less time to train VQC than EfficientSU2.

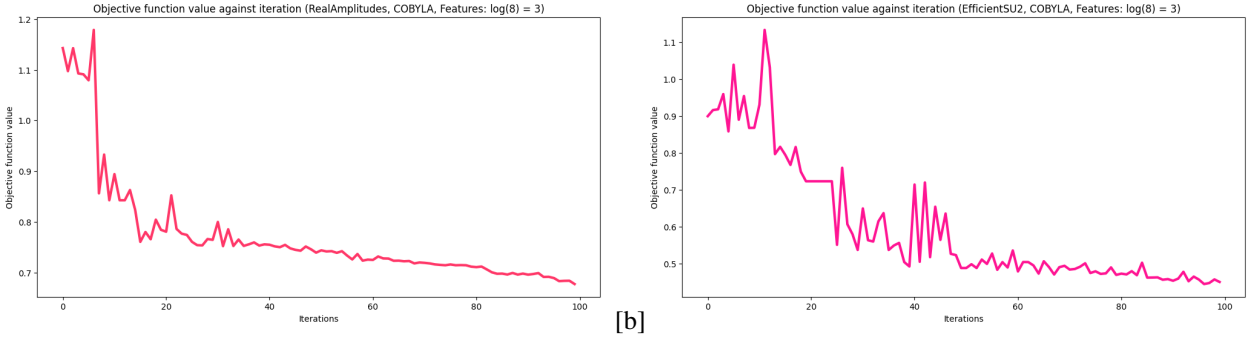
In Variational Quantum Classification (VQC), the objective function reflects the alignment between predicted and actual labels, guiding model optimization. Particularly in setups utilizing EfficientSU2 and COBYLA with 3 attributes, objective function minimization correlates with heightened accuracy compared to configurations with 8 attributes. Moreover, this value tends to be lower in EfficientSU2 and COBYLA setups than in RealAmplitudes and COBYLA configurations, indicating superior performance in accurately classifying input data points.

The Objective function value exhibited minimal fluctuations and reached a stable state after only 50 and 60 iterations for EfficientSU2 and RealAmplitudes respectively. This suggests that the model's performance, as measured by the objective function, converges to a consistent value relatively quickly when using this subset of features. Fig. 5 corresponds to the utilization of 3 features which have a high degree of stability.




[a] [b]

Fig. 4. Objective function value generated in VQC using 8 features, various parameterized quantum circuits and COBYLA: (a) RealAmplitudes (b) EfficientSU2




[a] [b]

Fig. 5. Objective function value generated in VQC using 3 features, various parameterized quantum circuits and COBYLA: (a) RealAmplitudes (b) EfficientSU2

Conversely, Fig. 4 employed 8 features and observed a substantially different patterns. The Objective function value exhibited significant fluctuations over the course of the iterations. Unlike the 3 features scenario, stability was not achieved within the same timeframe, indicating that the model's performance remained more volatile when utilizing this larger set of features.

The TABLE I presents a comprehensive comparison between different Variational Quantum Classifier (VQC) setups based on various Quantum Circuits and Optimizers alongside Training Time. For 8 features, RealAmplitudes with COBYLA optimizer boasts the highest test score of 0.89 and train score of 0.87, accompanied by a comparatively low training time of 1316 seconds. Conversely, EfficientSU2, under the same COBYLA optimizer, exhibits a slightly lower test score and train score which are 0.80 and 0.77 respectively. It required training time 1506 seconds.

On the other hand, when utilizing the AQSD optimizer, training Variational Quantum Classifiers (VQC) suffer significant time costs and yields lower efficiency. For 8 features, AQSD required a lengthy training time of 9047 seconds, resulting in lower accuracy (0.49 in testing, 0.45 in training) for RealAmplitudes. Similarly, EfficientSU2 under AQSD exhibited a prolonged training duration of 9738 seconds, accompanied by reduced accuracy (0.46 in testing, 0.42 in training).

When reducing attributes from 8 to 3 using Principal Component Analysis (PCA), VQC demonstrated remarkable performance enhancements, particularly with EfficientSU2 and COBYLA. Compared to RealAmplitudes under the same optimizer configuration, EfficientSU2 achieved superior accuracy, scoring 0.90 in testing and 0.93 in training. Moreover, it trained efficiently in only 356 seconds. Conversely, RealAmplitudes attained lower accuracy scores of 0.81 in testing and 0.82 in training, requiring less time 275 seconds for convergence. These datapoints proves the potential of EfficientSU2 and COBYLA in exploiting reduced attribute sets for optimal VQC training, and showing their efficacy in quantum classification tasks. Moreover, these results provides the significance of various quantum circuits and optimizers selections for improved classifier performance to detect anomalies.

TABLE I
TEST AND TRAINING SCORES FOR OUR VQC IMPLEMENTATIONS

| QCircuit | Features | Optimizers | Test | Train | Train time |
|---|---|---|---|---|---|
| RealAmplitudes | 8 | AQSD | 0.49 | 0.45 | 9047 |
| EfficientSU2 | 8 | AQSD | 0.46 | 0.42 | 9738 |
| RealAmplitudes | 8 | COBYLA | 0.89 | 0.87 | 1316 |
| EfficientSU2 | 8 | COBYLA | 0.79 | 0.81 | 1441 |
| RealAmplitudes | 3 | COBYLA | 0.81 | 0.82 | 275 |
| EfficientSU2 | 3 | COBYLA | 0.90 | 0.93 | 356 |

In TABLE II, our VQC with NSL-KDD dataset outperforms existing work with IRIS dataset with a remarkable testing accuracy of 90% compared to 76.76% and 89.25% achieved by VQC and Classical SVM, respectively. Additionally, our VQC exhibits superior training accuracy of 93% surpassing 82.10%

TABLE II
COMPARISON OUR VQC WITH EXISTING WORK

| | Dataset | Test(%) | Train(%) |
|---|---|---|---|
| Classical SVM(Saxena et al.,22)[34] | IRIS | 89.25 | 90.00 |
| VQC (Saxena et al.,22)[34] | IRIS | 76.76 | 82.10 |
| **Our VQC** | **NSL-KDD** | **90.00** | **93.00** |

and 90% achieved by VQC and Classical SVM, respectively.

## VI. CONCLUSION

In conclusion, we applied various parameterized quantum circuits and optimizers for training and testing Variational Quantum Classifier (VQC) which demonstrates exceptional performance in cyber attack detection after fine tuning and it is proved when it is evaluated against existing works. With a testing accuracy of 90%, our VQC outperforms existing VQC and Classical SVM models, achieving 76.76% and 89.25% respectively on the IRIS dataset. Furthermore, our VQC showcases superior training accuracy, reaching 93%, surpassing the performance of both VQC and Classical SVM models on the IRIS dataset. This underscores the efficacy of our approach in enhancing cyber attack detection capabilities.

## ACKNOWLEDGMENT

The work is supported by the National Science Foundation under NSF Award 1946442, 2433800, and 2100134. Any opinions, findings, recommendations, expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

## REFERENCES

[1] Rahman, Md Abdur, Hossain Shahriar, Victor Clincy, Md Faruque Hossain, and Muhammad Rahman. "A Quantum Generative Adversarial Network-based Intrusion Detection System." In 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1810-1815. IEEE, 2023.

[2] J. Preskill, Quantum computing in the nisq era and beyond, Quantum 2 (2018) 79.

[3] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, S. Lloyd, Quantum machine learning, Nature 549 (7671) (2017) 195–202.

[4] Upama, Paramita Basak, Md Jobair Hossain Faruk, Mohammad Nazim, Mohammad Masum, Hossain Shahriar, Gias Uddin, Shabir Barzanjeh, Sheikh Iqbal Ahamed, and Akond Rahman. "Evolution of quantum computing: A systematic survey on the use of quantum computing tools." In 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 520-529. IEEE, 2022.

[5] Preskill, J. Quantum Computing in the NISQ era and beyond. Quantum 2018, 2, 79. [CrossRef]

[6] Harrow, A.W.; Montanaro, A. Quantum computational supremacy. Nature 2017, 549, 203–209. [CrossRef]

[7] Biamonte, J.; Wittek, P.; Pancotti, N.; Rebentrost, P.; Wiebe, N.; Lloyd, S. Quantum machine learning. Nature 2017, 549, 195–202. [CrossRef]

[8] Rebentrost, P.; Mohseni, M.; Lloyd, S. Quantum Support Vector Machine for Big Data Classification. Phys. Rev. Lett. 2014, 113, 130503. [CrossRef]

[9] Dong, D.; Chen, C.; Li, H.; Tarn, T.J. Quantum Reinforcement Learning. IEEE Trans. Syst. Man Cybern. Part B 2008, 38, 1207–1220. [CrossRef]

[10] Khoshaman, A.; Vinci, W.; Denis, B.; Andriyash, E.; Sadeghi, H.; Amin, M.H. Quantum variational autoencoder. Quantum Sci. Technol. 2018, 4, 14001. [CrossRef]

[11] Masum, Mohammad, Mohammad Nazim, Md Jobair Hossain Faruk, Hossain Shahriar, Maria Valero, Md Abdullah Hafiz Khan, Gias Uddin et al. "Quantum Machine Learning for Software Supply Chain Attacks: How Far Can We Go?." In 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 530-538. IEEE, 2022.

[12] Rahman, Md Abdur. "Detection of distributed denial of service attacks based on machine learning algorithms." International Journal of Smart Home 14, no. 2 (2020): 15-24.

[13] Azad, Md Abul Kalam, Amina Khatun, and Md Abdur Rahman. "A slotted-sense streaming MAC for real-time multimedia data transmission in industrial wireless sensor networks." International Journal of Advanced Engineering Research and Science 4, no. 3 (2017).

[14] Shahriar, Hossain, and Mohammad Zulkernine. "Mitigating program secu- rity vulnerabilities: Approaches and challenges." ACM Computing Surveys (CSUR) 44, no. 3 (2012): 1-46.

[15] Shahriar, Hossain, Komminist Weldemariam, Mohammad Zulkernine, and Thibaud Lutellier. "Effective detection of vulnerable and malicious browser extensions." Computers Security 47 (2014): 66-84.

[16] Akter, Shapna., Rahman, Md. Abdur., Shahriar, Hossain., Rahman, Muhammad. (2023, December). Early Prediction of Cryptocurrency Price Decline: A Deep Learning Approach. 26th International Conference on Computer and Information Technology (ICCIT), Cox's Bazar, Bangladesh (accepted presented at Dec 14, 2023).

[17] Rahman, Md Abdur, and Shahriar, Hossain. (2023, December). "Clustering Enabled Robust Intrusion Detection System for Big Data using Hadoop-PySpark", 2023 IEEE 20th Interna- tional Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET), Boca Raton, Florida, USA.

[18] J. Preskill, Quantum computing in the nisq era and beyond, Quantum 2 (2018) 79.

[19] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, et al., Variational quantum algorithms, Nature Reviews Physics 3 (9) (2021) 625–644.

[20] D. A. Fedorov, B. Peng, N. Govind, Y. Alexeev, Vqe method: A short survey and recent developments, Materials Theory 6 (1) (2022) 1–21.

[21] H. Wang, Y. Ding, J. Gu, Y. Lin, D. Z. Pan, F. T. Chong, S. Han, Quantumnas: Noise-adaptive search for robust quantum circuits, in: 2022 IEEE International Symposium on High-Performance Computer Architecture (HPCA), IEEE, 2022, pp. 692–708.

[22] O. R. Meitei, B. T. Gard, G. S. Barron, D. P. Pappas, S. E. Economou, E. Barnes, N. J. Mayhall, Gate-free state preparation for fast variational quantum eigensolver simulations, npj Quantum Information 7 (1) (2021) 1–11.

[23] X.-Y. Guo, C. Yang, Y. Zeng, Y. Peng, H.-K. Li, H. Deng, Y.-R. Jin, S. Chen, D. Zheng, H. Fan, Observation of a dynamical quantum phase transition by a superconducting qubit simulation, Physical Review Applied 11 (4) (2019) 044080.

[24] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, S. Lloyd, Quantum machine learning, Nature 549 (7671) (2017) 195–202.

[25] W. Jiang, J. Xiong, Y. Shi, When machine learning meets quantum computers: A case study, in: 2021 26th Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE, 2021, pp. 593–598.

[26] Z. Wang, Z. Liang, S. Zhou, C. Ding, Y. Shi, W. Jiang, Exploration of quantum neural architecture by mixing quantum neuron designs, in: 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD), IEEE, 2021, pp. 1–7.

[27] Alom, M. Z., et al. (2019). Quantum Computing: A Survey for Healthcare. arXiv preprint arXiv:1906.11467.

[28] Sharma, S., et al. (2020). Quantum Computing: Vision and Innovations. IEEE Access, 8, 115415-115435.

[29] Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79.

[30] Chen, T., et al. (2017). Quantum cryptography: Public key distribution and coin flipping. Reviews of Modern Physics, 89(4), 041001.

[31] Apon, A. W., et al. (2021). Post-quantum cryptography and its recent advancements: A survey. Digital Communications and Networks, 7(3), 261-272.

[32] Khrais, I. A., et al. (2020). Cybersecurity Threats, Challenges, and Future Perspectives: A Survey. Journal of King Saud University-Computer and Information Sciences.

[33] Jones, N. C., et al. (2021). Quantum Computing: A Survey of Industrial Applications. Frontiers in Physics, 8, 750.

[34] N. Saxena and A. Nigam, "Performance Evaluation of a Variational Quantum Classifier," 2022 IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Prayagraj, India, 2022, pp. 1-5, doi: 10.1109/UPCON56432.2022.9986421.