


Article

Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid

Dhaou Said 

Department of Electrical and Computer Engineering, University of Sherbrooke, Sherbrooke, QC J1K 2R1, Canada; dhaou.said@usherbrooke.ca

Abstract: Machine learning (ML) is efficiently disrupting and modernizing cities in terms of service quality for mobility, security, robotics, healthcare, electricity, finance, etc. Despite their undeniable success, ML algorithms need crucial computational efforts with high-speed computing hardware to deal with model complexity and commitments to obtain efficient, reliable, and resilient solutions. Quantum computing (QC) is presented as a strong candidate to help MLs reach their best performance especially for cybersecurity issues and digital defense. This paper presents quantum support vector machine (QSVM) model to detect distributed denial of service (DDoS) attacks on smart micro-grid (SMG). An evaluation of our approach against a real dataset of DDoS attack instances shows the effectiveness of our proposed model. Finally, conclusions and some open issues and challenges of the fitting of ML with QC are presented.

Keywords: quantum computing; quantum support vector machine; machine learning; digital defense; cybersecurity; support vector machine; distributed denial of service (DDoS) attacks



Citation: Said, D. Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid. *Energies* **2023**, *16*, 3572. <https://doi.org/10.3390/en16083572>

Academic Editors: Ahmed Abu-Siada and Yun Liu

Received: 14 March 2023

Revised: 6 April 2023

Accepted: 19 April 2023

Published: 20 April 2023



Copyright: © 2023 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

As it massively based on Information, Communication, and Technologies (ICT)s such as Artificial Intelligence, Blockchain, Game Theoretic, Internet-of-Things schemes, etc., the Smart Micro-Grid (SMG) [1,2] is an advanced model in Modern Power Grid to ensure fast, resilient, and reliable interaction between all elements and provide reliable electricity service. SMG is expected to be flexible and smart enough to detect, identify, and react in emergencies such as electricity service interruptions resulting from natural disasters, terrorist attacks, cyber attacks, etc. One of the most disruptive innovations of AI is machine learning (ML), which allows the computer system to learn an intended input-output behavior to perform predictions and recommendations in SMG. This is performed by analyzing and processing the given historical data rather than following explicit programming instructions. To improve the learning system capabilities, for example, in terms of accuracy and precision, mathematical models based extensively on linear algebra theory and matrix operations, require not only large amounts of historical data, but also more flexibility and adjustments for their parameters. For example, the artificial neural network (ANN) and deep learning (DL) schemes need, in some cases, billions of weights to be used in each layer to make the learning system more reliable.

Moreover, in classical cryptography, the security is based on computational complexity assumptions which make it severely challenged with the rapid development of smart city applications. For example, the identity and privacy prediction for avatars is highly complicated when switching between real and virtual spaces in the metaverse application for a modern power grid. Thus, the success of SMG, which relies heavily on ML models, depends on the available computation capabilities such as computing hardware schemes.

In parallel, quantum computing (QC) is presented as a strong candidate to help reach the best performance of ML. QC is expected to disrupt many technological systems. In that

given context, it is proved that QC can solve several complex issues much faster than digital computing. Therefore, solving ML problems using quantum computers is a very promising solution to accelerate progress which can lead to innovative SMG products that are able to disrupt the economy and society. However, these quantum benefits come with several challenges and risks, and so more effort and attention have to be considered, especially when combining quantum-AI with IoT and blockchain in cybersecurity, as well as when dealing with ethical problems associated with sensitive and private data.

Quantum security (QS) and quantum cryptography is a subset of QC that aims to speed up in real time, computational especially with a very large amount of data processing. Thus, QS is expected to create accurate encryption codes more quickly and detect any eavesdropper during the encryption exchange phase.

As presented in Table 1, QC and ML are both challenging developers and researchers in data sciences with their capabilities.

Table 1. ML and QC capabilities which challenge data science developers and researchers.

	ML	QC
Defender	Detect possible risks and potential attacks; Fighting security vulnerabilities or weaknesses. Analyze collected data to manage threat notifications and vulnerabilities.	Fast detection of attacks and threads. Create accurate encryption codes quickly.
Attacker, Threat actors	Can be used by cyber-criminals to create crucial cyber-attacks.	Can be used to break encrypted crypto codes faster.

First, ML can be used both by defenders and cyber-criminals. It is proven [3,4] that non-criminals can apply ML to efficiently optimize processes and rules (data analysis, prediction, etc.), for example, to enforce access control, authentication, and attack detection. In analogue, criminals can create intensive and crucial cybersecurity risks via ML, leading to vast economic and social impacts on governments, companies, and communities.

Second, the same downside exists with QS/QC. Despite the undeniable security that comes with their capabilities for fast threat detection and quick vulnerability management based on the principles of quantum mechanics, QS skills can be used to break hard encryption and crypto codes faster, aiming to lose system control.

1.1. Literature View

Classical ML technics are considered to detect DDoS in several research works. For example, a recent scientific paper [5] proposes a framework based on feature and model selection (FAMS) used for detecting DDoS attacks when identifying the features and models with a high generalization capability, high prediction accuracy, and short prediction time. In the same context, in [6], a complete systematic approach for the detection of the DDoS attack is proposed. It uses ML approaches such as random forest and XGBoost classification algorithms to detect DDoS attack types of classification and prediction. In addition, reference [7] develops an approach that provides protection against the amplification of DDoS attacks in smart grid. Despite the performance shown, this approach fails to detect encrypted DDoS attacks. Reference [8] proves the effectiveness of several ML methods such as tree, random forest, quadratic discriminant analysis, support vector machine, naïve Bayes, and extreme gradient boosting to detect DDoS on smart grids for specific conditions and assumptions. A recent work [9] proposes iCAD—an information-centric architecture scheme—to mitigate DoS/DDoS attacks in smart grid. A hybrid detection framework which is able to recognize potentially malicious activities (DDoS, FDI, etc.) occurring in the cyber layer of a typical power grid is developed [10].

On the other hand, quantum technologies are a global field with a vast scientific literature. Modern power grid researchers started exploring capabilities of quantum security algorithms to build secure power grid networks in terms of the reliability and resilience of service restoration after extreme environmental events, cyber-attacks, outages, etc. A

study in [11], which reviews the current literature research of the QC in smart grid, explores their early quantum experiences in optimization, simulations, communications, and ML. Moreover, as the QC era requires talented and skilled people, a web-based tool is introduced in [12] to simplify the application of QSVM onto different real-world classification problems for all researchers derived from various scientific backgrounds with and without physics skills.

From this literature review, we note that the connection between QC and SMG as part of a power grid requires not only talented and skilled people, but also efforts to establish standards for flexible quantum programming tools and environments, quantum hardware, software, and algorithms.

1.2. R&D in Quantum Computing

Recently, QC is investigated to increase computing capacities so as to compute ultra-fast real-time decisions and address cybersecurity problems that are intractable on any classical computer as well as super-calculators. Thus, QC is attracting the attention of several industries, businesses, and researchers. Many countries are well-known as leaders in this domain, such as the United States, which focuses on quantum computing innovations, Europe, which concentrates efforts on quantum mechanics, and China, which targets the quantum communication and cryptography [13–20]. Several universities are deeply working in quantum and allocating resources to accelerate research in QC, among which is Harvard University, with a focus on advancing the science and engineering of quantum systems and their applications. An alliance with Amazon’s AWS is stated to build quantum networks.

From an industrial point of view, today, there are several QC companies worldwide. The development of QC hardware is mainly based on gate-based and annealing approaches. First, the gate model QCs are the QC circuit schemes. They present the problem in the form of quantum gate sequences to simplify operations and measurement algorithms.

Second, quantum annealing is a QC method based on specific properties of quantum physics such as quantum tunneling, entanglement, and superposition. Its main objective is to deal with multiple solutions to select the optimal one. Table 2 presents some QML platforms.

Table 2. QML platforms.

QC Platform	Type	Realization	Qubits	Country
Xanadu, 2016 [13–20]	Gate-based	Photonic	24	Canada
D-Wave, 1999 [17,18]	Analog-based	Annealing	+2000	Canada
ALIBABA, 2017 [19]	Gate-based	Superconducting	11	China
IBM Q, 2016 [20]	Gate-based	Superconducting	127	U.S.

Indeed, Xanadu is a Canadian company making the first photonics-based QC platform based on light. Additionally, a software platform based on cloud service and application libraries such as Strawberry Fields is offered by Xanadu [13]. D-Wave is also a Canadian startup, having the status of an “analog quantum computer” as it can solve only a narrow range of the quantum annealing task. D-Wave declares its capacity to be about 2000 qubits [18]. A promising U.S. company is IBM Q which started in 2016, creating a quantum device up to 127 qubits and public access to quantum devices up to 32 qubits. IBM Q plans to launch the 1121-qubit Condor processor by 2023 and to achieve hundreds of thousands of qubits from 2026. Another important Chinese startup in this field is Alibaba, which is the first superconducting QC platform in China, starting with 11-qubit quantum computer and is expected to reach 144 qubits by 2022 and 1024 by 2025 [19].

This paper investigates the cyberattacks era and presents a QC-based support vector machine (QSVM) to detect distributed denial of service (DDoS) attacks.

Our contributions are as follows: (1) to date, this work is the first to focus on applying QSVM to tackle the cybersecurity challenge in SMG; (2) the potential of QC via QSVM in

DDoS attack detection is shown and highlighted; (3) we implement the classical SVM and QSVM using real dataset of DDoS attack instances, the open-source Qiskit software and Harrow–Hassidim–Lloyd (HHL) quantum algorithm; and (4) we prove the effectiveness of our proposed model in terms of the accuracy and consumption of computational resources.

The remainder of the paper is organized as follows. Section 2 details the SVM models. The QSVM model for cybersecurity in SMG application is developed and discussed in Section 3. Evaluations and comparative results of QSVM vs. classical SVM in DDoS detection are shown in Section 4. Section 5 draws conclusions.

2. SVM Model

The classical security system in SMG relies on mathematical models which cannot resist quantum attacks. In the following, we detail the the support vector machines (SVM) technique.

The SVM model is used for several applications such as to perform the prediction of energy production, consumption, cyber-attacks, fraud, and fault detection, and or renewable energy forecasting (solar, wind power, etc.) based on the supervised ML algorithm for classification, approximation, and regression. The mathematical formulation of the SVM optimization problem can be summarized as follows:

For a training dataset of input–output pairs $\{(x_1, y_1), \dots, (x_n, y_n)\} \in \mathbb{R}^d \times \mathbb{R}$, where \mathbb{R}^d is the space of the input features, x_i , with dimension d , the target variables $y_i \in \mathbb{R}$, and n is the training data size. The ML model can be formulated as shown in Equation (1):

$$f(x) = w^T \cdot \theta(x) + b \tag{1}$$

where f is the approximation function, w is the weight vector, b is the bias term, $\theta(x)$ is a nonlinear mapping function, and (\cdot) denotes the dot product in \mathbb{R}^d .

The optimization problem for SVM can be reduced to finding w by minimizing Equation (2):

$$\min \left\{ \frac{1}{2} w^2 + C \sum_{i=1}^n (\zeta_i + \zeta_i^*) \right\} \tag{2}$$

with constraints described by Equations (3)–(5):

$$y_i - w^T \cdot \theta - b \leq \varepsilon + \zeta_i \tag{3}$$

$$-y_i + w^T \cdot \theta + b \leq \varepsilon + \zeta_i^* \tag{4}$$

$$\zeta_i, \zeta_i^* \geq 0 \tag{5}$$

where ζ_i and ζ_i^* are slack variables, C is the penalization parameter of the error that is applied to control the trade-off between the regularization term and empirical risk, and ε is equivalent to the function approximation accuracy placed on the training data samples [21].

Lagrange multipliers α_i and α_i^* , are then introduced to solve the SVM minimization problem. Subject to the previous constraints, this leads to the following form:

$$f(x) = \sum_{i=1}^n (\alpha_i - \alpha_i^*) K(x, x_i) + b \tag{6}$$

where K denotes the kernel function which allows mapping the input data into a higher dimension space. Then the linear regression in the higher dimension space corresponds to nonlinear regression into the original space. The kernel function could be a linear function, or polynomial (Poly), or radial base function (RBF), or exponential radial basis function (ERBF), or customized kernel function.

The validation of the results is achieved using the R-squared error (RSE) computed according to the following formula:

$$R^2 = 1 - \frac{\sum_{i=1}^n (y_i \hat{y}_i)^2}{\sum_{i=1}^n (y_i \bar{y}_i)^2} \tag{7}$$

where $\hat{y}_i = f(x_i)$ are the predicted values and \bar{y}_i is the average value of y_i .

The soft margin SVM problem has a feasible solution even if the data are not linearly separable. The support vectors marked by black circles are all $x \in T$ that are either at the edge of the margin (such as in the hard margin case), inside the margin, or misclassified. Here, the regularization parameter is $C = 1$.

3. QSVM Model

There are two versions of QSVM that present quadratic and exponential speedup separately. The first one focuses on solving non-convex optimization problems by using Grover’s algorithm as a subroutine. The second one targets the analysis of the least-squares approximation of the SVM.

In this paper, we adopt the second QSVM version which is based on HHL algorithm which is able to provide an exponential speedup.

3.1. Background: Qubit and Quantum State

Similar to the classical bit information, the quantum bit information is noted as qubit and it is usually represented by Dirac notation:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8a}$$

and

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{8b}$$

Considering the superposition quantum criteria:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{9}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.

Equation (9) shows that $|\varphi\rangle$ can be in both state $|0\rangle$ and $|1\rangle$ with the probability of $|\alpha|^2$ and $|\beta|^2$, respectively.

3.2. Quantum Circuits: Gates

Quantum gate is the basic quantum circuit for qubits. It is based on building blocks circuits. Quantum gates have the same number of inputs and outputs. Quantum gates are in the form of operators (e.g., unitary matrices) which manipulate quantum state such as:

$$U|\varphi\rangle = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = |\gamma\rangle \tag{10}$$

For the basic quantum gates, there are the well-known elementary quantum gates such as: Pauli-X, Pauli-Y, Pauli-Z, Hadamard, Phase Shift [19]. The following are for Qubit gates:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : \text{it switches } |0\rangle \text{ by } |1\rangle \text{ and } |1\rangle \text{ by } |0\rangle ;$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} : \text{it switches } |0\rangle \text{ by } i|1\rangle \text{ and } |1\rangle \text{ by } -i|0\rangle ;$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : \text{it keeps } |0\rangle \text{ unchanged and switches } |1\rangle \text{ and } -|1\rangle ;$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} : \text{it creates a superposition of two states, it switches } |0\rangle \text{ by } \frac{|0\rangle+|1\rangle}{\sqrt{2}} \text{ and switches } |1\rangle \text{ by } \frac{|0\rangle-|1\rangle}{\sqrt{2}} ;$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\sigma} \end{pmatrix} : \text{it keeps the state } |0\rangle \text{ unchanged and switches } |1\rangle \text{ by } e^{-i\sigma}|1\rangle .$$

For the two-qubit gates configuration we have Controlled NOT (CNOT) and SWAP:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : \text{it is used for 2 qubits and performs the NOT operation when the control qubit is } |1\rangle . \text{ It causes switching between the last two rows of identity matrix;}$$

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} : \text{it causes switching from row 2 to row 3 in identity matrix.}$$

3.3. Measurement

The main piece to interpret quantum mechanics is measurement. We consider the practical physics measurement.

As presented in several references, quantum measurements are described by a collection M_m of measurement operators.

These operators measure the state space of the system. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\varphi\rangle$, then the probability that the result m occurs is given by:

$$\rho(m) = \langle \varphi | M_m^T M_m | \varphi \rangle \tag{11}$$

The measured state is:

$$\begin{cases} \frac{M_m|\varphi\rangle}{\sqrt{\langle \varphi | M_m^T M_m | \varphi \rangle}} \\ \text{where } \sum_m M_m^T M_m = I \end{cases} \tag{12}$$

Furthermore:

$$\sum_m \rho(m) = \sum_m \langle \varphi | M_m^T M_m | \varphi \rangle = 1 \tag{13}$$

For example, $M_0 = |0\rangle \langle 0|$ and $M_1 = |1\rangle \langle 1|$.

According the Equation (11), we have $M_0^T M_0 + M_1^T M_1 = I$.

Then, the probabilities of obtaining the measurement of 0 and 1 are, respectively:

$$\begin{aligned} \rho(0) &= \langle \varphi | M_0^T M_0 | \varphi \rangle = |\alpha|^2 \\ \rho(1) &= \langle \varphi | M_1^T M_1 | \varphi \rangle = |\beta|^2 \end{aligned} \tag{14}$$

and the corresponding state measurements are:

$$\begin{cases} \frac{M_0|\varphi\rangle}{\sqrt{\langle \varphi | M_0^T M_0 | \varphi \rangle}} = \frac{a}{|\alpha|} |0\rangle \\ \frac{M_1|\varphi\rangle}{\sqrt{\langle \varphi | M_1^T M_1 | \varphi \rangle}} = \frac{b}{|\beta|} |1\rangle \end{cases} \tag{15}$$

As presented in the before, the support vector machine (SVM) algorithm is a supervised machine learning algorithm used to find a hyperplane to distinguish two classes of data. Quantum support vector machines are an advanced version of the SVM. They employ quantum circuits to define the kernel function. QSVM algorithm is able to reduce the computation complexity and to speed up the execution exponential.

As detailed in reference [22] and based on Equations (1)–(6), the training vector is given by:

$$\omega = \sum_i^N \alpha_i x_i \tag{16}$$

Based on Equations (1)–(6), we employ the least-squares reformulation of SVM based on the quadratic programming technics, and we obtain:

$$F \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ I & K + \gamma^{-1} I_N \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ y \end{pmatrix} \tag{17}$$

where K is the linear kernel matrix.

We note that the approximation of the hyperplane-finding procedure of SVM is realized by solving the linear Equation (17). Now, we introduce the training data to obtain encoded data as:

$$|x_i\rangle = \frac{1}{|x_i|} \sum_i^M (x_i) |j\rangle \tag{18}$$

where the initial state is given by:

$$\frac{1}{\sqrt{M}} \sum_i^M |i\rangle \tag{19}$$

Thus, for the general state we obtain:

$$|s\rangle = \frac{1}{\sqrt{N_s}} \sum_i^M |x_i||i\rangle |x_i\rangle \tag{20}$$

Using HHL algorithm to solve the linear equations, we can obtain an optimized form of the hyperplane parameters as:

$$(b, a^T)^T = F^{-1}(0, y^T)^T \tag{21}$$

when the quantum register is initialized as:

$$|0, y\rangle = \frac{1}{\sqrt{N_{0,y}}} \left(|0\rangle + \sum_i^M y_i |i\rangle \right) \tag{22}$$

By performing the matrix inversion of F , the quantum state is transferred to:

$$|b, a\rangle = \frac{1}{\sqrt{N_{a,b}}} \left(b|0\rangle + \sum_i^M a_i |i\rangle \right) \tag{23}$$

With the optimized parameters b and a_i , the classification result then can be represented as:

$$y(x_0) = \text{sgn}\left(\sum_i^N \alpha_i(x_i \cdot x_0) + b\right) \tag{24}$$

4. Evaluation and Results: DDoS Attacks Detection

In this section, we perform evaluation results and discussions of our proposed scheme.

We used the dataset (2019) produced by the Canadian Institute for Cybersecurity (DDoS Evaluation Dataset [23,24] (CIC-DDoS2019)). This dataset provides suitable data on DDoS reflective attacks that can target power grid security. As we are using SVM and QSVM as a supervised ML, the dataset is divided into two classes, one for training and one for testing the evaluations.

Additionally, this dataset contains benign and the most up-to-date common DDoS attacks. We note that a sample of 38 features and 2950 data points (containing benign and simple service discovery protocol (SSDP) type DDoS attacks) are selected.

The preprocessing data phase is performed using three steps: class balancing, features selection and dimension reduction, and data encoding.

For the QSVM, we also consider:

- (1) A quantum programming language, including Q# (Q sharp) and quantum computation language (QCL). Q# can be installed on Windows, OSX, and Linux.
- (2) We use the HHL quantum algorithm [25] to solve system problems. Thanks to its exponential speed-up compared to classical methods, scientists and developers recommend HHL scheme as a basic model of many important quantum computing algorithms.
- (3) A quantum framework to simulate our models in our local computer. Indeed, we implement our approach using data provided classically and use the quantum state

space as feature space through the QSVM algorithm of the open-source software quantum framework Qiskit developed by IBM. We note that Qiskit provides access to a quantum simulator already developed with Python programming language.

We present a quantum model to detect DDoS attacks. We show our model performance in terms of accuracy, precision, sensitivity, and consumption of computational resources.

Our proposed quantum model proves his effectiveness in supporting current and future cybersecurity systems.

The confusion matrix which is also called error matrix, is a better method to evaluate the performance of a classifier by counting the number of instances for predicted or observed values in class A and which are classified as class B. Table 3 shows the confusion matrix used in ML models to define, visualize, and summarize the performance of classification schemes. In the following, equations used to define performance metrics (accuracy, precision, and recall) are presented:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (25)$$

$$Precision = \frac{TP}{TP + FP} \quad (26)$$

$$Recall = \frac{TP}{TP + FN} \quad (27)$$

Table 3. Confusion matrix.

Observed/Predicted	Positive	Negative	Count
Positive	True Positive (TP)	True Negative (TN)	P
Negative	False Positive (FP)	False Negative (FN)	N

Recall is a parameter describing the “sensitivity”: it measures the ratio of positive instances.

Figure 1 displays the variation of the accuracy, precision, and recall parameters of our QSVM model to show its ability to detect DDoS attacks. Curves vary between 99.91% and 99.94%. This result can be explained by the fact that our QSVM performs easily the classification procedure with a very low error rate.

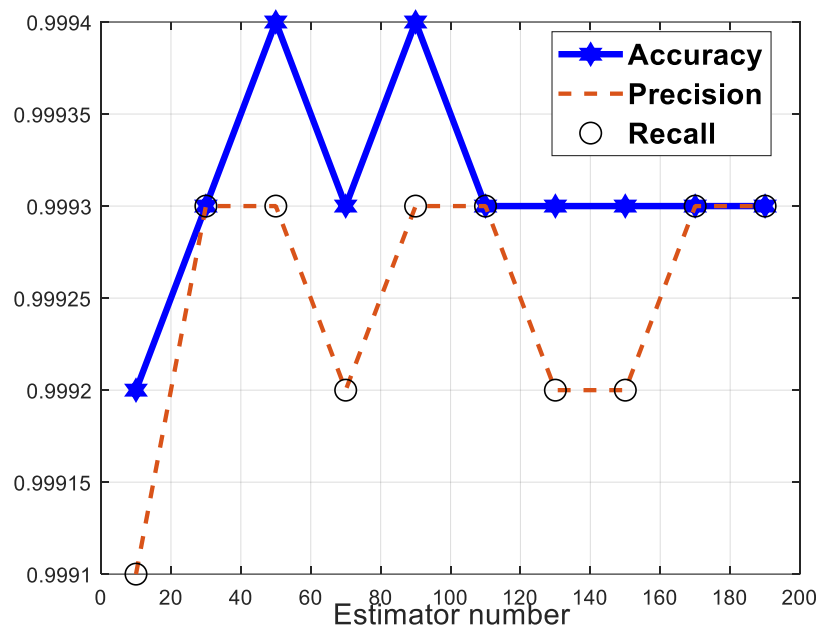


Figure 1. QSVM performance: accuracy, precision, and recall parameter visualization.

Figure 2 compares the normalized average value of accuracy, precision, and recall parameter variation of our QSVM (represented by blue color) and the classical SVM (highlighted by red color). From Figure 2, it is clear that QSVM maximizes the success rate (close to 100%) to detect and classify data and outperforms the classical SVM model in terms of the three metrics considered in this work (accuracy, precision, and recall). To prove the performance of our proposed scheme QSVM, we study its behavior in terms of the execution time (calculation time). For this issue, Figure 3 compares our QSVM (represented by blue color) and SVM (highlighted by red color). It is clear that our QSVM outperforms SVM with a saving rate of 93%. This result proves the effectiveness of our proposed QSVM.

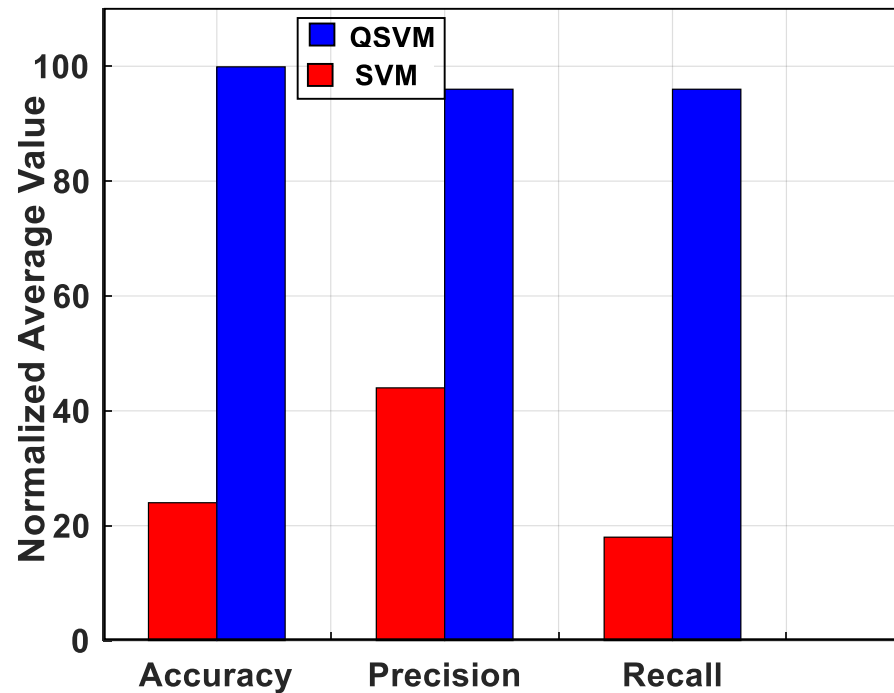


Figure 2. QSVM vs. SVM performance comparison: accuracy, precision, and recall parameters.

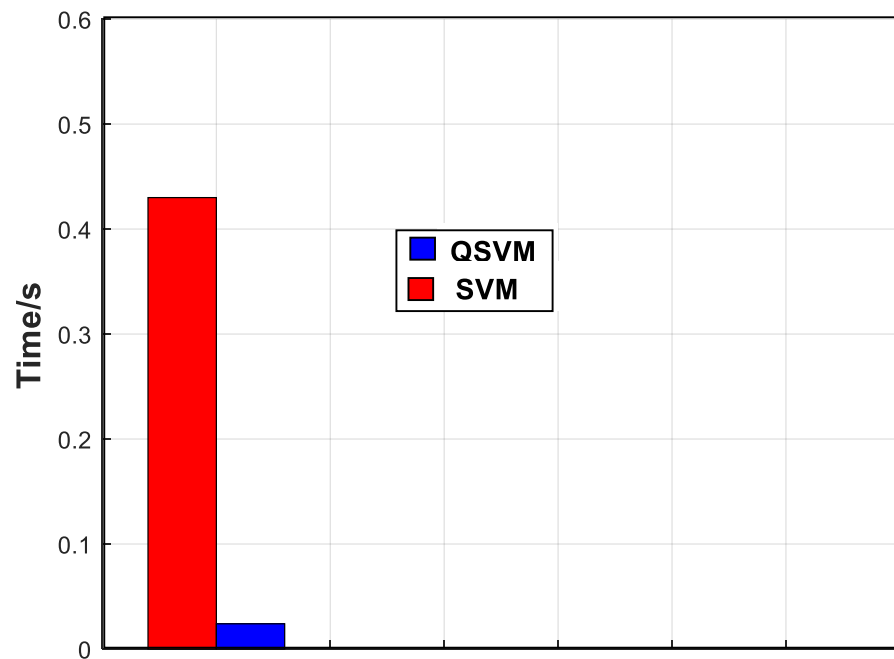


Figure 3. QSVM vs. SVM performance comparison: execution time.

5. Conclusions and Discussion

This paper highlights the potential of the QC in ML models to tackle the cyber-attacks in SMG. A comprehensive vision of the combination of ML and QC exploits the quantum mechanical phenomenon for data processing. The SVM and QSVM are twice implemented using a real dataset of DDoS attack instances, the open-source Qiskit software, and HHL quantum algorithm. A comparative evaluation proves the effectiveness of the QSVM model in terms of the accuracy and consumption of computational resources.

To conclude, QC presents an important computational power able to disrupt all software and hardware models. However, it needs several skills and thinking models compared to digital computing, especially in SMG, to establish standards for flexible quantum programming tools and environments, quantum hardware, software, and algorithms.

As a future work, we plan to extend this work and we propose to study the unsupervised learning toward the supervised one for unlabeled and labeled datasets in the DDoS attacks detection. Additionally, more research attention is needed with regard to quantum error correction and fault tolerance (QEFT) for bit and phase flipping, as well as quantum key distribution (QKD), which challenges the quantum era in SMG from both the points of view of the cyber-defenders and cyber-attackers.

Funding: This research received no external funding.

Data Availability Statement: No data available except those from reference part.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Said, D.; Elloumi, M.; Khoukhi, L. Cyber-Attack on P2P Energy Transaction Between Connected Electric Vehicles: A False Data Injection Detection Based Machine Learning Model. *IEEE Access* **2022**, *10*, 63640–63647. [CrossRef]
2. Said, D.; Elloumi, M. A New False Data Injection Detection Protocol based Machine Learning for P2P Energy Transaction between CEVs. In Proceedings of the 2022 IEEE International Conference on Electrical Sciences and Technologies in Maghreb (CISTEM), Tunis, Tunisia, 26–28 October 2022; pp. 1–5. [CrossRef]
3. Said, D. Intelligent Photovoltaic Power Forecasting Methods for a Sustainable Electricity Market of Smart Micro-Grid. *IEEE Commun. Mag.* **2021**, *59*, 122–128. [CrossRef]
4. Said, D. A Decentralized Electricity Trading Framework (DETF) for Connected EVs: A Blockchain and Machine Learning for Profit Margin Optimization. *IEEE Trans. Ind. Inform.* **2020**, *17*, 6594–6602. [CrossRef]
5. Ma, R.; Chen, X.; Zhai, R. A DDoS Attack Detection Method Based on Natural Selection of Features and Models. *Electronics* **2023**, *12*, 1059. [CrossRef]
6. Mohmand, M.I.; Hussain, H.; Khan, A.A.; Ullah, U.; Zakarya, M.; Ahmed, A.; Raza, M.; Rahman, I.U.; Haleem, M. A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks. *IEEE Access* **2022**, *10*, 21443–21454. [CrossRef]
7. Merlino, J.C.; Asiri, M.; Saxena, N. DDoS Cyber-Incident Detection in Smart Grids. *Sustainability* **2022**, *14*, 2730. [CrossRef]
8. Meriaux, E.; Koehler, D.; Islam, Z.; Vokkarane, V.; Lin, Y. Performance Comparison of Machine Learning Methods in DDoS Attack Detection in Smart Grids. In Proceedings of the 2022 IEEE MIT Undergraduate Research Technology Conference (URTC), Cambridge, MA, USA, 30 September–2 October 2022; pp. 1–5. [CrossRef]
9. Torres, G.; Shrestha, S.; Misra, S. iCAD: Information-Centric network Architecture for DDoS Protection in the Smart Grid. In Proceedings of the 2022 IEEE International Conference on Communications, Control, Singapore, Singapore, 25–28 October 2022, and Computing Technologies for Smart Grids (SmartGridComm); pp. 154–159. [CrossRef]
10. Naderi, E.; Asrari, A. Toward Detecting Cyberattacks Targeting Modern Power Grids: A Deep Learning Framework. In Proceedings of the 2022 IEEE World AI IoT Congress (AIoT), Seattle, WA, USA, 6–9 June 2022; pp. 357–363. [CrossRef]
11. Ullah, H.; Eskandarpour, R.; Zheng, H.; Khodaei, A. Quantum computing for smart grid applications. *IET Gener. Transm. Distrib.* **2022**, *16*, 4239–4257. [CrossRef]
12. Acampora, G.; Di Martino, F.; Robertazzi, G.A.; Vitiello, A. A Web Application for Running Quantum-enhanced Support Vector Machine. In Proceedings of the 2022 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Padua, Italy, 18–23 July 2022; pp. 1–7. [CrossRef]
13. Xanadu. Xanadu Quantum Cloud. Available online: <https://www.xanadu.ai/> (accessed on 14 March 2023).
14. Xanadu. Available online: <https://www.xanadu.ai/cloud> (accessed on 14 March 2023).
15. Xanadu. Strawberry Fields: A Cross-Platform Python Library for Simulating and Executing Programs on Quantum Photonic Hardware. Available online: <https://strawberryfields.ai/> (accessed on 14 March 2023).
16. Xanadu. PennyLane: A Cross-Platform Python Library for Differentiable Programming of Quantum Computers. Available online: <https://pennylane.ai/> (accessed on 14 March 2023).

17. D-Wave. Unlock the Power of Practical Quantum Computing Today. Available online: <https://www.dwavesys.com/> (accessed on 14 March 2023).
18. McGeoch, C.; Farré, P. *The D-Wave Advantage System: An Overview*; Technical report; D-Wave Systems Inc.: Burnaby, BC, Canada, 2020.
19. Alibaba Cloud. Available online: <https://www.alibabacloud.com/press-room/alibaba-cloud-and-caslaunch-one-of-the-worlds-mos> (accessed on 14 March 2023).
20. IBM Quantum Experience. Available online: <https://quantum-computing.ibm.com/> (accessed on 14 March 2023).
21. Khabbouchi, I.; Said, D.; Oukaira, A.; Mellal, I.; Khoukhi, L. Machine Learning and Game-Theoretic Model for Advanced Wind Energy Management Protocol (AWEMP). *Energies* **2023**, *16*, 2179. [[CrossRef](#)]
22. Bullock, S.S.; Markov, I.L. An arbitrary two-qubit computation in 23 elementary gates or less. In Proceedings of the 2003 Design Automation Conference (IEEE Cat. No.03CH37451), Anaheim, CA, USA, 2–6 June 2003; pp. 324–329. [[CrossRef](#)]
23. DDoS Evaluation Dataset (CIC-DDoS2019). Available online: <https://www.unb.ca/cic/datasets/ddos-2019.html> (accessed on 14 March 2023).
24. Sharafaldin, I.; Lashkari, A.H.; Hakak, S.; Ghorbani, A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–8. [[CrossRef](#)]
25. Boyer, M.; Brassard, G.; Godbout, N.; Liss, R.; Virally, S. Simple and Rigorous Proof Method for the Security of Practical Quantum Key Distribution in the Single-Qubit Regime Using Mismatched Basis Measurements. *Quantum Rep.* **2023**, *5*, 52–77. [[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.