International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 12, Issue 6 [June. 2023] PP: 47-56

Quantum Machine Learning and Cybersecurity

Jollanda Shara.
University "Eqrem Cabej", Gjirokaster, Albania

ABSTRACT: *The idea of quantum computers was developed by Richard Feynman and Yuri Manin. Quantum computation is a computational model which is based on the laws of quantum mechanics. Quantum computers can efficiently solve selected problems that are believed to be hard for classical machines. This is achieved by carefully exploiting quantum effects such as interference or likely entanglement.*

In the situation where the cyberattack are increasing in density and range, Quantum Computing companies, institutions and research groups may become targets of nation state actors, cybercriminals and hacktivists for sabotage, espionage and fiscal motivations. Quantum applications have expanded into commercial, classical information systems and services approaching the necessity to protect their networks, software, hardware and data from digital attacks. Recently, with the introduction of quantum computing, we have observed the introduction of quantum algorithms in Machine Learning. There are several approaches to QML, including Quantum Neural Networks (QNN), Quantum Support Vector Machines (QSVM) and Quantum Reinforcement Learning (QRL). In this paper we emphasize the importance and role of QML on cybersecurity.

Date of Submission: 26-05-2023 Date of acceptance: 07-06-2023

I. INTRODUCTION

Networks have transformed our lives through many purposes such as email, file transfer, web search, e-commerce, online banking, monetary transaction, education, collaboration, social networking, etc. But we are disposed to serious security risks because the internet is an insecure mean of communication.

Any device connected to the internet is vulnerable. Cybersecurity is safety against cyber-attacks. Cyber-attacks are launched by hackers to gain unauthorized access or steal important data. The estimated total damage caused by global cybercrime has increased from $300 billion in 2013 to $945 billion in 2020 (see [3, 4]).

The Quantum computer Network is a network that connects distant quantum devices using quantum links in conjunction with conventional ones. Regular computers use and analyse data in bits (0 or 1), while quantum computers use qubits, or quantum bits, which can simultaneously represent other states aside from ones and zeros. This is the main difference between quantum computers and traditional computers. [2]

The security of the internet will be seriously threatened by quantum computers. Many sectors, such as artificial intelligence, weather prediction, and medical research, carry significant potential for quantum computing. However, it also presents a serious risk to cyber security, suggesting us how to move in order to protect our data. Even though most of the present kinds of encryption can be decrypted by quantum computers, we still need to predict the threat and develop quantum-proof solutions. Furthermore, quantum technology will enhance cyber security. In today's cutting-edge technology, quantum devices can be utilized to enhance security by performing activities that are otherwise impossible, including secret key expansion with complete security [5].

Quantum machine learning (QML) can further improve the quality of conventional machine learning (ML) applications. These technologies in the noisy intermediate-scale quantum (NISQ) era explore the potential for developing systems that conclude with the search for advanced applications by quantum technologies. Modern ML has provided us with generative modeling techniques that are perfectly suited for the emerging landscape of NISQ hardware. An excellent example of this is the development of security systems against computer threats. There are three approaches of QML algorithms [7]: First, QML algorithms which are the quantum versions of conventional ML algorithms; second, the quantum-inspired ML algorithms that use the principles of quantum computing to improve classical methods of ML algorithms; third, the hybrid quantum-classical ML which combine quantum algorithms and classical ML algorithms to improve performance. [6]

II. QUANTUM COMPUTING

In the early 20th century, as we all know, the Theory of Relativity and the Theory of Quantum mechanics completely changed the path of Physics. They not only changed the physics but the whole technology creating an entire new field of computation usually known as Quantum Computing (QC). Quantum technology is going to be the next step to make computers faster and smarter, as well.

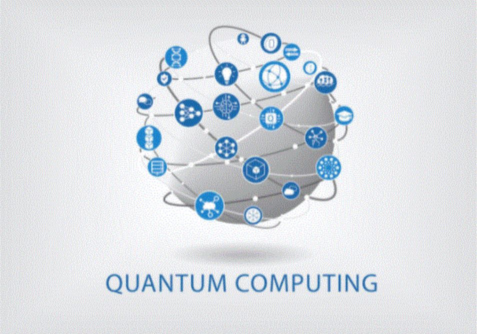

Fig. 1 Quantum Computing

Let us remember this marvellous quote of Max Planck: ” A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up that is familiar with it”. Quantum technologies have effected exactly in the same way the technologies of today. Quantum Computing is going to be the latest and the most powerful tool for Computational requirements. Currently computer security is handled by using mathematical theories for encrypting and decrypting the data in communication between sender and receiver. But even though we take into account the high performance computer, it would take exponentially long time to decrypt this information. While Quantum Computers can solve exponentially big mathematical problems in parallel in seconds. [8] Many unsolvable problems with the use of classic computing, have been responded by the Quantum Computing. It takes into account quantum mechanics laws, i.e., the part of physics that studies the smallest particles and how they assume more than one state at the same time [10]. In essence, we can even state that quantum mechanics is the basis of quantum computing. Indeed, it refers to the scientific laws that regulate the behavior of molecules, atoms, and subatomic particles and uses the related physical phenomena known as superposition and entanglement for the calculation [11].

Computers normally process information in bits that are zeros and one sequence (i.e., on and off), while quantum computers use Quantum Bits (i.e., qubits), which implement the concept of superposition. Simply speaking, the latter is when a bit can assume a value of zero, one, or even both at the same time. The superposition state represents a combination of all possible configurations. Overlapping groups of qubits can create complex and multidimensional computational spaces. It is in these spaces that complex problems are represented in new ways. (see [9]) The quantum devices that are expected to realise the first step in the demand for computing power are the so-called NISQ devices: noisy intermediate-scale quantum, involving a limited number of qubits that are not yet error-corrected nor noisefree. (see [12, 13])

A BRIEF HISTORY

The theory of quantum communication was first proposed by Albert Einstein. He noticed the existence of microscopic phenomenon and defined it as “spooky action at a distance” [15]. The first attempts at creating a quantum information theory were published in 1976 by Roman Stanisław Ingarden of the Nicolaus Copernicus University in Toruń, Poland. In 1981 a keynote speech titled Simulating Physics with Computers, Richard Feynman of the California Institute of Technology argues that a quantum computer had the potential to simulate physical phenomena that a classical computer could not simulate. In 1992, Deutsch–Jozsa algorithm is one of the first examples of a quantum algorithm that is exponentially faster than any possible deterministic classical algorithm. In 1996 , Lov Grover of Bell Laboratories invents the quantum database search algorithm. In 2002, the first version of the Quantum Computation Roadmap, a living document involving key quantum computing researchers, is published. In 2011, the first commercially available quantum computer is offered by D-Wave Systems. In 2012 1QB Information Technologies (1QBit), the first dedicated quantum computing software company, is founded. In 2017 Chinese researchers report the first quantum teleportation of independent single-photon qubits from a ground observatory to a low Earth orbit satellite with a distance of up to 1400 km. In 2019 Google claims to have reached quantum supremacy by performing a series of operations in 200 seconds that would take a supercomputer about 10,000 years to complete; IBM responds by suggesting it could take 2.5 days instead of 10,000 years, highlighting techniques a supercomputer may use to maximize computing speed. [14]

APPLICATIONS OF QUANTUM COMPUTING

Artificial Intelligence & Machine Learning

Artificial intelligence (AI) and Machine Learning (ML) are currently some of the more notable areas, because the emerging technologies have infiltrated in almost every aspect of our lives. Some of their common applications, as we know, are those in voice, image and handwriting recognition. However, with the increasing of the number of applications, it becomes a challenging task for traditional computers, to combine well the accuracy and speed. And, that's where quantum computing can help in processing through complex problems in very less time, which would have taken traditional computers thousands of years.[14]

Computational Chemistry

It is believed that the number of quantum states, even in a tiniest of a molecule, is extremely vast. So, it is very difficult for conventional computing memory to process that. The quantum computers can help here because they have the ability to focus on the existence of both 1 and 0 simultaneously. This could provide immense power to the machine to successfully map the molecules which, in turn, potentially opens opportunities for pharmaceutical research. Some of the critical problems that could be solved via quantum computing are improving the nitrogen-fixation process for creating ammonia-based fertilizer; creating a room-temperature superconductor; removing carbon dioxide for a better climate.

Drug Design & Development

One of the most challenging problem in quantum computing is the design and development of a drug. Usually, drugs are being developed via the trial and error method, which is not only very expensive but also a risky and challenging task to complete. Researchers believe that the quantum computing can be effectively used for understanding the drugs and its reactions on humans. This, in turn, can save much money and time for drug companies. These advancements in computing could enhance efficiency dramatically, by allowing companies to perform more drug discoveries to uncover new medical treatments for the better pharmaceutical industry. [14]

Cyber security & Cryptography

The online security space currently has been quite exposed because of the increasing number of cyber-attacks occurring daily in the world. The companies are creating necessary security framework in their organisations, but the process becomes daunting and impractical for classical digital computers. And, therefore, cybersecurity has continued to be an essential concern around the globe. Our increasing reliance on digitalisation, has becoming us even more vulnerable to these threats. Quantum computing with the help of machine learning can help in developing various techniques to combat these cybersecurity threats. In addition, quantum computing can help in creating encryption methods, also known as, quantum cryptography. [14]

Financial Modelling

Finding the right mix for successful investments based on expected returns, the risk associated, and other factors are important for a finance industry to survive in the market. To achieve that, the technique of 'Monte Carlo' simulations is continually being run on conventional computers, which, in turn, consume an enormous amount of computer time. The quantum technology can be applied to perform these massive and complex calculations. So, the companies can not only improve the quality of the solutions but also reduce the time to develop them. This is very important for the financial leaders who handle billions of dollars because even a very small improvement in the expected return can be worth a lot for them.

Logistics Optimisation

Improved data analysis and robust modelling will in fact allow a wide range of industries to optimise their logistics and arranging workflows associated with their supply-chain management. The operating models need to continuously calculate and recalculate optimal routes of traffic management, fleet operations, air traffic control, freight and distribution, and that could have a severe impact on applications. Usually, to do these tasks, conventional computing is used; however, some of them could turn into more complex for an ideal computing solution, whereas a quantum approach may be able to do it. [14]

Weather Forecasting

Currently, the process of analysing weather conditions by traditional computers can sometimes take longer than the weather itself does to change. But a quantum computer's ability to crunch great amounts of data, in a short period, could lead to enhancing weather system modeling. This can help scientists to predict the changing weather patterns in no time and with excellent accuracy. Weather forecasting includes several variables to consider, such as air pressure, temperature and air density. So, it can be difficult to be predicted with great accuracy. Application of quantum machine learning can help in improving pattern recognition. This, in turn, will make it easier for scientists to predict extreme weather events and potentially save thousands of lives a year. With quantum computers, meteorologists will also be able to generate and analyse more detailed climate models, which will provide a more accurate and deep understanding into climate change and ways to mitigate it.[14]

III. QUANTUM MACHINE LEARNING

Quantum machine learning (QML) is the intersection of machine learning and quantum computing. QML aims to use the capacity of quantum computers to process data at much faster speeds than traditional computers. QML refers to the use of quantum systems to embody algorithms that allow computer programs to improve through experience. Thus, in QML, quantum computers are used to handle machine learning problems making use of the natural efficiency of quantum computers. [16]

One area of research that has attracted significant interest is the design of machine learning algorithms that naturally depend on quantum properties to quicken their performance. One key observation that has led to the application of quantum computers to machine learning is their ability to perform fast linear algebra on a state space that grows exponentially with the number of qubits. These quantum accelerated linear-algebra based techniques for machine learning can be considered the first generation of quantum machine learning (QML) algorithms tackling a wide range of applications in both supervised and unsupervised learning, including principal component analysis, support vector machines, kmeans clustering, and recommendation systems. [17] The first approach: Quantum machine learning algorithms are quantum versions from conventional ML. The authors in [19] implemented SVM on quantum annealer device ([20]) (DW2000Q) called QA-SVM. They used quantum annealer to train and optimize SVM depends on QUBO equation to minimize cost energy. They utilized some of feature of quantum annealing (i.e. reverse annealing, and special annealing schedules to improve final results. Rebentrost, P. et al [21] presented SVM algorithm which runs on quantum computer and depends on a non-sparse matrix called QSVM. QSVM is a big data binary classifier. It works with a large number of features and samples in complexity logarithmic. Da Silva, A. et al [22] introduced a new quantum neural network named “quantum perceptron over a field” (QPF) and its learning algorithm (SAL). The learning algorithm (SAL) is based on superposition feature and quantum operator. Also, it performs NN architecture with polynomial time. QPF overcomes the limitations of quantum perceptron models. In [23] the authors proposed a version of linear regression called quantum linear regression which works on quantum data with N - dimensions of features in logarithmic time. The second approach is quantum-inspired machine learning. It applies the principles of Quantum Computing (QC) to improve classical methods of machine learning (ML).

The authors in [24] introduced a new quantum-inspired binary classifier (QIBC), based on decision theory, classical ML and theory of quantum detection that utilize one of the laws of quantum mechanics, superposition to increase the higher degree of freedom in decision making. The proposed classifier can be achieved high precision, recall and F-measure comparable with KNN, and SVM and other classical techniques. Sergioli et al. [25] proposed a novel quantum-inspired classifier for binary supervised learning called Helstrom Quantum Centroid (HQC). It is based on density matrices and formalism of quantum theory. The authors evaluated the performance of their model by fourteen datasets compared to different classical models. Ding et al. [26] proposed a novel algorithm inspired by the quantum support vector machines (SVM) to solve classification problems in exponential speedup, based on linear transformation. Sergioli et al. [27] introduced a Quantum Nearest Mean Classifier (QNMC) based on the idea of classical minimum distance classifier. The algorithm achieved higher accuracy in many medical data sets than the classical counterpart (NMC) exclusively cancer data set. In [28] is proposed a new model based on Quantum KNN and parallel computing for image classification, improving efficiency and classification performance. The authors in [29] used powerful parallel computing to introduce an inspired Quantum K Nearest-Neighbor (QKNN). It is based on one of the well-known properties of QC, superposition, to obtain parallel computing and “quantum minimum search algorithm” to speed up the search. The third approach is the hybrid quantum-classical machine learning. It includes the algorithms that combine quantum algorithms and classical (traditional algorithms) to obtain higher performance and decrease the learning cost.

The authors in [30] used the quantum circuit to present a new variational quantum classifier with a single quantum system (Qu *N* it). It aims to encode data in N-dimensional with a training algorithm called “single-shot training”. The main advantage of single-shot training is that it uses a fewer parameter for training and achieve a higher precision. In [31], the authors introduced a new quantum algorithms based on many subroutines as a quantum oracle, counting, amplitude amplification, and quantum amplitude estimation for feature selection named (HQFSA) with purpose enhancement of performance ML techniques. The proposed algorithm accomplished quadratic time complexity and better performance in some of the cases. The main disadvantage of HQFSA is that it runs on a quantum simulator only. Havlicek et al. [32] suggested two different models of quantum support vector machines. The first one is the variational quantum SVM based on quantum variation circuit. Maria Schuld et al. [33] proposed two- hybrid quantum techniques for classification problems. Schuld showed that quantum computing enhances classical ML algorithms like kernel methods. Quantum computing performs complex computations in Hilbert space more efficient. The authors focused on using feature maps and kernel methods in the quantum computing world. [18]

Quantum Machine Learning (QML) techniques are more effective in many real-world applications comparable to traditional machine learning in speed and accuracy. We can mention here the big data classification, forecasting series, spam detection, image compression, medical domain, electronic calculations, decision games, natural language processing (NLP), recommendation systems, speech recognition, image classification,and electrocardiogram signals classification. As applications related to hybrid quantum-classical approach we can mention those of scheduling problems, and classification task. [18]

IV. QUANTUM COMPUTING ON CYBERSECURITY

Quantum technologies are an important aspect in security world because of potential vulnerability of digital information and its interaction with other technologies. It is stated that being first in quantum technologies will surely bring a great strategic advantage, and not only. This will provide political and economic benefits, as well. At the centre of all this is the effect of quantum computing in cryptography. Highly important and huge amounts of data can be accessed using these technologies. This presents significant threat to existing technological infrastructure. To secure data and communication systems from these threats, the field of Cryptography is used. [8]

One of the areas where quantum computing has the greatest immediate effects on cyber security is cryptography. Public key encryption is widely used today to encrypt nearly all critical communications and data transferred over internet or to the cloud. Every internet browser which is currently used has the essential public - key encryption built in to protect traffic over the open internet. Most businesses make use of public key encryption to protect their internal data, communications, and user access to linked devices, as well. [34]

Cyber security impacts the security of computer systems from intrusions that might corrupt the data, software, or hardware [35]. By permitting illegal use, these assaults run the risk of exposing confidential information and causing harm or disruption. The quantum encryption is used to secure the CPS's classical communications infrastructure, which cannot be broken by quantum computers [36]

The current turn to remote work and the growing digitalization is associated by the increase of cyberattacks. Entities which collect and store sensitive data such as intellectual property, despite of sector or size, are at a higher risk of being selected for a cyberattack, such as espionage or sabotage. See, for example, [37, 38, 39]

Let us consider the case of theoretical conjectures about RSA-2048 bit decryption with quantum accelerators. Recent work by Google estimate 20 million NISQ device qubits to break an RSA key within 8h [40]. At the same time the newest developments in physical - not error corrected logical - qubits have not officially exceed the 100 qubit mark for NISQ devices [41], excluding digital annealer technologies - special purpose analog machines for optimization. Other theoretical advances promise the possibility of breaking RSA-2048 encryption with 13436 qubits in 177 Days [42] and the premise of a multimode quantum memory, which also is a theoretical presumption that has not been found. Even though we had a quadratic speedup due to a Grover algorithm for quantum accelerated pre-sampling to brute force key search against AES, it wouldn’t be possible to break anything above AES-256 bit key length with supercomputers nowadays [43]. Here, researchers argue that classified, encrypted data with longer intelligence life and shorter key length than AES-256, can be stored and broken in the future [44]. These may face a quantum threat from the future, but intelligence with a shorter lifetime is not affected taking into account that decryption might take months. Hence, the reverse threat of quantum computing devices is not near and the intelligence life of data plays a significant role in it.

Behind every cyberattack stands a threat actor and a motivation associated with it. Threat actors are classified through their objectives: politically motivated adversaries with nation state nearness are distinguished as nation-state actors, while financially motivated threat actors hacktivists. They are directed by ideology, but these boundaries are cloudy because some nation-state threat actors also have financial motives. [1]

On an abstract level, adversary tactics are similar. The first step is the exploration of the target for knowing it. After that, a foothold is established, followed by escalating privileges and then increase rapidly throughout the network undetected. If the motive is espionage, the adversary will try to remain undetected and cause little disturbance, whereas if an attacker’s motive is sabotage, disruption and damage follow making public the presence of an adversary. Financial gain objectives follow the same example, but they combine with either communication for extraction or data being sold off in the background. To defend against specific threat vectors and threat actor strategies, need to be known their patterns of behavior. They are packed up under the concept of Tactics, Techniques, and Procedures (TTPs). But this is not enough because the organization or institution which has been targeted needs to know their own system and environment to effectively impede possible attacks. Quantum computing systems either run in enterprise ecosystems constituting of one or a mix of Windows, macOS, Linux, Azure AD, SaaS, IaaS, Network, Containers, etc. platforms; or they are part of industrial control systems (ICS) often managed by a Supervisory Control and Data Acquisition (SCADA) system, via programmable logic controllers (PLCs) or discrete process control systems (DPC). Even in the case of ICS, the control systems are rarely, air-gapped, that is, physically separated from any network. Targets for threat actors can be QaaS (Quantum-as-a-Serive), quantum application providers, as well as users processing or consuming such services. Top vulnerabilities for cloud, web applications and ICS systems apply. Common cloud security risks include the misconfiguration of services, infrastructure security, service or data integration and non-production environment exposure. The prime web application security risks haven't changed immensely over the last decade and OAWSP Top Ten represent an abundant base for minimizing these risks. Some of them are broken authentication methods or access control, sensitive data exposure or cross-site scripting, where an attacker might take advantage of an API or manipulate the DOM (Domain Object Model) to hijack user accounts, access browser histories, control browsers remotely or spread malware. Social engineering and phishing attacks have high rates of success exploiting human nature, i.e. associativity and curiosity. USB drop attacks, impersonation and asking for internals can lead to spear phishing and credential theft. Not just legacy systems, new software design and development too, has its drawbacks and dangers. The use of hard-coded credentials, missing or improper authorization or authentication for critical functions, incorrect default permissions and the exposure of sensitive information to unauthorized actors are part of the most common and most dangerous software weaknesses.

In the sequel, we present some defensive measures, mitigations and best practices. The first step is knowing our own technology stack and environment. Systems with a high level of cybersecurity maturity exhibit security operation programs with extensive logging and monitoring for threat detection and response activities. Dependent on the application, system or processes, there is always a trade-off between cost and available resources. Identifying relevant risks to our critical assets and processes aids in putting vital security controls in place. Cyber hygiene and people awareness are the first line of defense which can easily strengthen. Remote work policies need to be in place as the attack surface expands into the cloud and homes of the employees. This means endpoints need to be protected, data at rest and in transit should be encrypted. Depending on the risk appetite and critical assets and applications, hybrid and cloud architectures need to be well configured regarding segmentation, authorization, authentication and encryption for relevant perimeters with firewalls and DMZs (Demilitarized Zone in perimeter networks) or follow a complete zero trust model if resources allow it. Cloud security gap analyses and security reviews help in finding misconfigurations and weaknesses Non-production environments should not be neglected - especially research and development systems. Quantum Computing Systems embrace a mix of off-the shelf components with proprietary software and hardware, which implicates the responsibility for flashing by design and releasing source-code bug fixes if for commercial use. The responsibility in off-the shelf components lies in recognizing vulnerabilities and patching them. Having a closer look on control systems, fail-safe systems should be segmented thereby preventing single-points of failure. For instance, an attacker shouldn't be able to have access to the cooling system and control unit of the ADI/QPU through the same Host-CPU for a sabotage attack on a compromised Quantum Computing System. The people vector is also pivotal in ICS environments. An air-gapped system can only be breached by bridging that gap to gain physical access. Unauthorized access by an insider threat or unaware employee can be mitigated by tightly locking up physical access, only whitelisting approved USB sticks and/or having a device antivirus scan stage implemented. (see [1])

Knowing the risks that a large, fault-tolerant quantum computer poses to cybersecurity it is of great importance to consider all the range of implications in order to reduce possible damages. We point out the following four basic ways in which quantum computers can be utilized to sabotage cybersecurity, as they are presented in [45]: "…

1. Information intercepted in the past, if recorded and stored properly, can be decrypted in the future by quantum computers. This is an inevitable risk that exists today—state actors or criminals may collect encrypted data with the hope that future advancements will enable them to decrypt it later. There are limited ways to protect against the pre-capture of data. Migrating applications to quantum-resistant encryption as quickly as possible will help mitigate this risk.
2. Organizations that do not assess their risks and migrate in time to quantum-resistant encryption will be susceptible to systemic data insecurity. This risk is systemic due to the hyperconnected nature of the digital ecosystem. As connectivity becomes more ubiquitous, a greater amount of critical data, communications, and services are reliant on the security of our systems. In addition, greater interdependency exacerbates the risk that incidents occurring in one part of the ecosystem can impact organizations on the other side. We must ensure that the security of our systems runs across end-to-end processes, supply chains, and shared infrastructure in order to develop resilience to the advancing threat of quantum computers.
3. Organizations that procrastinate and then rush to migrate to quantum-resistant encryption will likely be vulnerable to design and implementation flaws across IT platforms, creating errors that can be exploited by hackers without quantum computers. Organizations should proactively assess quantum vulnerabilities and develop a plan for transitioning to quantum-resistant encryption.
4. Without clear communication about our preparations for the cybersecurity risks of quantum computing, trust and confidence in the digital ecosystem will continue to erode. Quantum readiness plans from public and private sector entities and clear federal guidance on the transition to quantum-resistant encryption would help mitigate this risk…"

V. QML ON CYBERECURITY

The researchers are very hopeful that QML will surpass its classical counterparts nearby, even with noisy intermediate-scale quantum (NISQ) hardware, by utilizing quantum mechanics principles such as superposition, tunneling, and entanglement. A clearly important principal element for QML models used for classification tasks where statistical patterns can be disclosed in complex feature spaces, is provided by the high-dimensional Hilbert space of sizable quantum systems. However, QML models, like many modern machine learning models, possess assets and are vulnerable to attack. Researchers have indicated that the adverserial strength of any classifier is more and more reduced by the dimensions of the space on which it classifies. This has attracted the interest of QC/QML researchers, because QML models make use of quantum systems'high dimensionality. We present here the following assets and vulnerabilities:

QML circuits have the following assets, a) training data embedded in state preparation circuit; b) type of encoding used in the state preparation circuit; c) PQC ansatz; d) number of parameters; e) number of qubits and number of PQC layers.

Several companies, including IonQ, D-Wave, IBM, and Rigetti, now give the permission to use their quantum computers via cloud-based partners such as Azure Quantum, Amazon Braket, Google Cloud etc, where researchers regularly deploy their QML models to evaluate the robustness/performance in noisy environments. These cloud service providers often have multiple hardware with varying hardware quality and architectures, such as the number of qubits, coupling map, etc. The scheduler at the cloud service provider's end may have multiple hardware with the same coupling map at times. Furthermore, coupling maps of larger hardware, such as ibmq_rochester, with a greater number of qubits, can fit the coupling map of many smaller hardware, such as ibmq_london and ibmq_santiago. Hence, many choices of the user defined coupling map architecture exists in the quantum cloud. Unfortunately, user lacks capability to distinguish the identical coupling maps at cloud end. Thus, third-party cloud vendors may assign low-quality hardware to the job, leading to poor results and/or a longer convergence time for the quantum circuit. Some of the attack models and defenses are the followings:

Unreliable Hardware Allocator: For the purpose of saving money or meeting their falsely advertised qubit or quantum hardware specifications, untrustworthy quantum computers from third parties can distribute poor quality hardware. This can degrade severely QML model performance. To verify the identity of the hardware assigned by the cloud-based scheduler before sending the actual workload, authors in [49] proposed Quantum Physically Unclonable Function (QuPUF). It is known that each qubit is distinct with regard to gate error, readout error, decoherence error. So, they aimed to design a QuPUF for converting these error rates into qubit signature, which forms the hardware signature. QuPUF can also be used to defend against unreliable hardware allocator attack for QML application..

Compilation Oriented Attacks: A new split methodology to secure IPs from untrusted compilers while taking advantage of their optimizations is presented in [50]. The main idea behind their proposed method is that instead of sending the entire quantum circuit at once, it is divided into multiple parts that are sent to a single compiler at different times or to multiple compilers. These sub-circuits are later combined together accordingly by the designer post-compilation. Conducting extensive experiments with 152 circuits they concluded that this split compilation method can completely secure IPs or introduce factorial time reconstruction complexity with a minor overhead (max 6%). To make circuits more robust against any kind of tampering/counterfeiting from untrusted third party compilers, the authors in [51] insert dummy SWAP gates to corrupt the functionality of the program. They presented a method for determining the best position for dummy SWAP gate insertion that maximizes Total Variation Distance (TVD) without requiring time-consuming quantum circuit simulation. Experiments show that their proposed metric achieved a ≈ 6% improvement over average TVD and a ≈ 12% improvement over best TVD with minimal overhead. Consequently, third-party cloud suppliers may assign low-quality hardware to the job.

Fault Injection Attacks: The gate error of an isolated operation may differ from the gate error with another gate operation in parallel. This is known as the crosstalk error. In another research, [48], it is shown that the gate error with another operation in parallel can be ≈ 3 times higher than an isolated gate operation. Because of this, crosstalk may negatively impact the prediciton/classification accuracy of a QML model. In [47], the authors have demonstrated that an external adversary can inject faults into another user's program sharing the same hardware by repeatedly driving qubits using CNOT gates. This would cause a QNN to perform worse than it would in a normal environment.

Saki et al. [47], investigated these types of threats on quantum circuits and classifiers, proposing a method to mitigate the above threat by introducing isolation/buffer qubits between user programs. This basically means that when one QNN circuit is running on a set of qubits in a hardware, another program is not allowed to run on the previous program's neighbouring qubits. This is maintained by inserting/considering those neighbouring qubits as buffer/isolation qubits. Their analysis shows that buffer qubits provide as much as 1.87× higher reliability at the cost of a few unused qubits. (see [46]).

Quantum-enhanced ML algorithms can surpass their classical ML counterpart algorithm in diverse applications. Taylor argued that quantum computing is similar to a double-edged sword; it significantly improves information technologies and could cause catastrophic or irreversible events [53]

A quantum hybrid reinforcement learning model is compared with a classical counterpart in [54]. As it has been suggested from the experiment results, for the most part, the classical reinforcement model presents better performance for a small problem, like the frozen lake problem. The hybrid quantum model converges earlier than the classical counterpart; however, it takes a longer runtime to finish. The authors suggested that quantum and classical counterpart models should be compared on more complex problems. A hybrid quantum CNN model was also introduced in [55]. In this work the authors adopted a federated learning approach to secure models and avoid privacy leakage attacks. The results of their experiment show that the models with additional quantum convolution have slightly improved accuracy than the baseline classical models. In [56], the authors have proposed a hybrid quantum–classical model with classical feed-forward fully connected neural network (FCNN) model conducting such a comparison to benchmark. In [57] was used another hybrid quantum-classical generative adversarial approach to develop an anomaly/fraudulent transaction detection using a credit card fraud dataset. The performances of their model equate with the classical counterpart in terms of the F1 score. However, noisy experiments were not included in this paper. For investigating the performance effects on the model, the authors suggested possible future works: including a realistic noise model, instead of only using a noiseless quantum computer setting.

Botnet attacks are notorious for using domain name system (DNS) traffic to hide their communication messages with a command and control (C&C) server and constitute a severe cybersecurity threat. Moreover, the DGA-based botnet type is one of the most disruptive and challenging to be detected since it hides its queries throughout the domain name system (DNS) traffics and uses CNC servers' domain names generated algorithmically. [62] Furthermore, in the current 5G and B5G networks era, potentially billions of smart devices are affected by botnet DGA attacks [63]. A recent survey paper on botnet detection can be seen in [64]. An overview of the current progress of the quantum DL which is an intersection between deep learning and quantum computing, is available in the literature [65]. (see [61])

The domain of cybersecurity, as we pointed out, has attracted many researchers from QML. Gong et al. compares VQCs against DNN, support vector machines, K-Nearest Neighbors, Naive Bayes and decision trees on the KDD Cup99 data set, that is focused on network intrusion. They find that their VQC approach achieves on the whole the highest precision, recall and F1 score and the lowest false negative rate compared to all other approaches. Furthermore, they test their model, which was trained with TensorFlow quantum (TFQ), with 100 randomly sampled data points on IBM quantum computers. Using the erroneous quantum hardware, they measure a prediction error of 11.96 %, compared to the TFQ simulator. Therefore, their approach suffers from the system noise of the quantum computer [59]

A different approach to cyber-attack detection was taken in [60]. The authors studied the controller area network (CAN) attack dataset for in-vehicle cyber-attack detection. They specifically concetrated on amplitude shift attacks, where the amplitude of a feature is shifted by a random value. Within their work, they encode the CAN data as an 13×13 image, which is used for further processing. The authors compare an LSTM, pure QVC and a hybrid QVC. For the hybrid QVC, they used a convolutional neural network (CNN) for feature extraction. The extracted features are then used in the QVC. Their results show that the quantum hybrid approach surpassed the other two models with an evaluation accuracy of 93.97 %. This value is about 6 % more than the LSTM and more than 30 % better than the pure quantum model.

The literature review shows that cyber-security is a promising research field for QML, since QVC approaches present similar or improved performance compared to classical models. On a practical basis, it can be observed that training QVCs on real quantum hardware is not feasible because of long run times and noise. Even the use of simulators, does not solve the run time issue. Both approaches have severe limitations on the number of qubits used and thus restrict the size of data sets used. Thus, we can use smaller models in parallel to help the reduction of runtime and allow solving larger datasets. (see [58])

VI. CONCLUSION

The birth and development of quantum computing can be the most impactful domain for cybersecurity that can emerge both as a threat and solution to critical cybersecurity issues. Quantum computing for cyber security indicates that quantum computing shall be utilized for the advancement of cybersecurity threats. The Quantum Computing industry is a probable target for sabotage, espionage and extortion motives.

Quantum Computing has a significant role in emerging technologies and specifically cyber security .This field opens new horizons for research in the fields of computation like diagnostics, drugs developments, financial services, networking, space communications, Artificial Intelligence etc. It can elevate the technologies to new great heights and will help us making our lives more easy and secure, as well. [8]

Quantum computing utilizes algorithms to solve difficult problems much faster than a classical computer. Quantum machine learning (QML) is a new emerging technology that takes advantage of both the quantum computing power and the efficiency of ML. In this paper, we tried to describe some of the QML applications on cybersecurity. Only a few years ago, most of the research works in this field were largely theoretical, but now we have many QML algorithms which have improved their ML counterparts and have been used successfully in many fields, especially in cybersecurity. Many interesting results are achieved in this area by many researchers, as we show in this study. But the amount of research works is being more and more abundant. It is almost inexhaustible. So, the interested reader can search other sources, as well.

REFERENCES

[1]. Natalie Kilber, Daniel Kaestle and Stefan Wagner, [2021], "Cybersecurity for Quantum Computing", arXiv:2110.14701v1 [quant-ph].

[2]. V. Bindhu, [2022], "Cyber Security Analysis for Quantum Computing", Journal of IoT in Social, Mobile, Analytics, and Cloud, Volume 4, Issue 2, 133-142 133, https://doi.org/10.36548/jismac.2022.2.006.

[3]. Vivek Dixit, Raja Selvarajan, Tamer Aldwairi, Yaroslav Koshka, Mark A. Novotny, Travis S. Humble, Muhammad A. Alam, and Sabre Kais, [2021], "Training a quantum annealing based restricted Boltzmann machine on cybersecurity data", arXiv:2011.13996v4 [quant-ph].

[4]. M. Smith, Zhanna, and E. Lostri, [2020], "The hidden costs of Cybercrime, Technical Report", Santa Clara: McAfee., https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

[5]. https://www.ibm.com/topics/quantum-computing.

[6]. Hatma Suryotrisongko and Yasuo Musashi, [2022], "Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection", ScienceDirect Procedia Computer Science 197, 223–229, www.sciencedirect.com.

[7]. Abohashima, Z., M. Elhosen, E. H. Houssein, and W. M. Mohamed, [2020], "Classification with quantum machine learning: A survey", arXiv preprint arXiv:2006.12270.

[8]. Abhishek Agnihotri, Ishika Pandya, [2021], "A Quantum Review: Cyber Security and Emerging Technologies", International Research Journal of Modernization in Engineering Technology and Science Volume 03, Issue 06, 1032-1035.

[9]. Mercaldo, F., Ciaramella G., Iadarola G., Storto M., Martinelli F., Santone A., [2022], "Towards Explainable Quantum Machine Learning for Mobile Malware Detection and Classification" Appl. Sci., 12, 12025. https://doi.org/10.3390/app122312025.

[10]. Hirvensalo M., [2003], "Quantum Computing", Springer Science & Business Media: Berlin, Germany.

[11]. Gill S.S., Kumar A., Singh H., Singh M., Kaur K., Usman, M., Buyya R., "Quantum computing: A taxonomy, systematic review and future directions", Softw. Pract. Exp., 52, 66–114.

[12]. Phillipson F., Wezeman R.S.,Chiscop I., [2021], "Indoor–Outdoor Detection in Mobile Networks Using Quantum Machine Learning Approaches", Computers, 10, 71, https://doi.org/10.3390/computers10060071.

[13]. Resch, S., Karpuzcu, U.R., [2019], "Quantum computing: An overview across the system stack", arXiv:1905.07240.

[14]. Nisha Jha, [2021], "Short Review on Quantum Computing and It Future Trends", International Journal of Research in Engineering and Science (IJRES), Volume 9 Issue 7, 71-75.

[15]. A. Einstein, M. Born, and H. Born, [2005], "The Born-Einstein letters: friendship, politics, and physics in uncertain times", Correspondence between Albert Einstein and Max and Hedwig Born from 1916 to 1955 with commentaries by Max Born. Macmillan, 2005.

[16]. Tariq M. Khan and Antonio Robles-Kelly, "Machine Learning: Quantum vs Classical", IEEE Access, 219275-219294, doi: 10.1109/ACCESS.2020.3041719.

[17]. Michael Broughton, Guillaume Verdon, Trevor McCourt, Antonio J. Martinez, Jae Hyeon Yoo, Sergei V. Isakov, Philip Massey, Ramin Halavati, Murphy Yuezhen Niu, Alexander Zlokapa, Evan Peters, Owen Lockwood, Andrea Skolik, Sofiene Jerbi, Vedran Dunjko, Martin Leib, Michael Streif, David Von Dollen, Hongxiang Chen, Shuxiang Cao, Roeland Wiersema, Hsin-Yuan Huang, Jarrod R. McClean, Ryan Babbush, Sergio Boixo, Dave Bacon, Alan K. Ho, Hartmut Neven and Masoud Mohseni, [2021] "TensorFlow Quantum: A Software Framework for Quantum Machine Learning", arXiv:2003.02989v2 [quant-ph] 26 Aug 2021.

[18]. Zainab Abohashima, Mohamed Elhoseny, Essam H. Houssein, Waleed M. Mohamed, "Classification with Quantum Machine Learning: A Survey".

[19]. Willsch D, Willsch M, De Raedt H, Michielsen K., [2020], "Support vector machines on the D-Wave quantum annealer", Computer Physics Communications, 248:107006.

[20]. Headquarters C. Technical Description of the D-Wave Quantum Processing Unit. 2019.

[21]. Rebentrost P, Mohseni M, Lloyd S., [2014], "Quantum support vector machine for big data classification". Physical review letters, 113(13):130503.

[22]. da Silva AJ, Ludermir TB, de Oliveira WR., [2016], "Quantum perceptron over a field and neural network architecture selection in a quantum computer". Neural Networks. 76:55-64.

[23]. Schuld M, Sinayskiy I, Petruccione F., [2016], "Prediction by linear regression on a quantum computer". Physical Review A, 94(2):022342.

[24]. Tiwari P, Melucci M. [2019], "Towards a quantum-inspired binary classifier". IEEE Access, 7:42354-72.

[25]. Sergioli G, Giuntini R, Freytes H., [2019], "A new quantum approach to binary classification", PloS one, 14(5).

[26]. Ding C, Bao T-Y, Huang H-L., [2019], "Quantum-Inspired Support Vector Machine", arXiv preprint arXiv:190608902.

[27]. Sergioli G, Russo G, Santucci E, Stefano A, Torrisi SE, Palmucci S, et al., [2018], "Quantum-inspired minimum distance classification in a biomedical context", International Journal of Quantum Information, 16(08):1840011.

[28]. Dang Y, Jiang N, Hu H, Ji Z, Zhang W., [2018], "Image classification based on quantum K-Nearest-Neighbor algorithm", Quantum Information Processing, 17(9):239.

[29]. Chen H, Gao Y, Zhang J., [2015], "Quantum k-nearest neighbor algorithm", Dongnan Daxue Xuebao, 45(4):647-51.

[30]. Sagheer A, Zidan M, Abdelsamea MM., [2019], "A novel autonomous perceptron model for pattern classification applications", Entropy, 21(8):763.

[31]. Adhikary S, Dangwal S, Bhowmik D., [2020], "Supervised learning with a quantum classifier using multi-level systems", Quantum Information Processing. 19(3):89.

[32]. Havlíček V, Córcoles AD, Temme K, Harrow AW, Kandala A, Chow JM, et al. [2019], "Supervised learning with quantum enhanced feature spaces", Nature, 567(7747):209-12.

[33]. Schuld M, Killoran N., [2019], "Quantum machine learning in feature Hilbert spaces", Physical review letters. 122(4):040504.

[34]. https://businessinsights.bitdefender.com/how-quantum-computing-will-impact-cybersecurity

[35]. Petros Wallden and Elham Kashefi, [2019]. “Cyber security in the quantum era”, Commun. ACM 62, 4, 120. https://doi.org/10.1145/3241037.

[36]. D. Tosh, O. Galindo, V. Kreinovich and O. Kosheleva, [2020], “Towards Security of Cyber-Physical Systems using Quantum Computing Algorithms”, IEEE 15th International Conference of System of Systems Engineering (SoSE), 2020, pp. 313-320, doi: 10.1109/SoSE50414.2020.9130525.

[37]. Bitdefender, Cyberattack against uk supercomputer archer forces operators to disable access for scientists, Accessed: 2021. URL: https://www.bitdefender.com/blog/hotforsecurity/cyberattack-against-uk-supercomputer-archer-forces-operators-to-disable-access-for-scientists.

[38]. J. News, [2021], “Forschungszentrum jülich - jsc - archiv newsletter "jsc news" - cyberattack against supercomputers”, Accessed: 2021. URL: https://www.fz-juelich.de/SharedDocs/Meldungen/IAS/JSC/EN/2020/2020-06-cyberattack.html?nn=1060464.

[39]. NCSC, [2021], “More ransomware attacks on uk education”, ncsc.gov.uk, URL: https: //www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector.

[40]. C. Gidney, M. Ekerå, [2019], “How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits”, URL: http://arxiv.org/abs/1905.09749http://dx.doi.org/10.22331/q-2021-04-15-433, doi:10.22331/q-2021-04-15-433.

[41]. IBM, [2021], “Ibm’s roadmap for scaling quantum technology”, ibm research blog, URL: https://research.ibm.com/blog/ibm-quantum-roadmap.

[42]. Élie Gouzien, N. Sangouard, [2021], “Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory”, Physical Review Letters 127, doi:10.1103/physrevlett.127.140503.

[43]. L. K. Grover, [1996], “A fast quantum mechanical algorithm for database search”, Proceedings of the Annual ACM Symposium on Theory of Computing Part F129452 212–219, URL: https://arxiv.org/abs/quant-ph/9605043v3.

[44]. J. Tibbetts, [2019], “Quantum computing and cryptography: Analysis, risks, and recommendations for decisionmakers”.

[45]. Michaela Lee, [2021], “Quantum Computing and Cybersecurity”.

[46]. Satwik Kundu, Swaroop Ghosh, [2022], “Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses” (Invited), arXiv:2204.03625v1 [cs.CR] 7 Apr 2022.

[47]. Abdullah Ash-Saki, Mahabubul Alam, and Swaroop Ghosh, [2020], “Analysis of Crosstalk in NISQ Devices and Security Implications in Multi-Programming Regime”, In Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED ’20), Association for Computing Machinery, 25–30. https://doi.org/10.1145/3370748.3406570.

[48]. Prakash Murali, David C. McKay, Margaret Martonosi, and Ali Javadi-Abhari, [2020], “Software Mitigation of Crosstalk on Noisy Intermediate-Scale Quantum Computers”, In Proceedings of the 25th International Conference on Architectural Support for Programming Languages and Operating Systems. ACM, 1001–1016.

[49]. Koustubh Phalak, Abdullah Ash Saki, Mahabubul Alam, Rasit Onur Topaloglu, and Swaroop Ghosh, [2021], “Quantum PUF for Security and Trust in Quantum Computing”, IEEE Journal on Emerging and Selected Topics in Circuits and Systems 11, 2, 333–342, https://doi.org/10.1109/JETCAS.2021.3077024.

[50]. Abdullah Ash Saki, Aakarshitha Suresh, Rasit Onur Topaloglu, and Swaroop Ghosh, [2021], “Split Compilation for Security of Quantum Circuits”, In 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD). 1–7, https://doi.org/10.1109/ICCAD51958.2021.9643478.

[51]. Aakarshitha Suresh, Abdullah Ash Saki, Mahabubul Alam, Rasit Onur Topaloglu, and Dr. Swaroop Ghosh. [2021], “A Quantum Circuit Obfuscation Methodology for Security and Privacy”, https://doi.org/10.48550/ARXIV.2104.05943.

[52]. Hatma Suryotrisongko, Yasuo Musashi, [2022], “Hybrid Quantum Deep Learning and Variational Quantum Classifier-Based Model for Botnet DGA Attack Detection”, International Journal of Intelligent Engineering and Systems, Vol.15, No.3, DOI: 10.22266/ijies2022.0630.18.

[53]. R. D. Taylor, “Quantum Artificial Intelligence: A ‘precautionary’ U.S. approach?”, Telecommunications Policy, p. 101909, 2020, doi: 10.1016/j.telpol.2020.101909.

[54]. Moll, M., and Leonhard Kunczik, [2021], “Comparing quantum hybrid reinforcement learning to classical methods”, Human-Intelligent Systems Integration 3(1), 15-23.

[55]. Yang, Chao-Han Huck, J. Qi, S. Y. C. Chen, P. Y. Chen, S. M. Siniscalchi, X. Ma and C. H. Lee, [2021], “Decentralizing feature extraction with quantum convolutional neural network for automatic speech recognition”, In ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) IEEE 6523-6527.

[56]. Adhikary, Soumik, Siddhart Dangwal, and Debanjan Bhowmik, [2020], “Supervised learning with a quantum classifier using multi-level systems”, Quantum Information Processing 19(3), 1-12.

[57]. Herr, Daniel Matthias, Benjamin Obert, and Matthias Rosenkranz, [2021], “Anomaly detection with variational quantum generative adversarial networks”, Quantum Science and Technology.

[58]. Maximilian Moll and Leonhard Kunczik, [2021], “A Case Study for Cyber-Attack Detection using Quantum Variational Circuits”, Springer Nature 2021.

[59]. Gong, C., Guan, W., Gani, A., Qi, H., [2022], “Network attack detection scheme based on variational quantum neural network”, The Journal of Supercomputing, 1–22.

[60]. Islam, M., Chowdhury, M., Khan, Z., Khan, S.M., [2022]. “Hybrid quantumclassical neural network for cloud-supported in-vehicle cyberattack detection”, IEEE Sensors Letters 6(4), 1–4, https://doi.org/10.1109/LSENS.2022.3153931.

[61]. Hatma Suryotrisongko, Yasuo Musashi, Akio Tsuneda, Kenichi Sugitani, [2022], “Adversarial Robustness in Hybrid Quantum-Classical Deep Learning for Botnet DGA Detection”, Journal of Information Processing Vol.30 636–644, DOI: 10.2197/ipsjjip.30.636.

[62]. Wang, T.S., Lin, H.T., Cheng,W.T. and Chen, C.Y., [2017], “DBod: Clustering and detecting DGA-based botnets using DNS traffic analysis”, Computers& Security, Vol.64, pp.1–15, DOI: 10.1016/j.cose.2016.10.001.

[63]. Zago, M., Gil P´erez, M. and Martinez Perez, G., [2021], “Early DGA-based botnet identification: Pushing detection to the edges”, Cluster Comput, DOI: 10.1007/s10586-020-03213-z.

[64]. Singh, M., Singh, M. and Kaur, S., [2019], “Issues and challenges in DNS based botnet detection: A survey”, Computers & Security, Vol.86, pp.28–52, DOI: 10.1016/j.cose.2019.05.019.

[65]. Garg, S. and Ramakrishnan, G., [2020], “Advances in Quantum Deep Learning: An Overview”, arXiv:2005.04316 [quantph].