Quantum Computing for Healthcare: A Review

Raihan Ur Rasool[1], Hafiz Farooq Ahmad[2], Wajid Rafique[3], Adnan Qayyum[4], Junaid Qadir[5] and Zahid Anwar[6]
[1] Victoria University, Melbourne, Australia
[2] King Faisal University, Al-Ahsa, Saudi Arabia
[3] University of Calgary, Calgary, AB T2N 1N4, Canada
[4] Information Technology University (ITU), Punjab, Lahore, Pakistan
[5] Qatar University, Doha, Qatar
[6] North Dakota State University (NDSU), Fargo, ND. USA

Abstract

Classical computing works by processing bits, or 0s and 1s representing electrical signals of on and off. Quantum computing employs a very different technique for information processing. It uses qubits, which can exist as both a 1 and 0 at the same time, and uses the properties of subatomic particles in quantum physics such as interference, entanglement, and superposition to extend computational capabilities to hitherto unprecedented levels. The efficacy of quantum computing for important verticals such as healthcare where quantum computing can enable important breakthroughs in the development of life-saving drugs, performing quick DNA sequencing, detecting diseases in early stages, and performing other compute-intensive healthcare related tasks is not yet fully explored. Furthermore, implementations of quantum computing for healthcare scenarios such as these have their own unique set of requirements. Unfortunately, existing literature that address all of these dimensions is largely unstructured. This research is intended to be the first systematic analysis of the capabilities of quantum computing in enhancing healthcare systems. This article is structured with the help of taxonomies developed from existing literature to provide a panoramic view of the background and enabling technologies, applications, requirements, architectures, security and open issues, and future research directions. We believe the paper will aid both new and experienced researchers working in both quantum computing and the healthcare domains in visualizing the diversity in current research, in better understanding both pitfalls and opportunities, and coming up with informed decisions when designing new architectures and applications for quantum computing in healthcare.

Index Terms

Internet of Things, quantum computing, healthcare services, qubits, high performance.

I. Introduction

Recent years have seen a strong impetus for smart healthcare and monitoring systems but current computing infrastructures face several challenges in keeping up with the sheer volume, veracity, and velocity of electronic health data. During the COVID-19 pandemic novel variants of the virus consecutively emerged over a short span of a few months. Healthcare professionals working on genome sequencing of the virus and caregivers monitoring infected patients were hard-pressed keeping up with using traditional computing systems available to them. Therefore, there is a strong need to explore novel ways which can speed up healthcare analysis and monitoring efforts in order to more efficiently cater to such future pandemic situations. Quantum computing promises a revolutionary and arguably the most potent–boost to healthcare technologies. To cater to this upcoming and advancing computing paradigm a large body of literature has been written on ways quantum computing could introduce new possibilities through higher computational speed to perform complex healthcare computations. In spite of the interest, the majority of the research works on quantum computing in healthcare remain largely unstructured. While some surveys and taxonomies of quantum computing use in the healthcare domain have been proposed they consider only a small proportion of the range of disruptive use cases. To the best of our knowledge, this research provides the first systematic analysis of quantum computing in the healthcare industry. The paper is structured to provide a panoramic view of the background and enabling technologies, applications, requirements, architectures, security and open issues, and future research directions. We contend that this structure and the taxonomies developed will aid both new and experienced researchers in both quantum computing and the healthcare domains in visualizing the diversity in current research, better understanding both pitfalls and opportunities, and coming up with informed decisions when designing new architectures and applications for quantum computing in healthcare. The following subsections introduce quantum computing, its use in healthcare, and our motivation for this survey in light of the limitations of existing surveys and its contributions.

A. Introduction to Quantum Computing

Quantum Computing (QC) is underpinned by quantum mechanics, and hence often explained through concepts of superposition, interference, and entanglement. In quantum physics, a single bit can be in more than one state simultaneously (i.e. 1 and 0) at a given time, and a QC system leverages this very behavior and recognizes it as a qubit (Quantum bit). Having roots in quantum physics, QC has the potential of becoming the fabric of tomorrow's highly powerful computing infrastructures, enabling the processing of gigantic amounts of data in real time. Quantum computing has recently seen a surge of interest by researchers who are looking to take computing prowess to the next level as we move past the era of Moore's law, however, there is a need for an in-depth systematic survey to explain possibilities, pitfalls, and challenges.

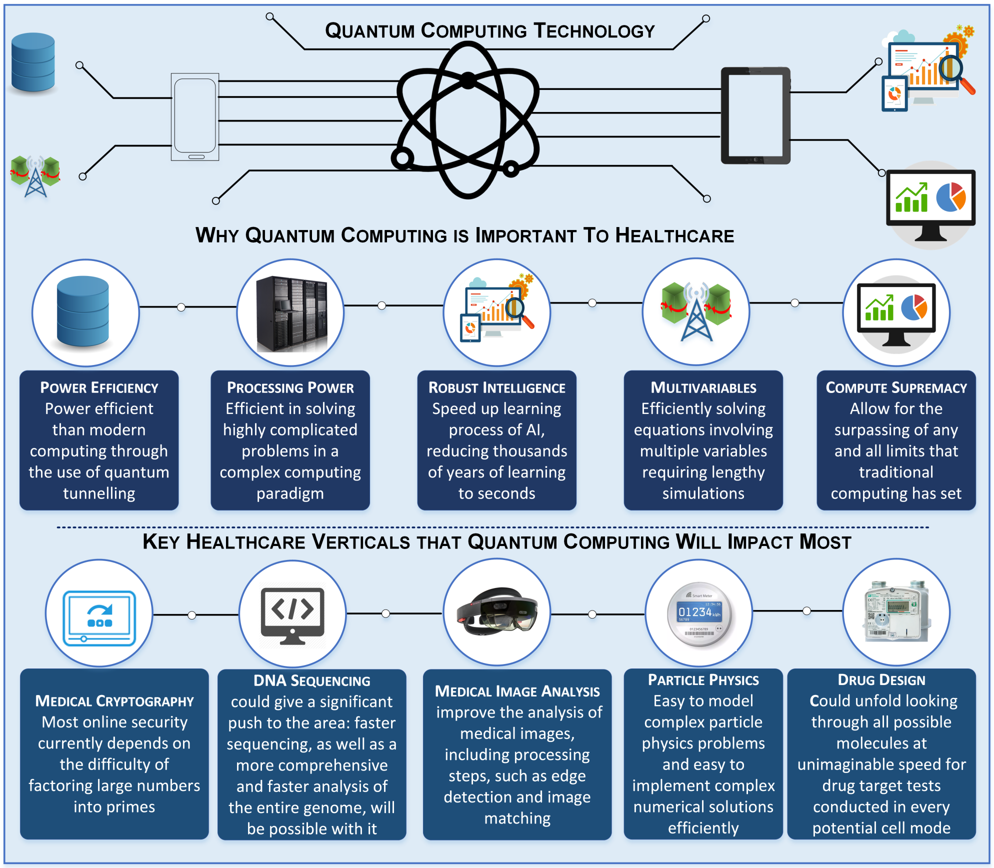

Fig. 1: *Why use quantum computing* and which *key verticals* will it disrupt?

B. Quantum Computing for Healthcare

Quantum computing is particularly well suited to numerous compute-intensive applications of healthcare (1) especially in the current highly connected IoT digital healthcare paradigm (2; 3), which encompasses interconnected medical devices (such as medical sensors) that may be connected to the Internet or the cloud. Healthcare IoT devices typically comprise of *sensors* that sense the environment; for example, a wearable glucose monitor senses the blood sugar level in a patient suffering from diabetes. Sensors will transmit the values using short-range communication protocols such as Bluetooth, 6LoWPAN, Zigbee, and Wi-Fi to a *controller* that processes the information for example determining the dosage of insulin to administer based on historic patient records and parameters configured by a physician. The *controller* will then signal another IoT device called an *actuator* that is designed to change the environment. In the case of our example, a pump will inject the patient with insulin. The challenges that healthcare IoT face is that devices such as sensors and actuators are large in number, they are extremely resource-constrained and require efficient Quality of Service (QoS), and therefore need to rely on more powerful servers for timely processing. With its capabilities, quantum computing can help address the challenges and issues that hamper the growth of IoT. Today's quantum computers require at least 25 kilowatts per annum to operate, generate a large amount of heat and are very unstable to conditions in their vicinity because any involvement or measurement causes a collapse of the state function- a situation known as decoherence. Therefore while it may be challenging to operate healthcare IoT devices such as sensors and actuators using quantum computing, it is expected to be deployed to the more powerful communication infrastructure (e.g., cloud, cellular, etc.) to which these devices are constantly connected. The high computational performance of quantum computers can be advantageous to IoT since these devices generate a massive amount of data warranting extensive processing and involved optimization procedures. Furthermore more secure communication of sensitive patient data is possible through quantum cryptography.

The massive increase in computational capacity is not only beneficial for healthcare IoT but can allow quantum computers to enable fundamental breakthroughs in this domain. When we leap from bits to qubits, it could improve healthcare pharmaceutical research (4), which includes analyzing the folding of proteins, determining how molecular structures for instance drug and enzyme fit together (5), determining strengths of binding interactions between a single biomolecule for example protein or DNA to its ligand/binding partner like a drug or inhibitor. (6), and accelerating the process of clinical trials(7). A few potential applications are briefly described next for an illustration. A quantum computer can do extremely fast DNA sequencing, which opens the possibility for personalized medicine. It can enable the development of new therapies and medicines through detailed modeling. Quantum computers have the potential to create efficient imaging systems that can provide clinicians with enhanced fine-grained clarity in real-time. Moreover, it can solve complex optimization problems involved in devising an optimal radiation plan that is targeted at killing cancerous cells without damaging the surrounding healthy tissues. Quantum computing is set to enable the study of molecular interactions at the lowest possible level, paving the pathway to drug discovery and medical research. Whole-genome sequencing is a time-demanding task, but with the help of qubits, whole-genome sequencing and analytics could be implemented in a limited amount of time. Quantum computing can revolutionize the healthcare system through modern ways of enabling on-demand computing, redefining security for medical data, predicting chronic diseases, and accurate drug discoveries.

TABLE I: A comparison of this survey with related works.

References	Year	Healthcare Focus	Security	Privacy	Architectures	Quantum Requirements	Machine/Deep Learning	Applications
Gyongyosi et al. (8)	2019	✓	✓	✓	✓		✓	
Fernandez et al. (9)	2019	✓	✓	✓			✓	
Gyongyosi et al. (10)	2018			✓			✓	
Arunachalam et al. (11)	2017					✓		
Li et al. (12)	2020					✓		✓
Shaikh et al. (13)	2016			✓	✓	✓	✓	
Egger et al. (14)	2020			✓	✓	✓	✓	✓
Savchuk et al. (15)	2019			✓	✓	✓	✓	✓
Zhang et al. (16)	2019	✓	✓	✓	✓	✓	✓	✓
Mcgeoch et al. (17)	2019			✓	✓		✓	✓
Shanon et al. (18)	2020	✓	✓					
Duan et al. (19)	2020			✓	✓	✓	✓	✓
Preskill et al. (20)	2018	✓	✓	✓	✓	✓	✓	✓
Roetteler et al. (21)	2018	✓	✓	✓		✓	✓	
Upretyet al. (22)	2020			✓	✓	✓	✓	✓
Rowell et al. (23)	2018			✓	✓	✓		
Padamvathi et al. (24)	2016	✓	✓		✓	✓		
Nejatollahi et al. (25)	2019	✓	✓		✓	✓		
Cuomo et al. (26)	2020				✓	✓		
Fingeruth et al. (27)	2018				✓	✓		
Huang et al. (28)	2018		✓	✓	✓	✓		
Botsinis et al. (29)	2018		✓	✓	✓	✓		
Ramezani et al. (30)	2020				✓	✓	✓	
Bharti et al. (31)	2020				✓	✓	✓	✓
Abbott et al. (32)	2021	✓					✓	✓
Kumar et al. (33)	2021	✓			✓		✓	✓
Olgiati et al. (34)	2021	✓					✓	✓
Gupta et al. (35)	2022	✓				✓	✓	✓
Kumar et al. (36)	2022	✓						✓
Our Survey	2022	✓	✓	✓	✓	✓	✓	✓

C. Comparison with Related Surveys

As far as we understand this is the first survey on quantum computing that considers security and privacy implications, applications and architecture, quantum requirements and machine learning aspects of healthcare. There are some other surveys that consider a subset of these dimensions that merit discussion. Table I presents a comparative analysis of these surveys with the current work.

Gyongyosi et al. (8) discuss computational limitations of traditional systems and survey superposition and quantum entanglement-based solutions to overcome these challenges. However, this survey encompasses complex quantum mechanics without discussing its general-purpose implications for society. Fernández et al. (9) survey resource bottlenecks of IoT and discuss a solution based on quantum cryptography. They develop an edge computing-based security solution for IoT where management software is used to deal with security vulnerabilities. However, this is a domain-specific survey that only deals with security challenges. Gyongyosi et al. (10) discuss quantum channel capacities, which ease the quantum computing implementation for information processing. In this approach, conventional information processing is achieved through quantum channel capacities. Survey literature lists a few other quantum-computing works including quantum learning theories (11; 12), quantum information security (16; 18; 21; 24), quantum Machine Learning (ML) (30; 31), quantum data analytics (13; 22). These surveys are limited in their coverage of quantum computing applications. Some of the existing works analyze the impacts of quantum computing implementation. Huang et al. (28) analyze the implementation vulnerabilities in quantum cryptography systems. Botsinis et al. (29) discuss quantum search algorithms for wireless communication. Cuomo et al. (26) survey existing challenges and solutions for quantum distributed solutions and proposed a layered abstraction to deal with communication challenges. Many of these surveys are only tangentially related to healthcare or don't consider healthcare at all.

D. Contributions and organization

This survey systematically presents the evolution of quantum computing and its enabling technologies, explores the core application areas, and categorizes requirements for its implementation in high-performance healthcare systems along with highlighting security implications. In summary, the salient contributions of this survey are as follows:

TABLE II: List of acronyms and their explanation.

3GPP	Third-Generation Partnership Project
5G	Fifth Generation
ADD	Aptamers for Detection and Diagnostics
AI	Artificial Intelligence
DH	Diffie-Hellman
ECC	Elliptic Curve Cryptography
EHR	Electronic Health Records
IC	Integrated Circuit
IoT	Internet of Things
IT	Information Technology
ML	Machine Learning
MRI	Magnetic Resonance Imaging
NIST	National Institute of Standards and Technology
QAOA	Quantum Approximate Optimization Algorithm
QKD	Quantum Key Distribution
QoS	Quality of Service
Qubits	Quantum Bits
RSA	Rivest-Shamir Adleman
SDK	Software-Development Kits
TLS	Transport Layer Security
TSP	Traveling Salesman Problem
VLSI	Very Large Circuits Integration

1) We present the first comprehensive review of quantum computing technologies for healthcare covering its motivation, requirements, applications, challenges, architectures, and open research issues.
2) We discuss the enabling technologies of quantum computing that act as building blocks for the implementation of quantum healthcare service provisioning.
3) We have discussed the core application areas of quantum computing and analyzed the critical importance of quantum computing in healthcare systems.
4) We review the available literature on quantum computing and its inclination toward the development of future-generation healthcare systems.
5) We discuss key requirements of quantum computing systems for the successful implementation of large-scale healthcare services provisioning and the security implications involved.
6) We discuss current challenges, their causes, and future research directions for an efficient implementation of quantum healthcare systems.

This paper has been organized as follows. Table II shows acronyms and their definition. Section II discusses enabling technologies of quantum computing systems. Section III outlines the application areas of quantum computing. Section IV discusses the key requirements of quantum computing for its successful implementation for large-scale healthcare services provisioning. Section V provides a taxonomy and description of quantum computing architectural approaches for healthcare architectures. Section VI discusses the security architectures of the current quantum computing systems. Section VII discusses current open issues, their causes, and promising directions for future research. Finally, Section VIII concludes the paper.

II. Quantum Computing: History, Background, and Enabling Technologies

In this section, we present enabling technologies of quantum computing that support the implementation of modern quantum computing systems. Specifically, we categorize quantum computing enabling technologies in different domains, i.e., hardware structure, control processor plane, quantum data plane, host processor, quantum control and measurement plane, and qubit technologies.

A. Quantum Computing vs. Classical Computing

We refer the reader to Figure 2 for a differentiation of quantum computing paradigms with classical computing approaches in terms of their strengths, weaknesses, and applicability. Unlike conventional computers that operate in terms of bits, the basic units of operation in a quantum computer are referred to as quantum bits or *"qubits"* that posses two states or levels, i.e., it can represent a single bit in both '1' and '0' simultaneously. Quantum physical systems, which leverage the orientation of a photon and spin of an electron, are used to create qubits. We note that quantum computers can come in various varieties including one-qubit computer (37), two-qubit computer (38), and higher-qubit quantum computers. Key advancements in quantum computing were made earlier in 2000 when the very first 5-qubit quantum computed was invented (39). Since then many important advancements have been made so far and the best-known quantum computer of the current era is IBM's newest quantum-computing chip that contains 128 qubits (40). However, the literature suggests that the minimum number of qubits to realize quantum supremacy is 50 (41). Quantum supremacy is defined as the ability of a programmable quantum device, which is capable to solve a problem that cannot be solved by classical computers in a feasible amount of time (42). The behavior of qubits relates directly to the behavior of a spinning electron orbiting an atom's nucleus, which can demonstrate three key quantum properties: quantum superposition, quantum entanglement, and quantum interference (43).

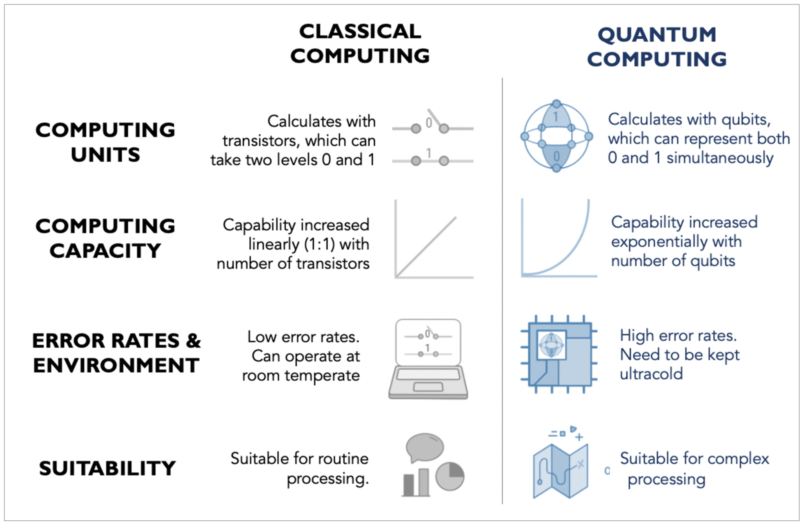

Fig. 2: Comparison of *Classical Computing vs. Quantum Computing*.

- The *quantum superposition* refers to the fact that a spinning electron's position cannot be pinpointed to any specific location at any time. On the contrary, it is calculated as a probability distribution in which the electron can exist at all locations at all times with varying probabilities. Quantum computers rely on quantum superposition in that they use a group of qubits for calculations and while classical computer bits may take on only states 0 and 1, qubits, can be either a 0 or 1, or a linear combination of both. These linear combinations are termed superposition states. Since a qubit can exist in two states, the computing capacity of a q-bit quantum computer grows exponentially in the form of 2^q.
- *quantum entanglement* takes place in a highly intertwined pair of systems such that knowledge of any one provides immediately provides information about the other regardless of the distance between them. This non-intuitive fact was described by Einstein as "spooky action at a distance" because it went against the rule information could never be communicated beyond light speed. Quantum entanglement in physics is when two systems such as photons or electrons are so highly interlinked that obtaining information about one's state like for example the direction of one electron's upword spin would provide instantaneous information about the other's state like for example the direction of the second electron's downward spin no matter how far apart they are. Modifying one entangled qubit's state therefore immediately perturbs the paired qubit's state in quantum computers. Thereby entanglement leads to the increased computational efficiency of quantum computers. Since processing one qubit provides knowledge about many qubits, doubling the number of qubits does not necessarily increase the number of entangled qubits. Quantum entanglement is therefore necessary for the exponentially faster performance of a quantum algorithm as compared to its classical counterpart.
- *Quantum interference* occurs because at the subatomic scale, particles have wavelike properties. These wavelike properties are often attributed to location, for example, where around a nucleus an electron might be. Two in-phase waves, which is to say they peak at the same time, constructively interfere, and the resulting wave peaks twice as high. Two waves that are out-of-phase, on the other hand, peak at opposite times and destructively interfere; the resulting wave is completely flat. All other phase differences will have results somewhere in between, with either a higher peak for constructive interference or a lower peak for destructive interference. In quantum computing, interference is used to affect probability amplitudes when measuring the energy level of qubits.

Quantum computing has applications in various disciplines including communication, image processing, information theory, electronics, cryptography, etc. Practical quantum algorithms are emerging with the increasing availability of quantum computers. Quantum computing possesses a significant potential to bring a revolution to several verticals such as financial modeling, weather precision, physics, and transportation (an illustration of salient verticals is presented in Figure 1). Quantum computing has already been used to improve different non-quantum algorithms being used in the aforementioned verticals. Moreover, the renewed efforts to envision physically-scalable quantum computing hardware have promoted the concept that a fully envisioned quantum paradigm will be used to solve numerous computing challenges considering its intractable nature with the available computing resources.

B. Brief History of Quantum Computing

The term quantum computing was first coined by Richard Feynman in 1981 and has since had a rich intellectual history. Figure 3 depicts a timeline of major events in this area. Noteworthy in the timeline is that while there were somewhat larger gaps between events earlier on, recently the field has started experiencing a more rapid series of developments. For example service providers have begun offering niche quantum computing products as well as quantum cloud computing services (e.g.,

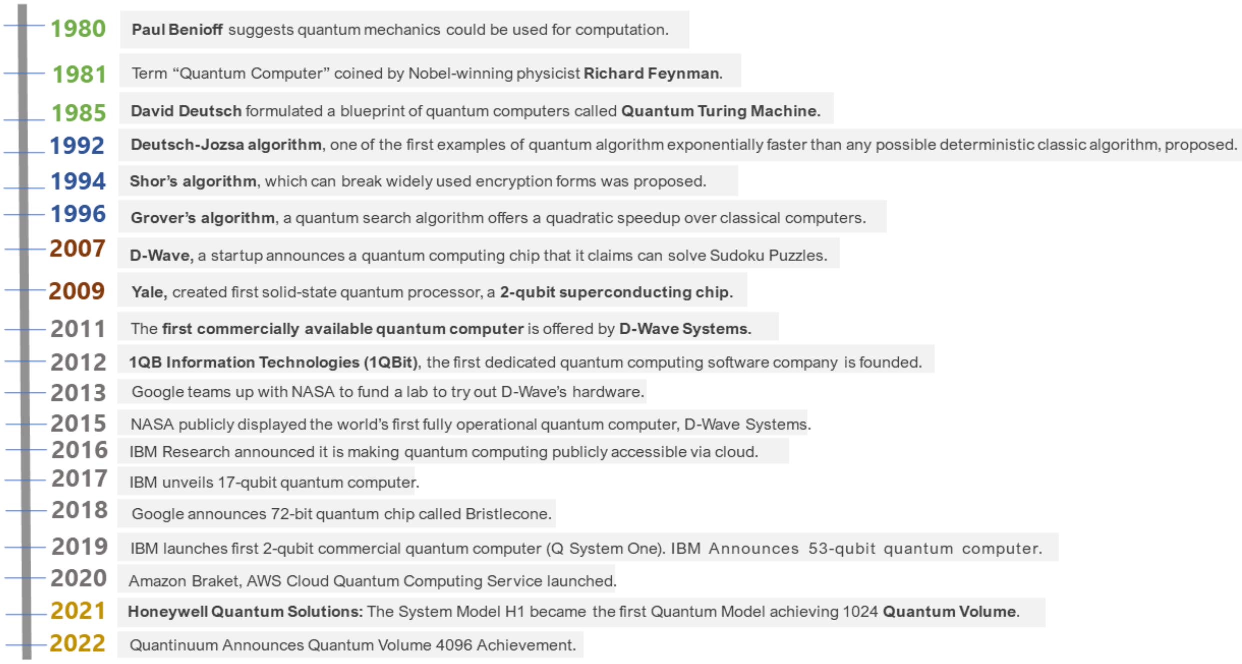

Fig. 3: *Timeline* of developments in quantum computing technology.

Amazon Braket). Recently, Google’s 54-qubit computer accomplished a task in merely 200 seconds that was estimated to take around over 10,000 years on a classical computing system (44). Nevertheless, quantum computing is still in its infancy stages and it will take some time before quantum computing chips reach desktops or handhelds. An important factor inhibiting the commoditization of quantum computing is the fact that controlling quantum effects is a delicate process and any noise (e.g. stray heat) can flip 1s or 0s and disrupt quantum effects such as superposition. This requires qubits to be fully operated under special conditions such as very cold temperatures, sometimes very close to absolute zero. This also motivates research exploring fault-tolerant quantum computing (45). Considering this fast-paced development of quantum computing, this is an opportune time for healthcare researchers and practitioners to investigate its benefits to healthcare systems.

C. Hardware Structure

Since quantum computer applications often deal with user data and network components that are part of traditional computing systems, a quantum computing system should ideally be capable of interfacing with and efficiently utilizing traditional computing systems. Qubits systems require carefully orchestrated control for efficient performance; this can be managed using conventional computing principles. An analogue gate-based quantum computing system could be mapped into various layers for building a basic understanding of its hardware components. These layers are responsible for performing different quantum operations; and consist of the quantum control plane, measurement plane, and data plane. The control processor plane uses measurement outcomes to determine the sequence of operations and measurements that are required by the algorithm. It also supports the host processor, which looks after network access, user interfaces, and storage arrays.

D. Quantum Data Plane

It is the main component of the quantum computing ecosystem. It broadly consists of physical qubits and the structures required to bring them into an organized system. It contains support circuits required to identify the state of qubits and performs gated operations. It does this for the gate-based system or controlling ”the Hamiltonian for an analog computer” (46). Control signals that are sent towards selected qubits set the Hamiltonian path thereby controlling the gate operations for a digital quantum computer. For gate-based systems, a configurable network is provided to support the interaction of qubits, while analog systems depend on richer interactions in qubits enabled through this layer. Strong isolation is required for high qubit fidelity. It limits connectivity as each qubit may not be able to directly interact with every other qubit. Therefore, we need to map computation to some specific architectural constraints provided by this layer. This shows that connection and operation fidelity are prime characteristics of the quantum data layer.

Conventional computing systems in which control and data plane are based on silicon technology. Control of the quantum data plane needs different technology and is performed externally by separating control and measurement layers. Analog qubits information should be sent to the specific qubits. Control information is transmitted through (data plane’s) wires electronically, in some of the systems. Network communication is handled in a way that it retains high specificity affecting only the desired qubits without influencing other qubits that are not related to the underlying operation. However, it becomes challenging when the number of qubits grows; therefore, the number of qubits in a single module is another vital part of the quantum data plane.

E. Quantum Control and Measurement Plane

The role of the quantum plane is to convert digital signals received from the control processor. It defines a set of quantum operations that are performed in the quantum data plane on the qubits. It efficiently translates the data plane's analog output of qubits to classical data (i.e. binary), which is easier to be handled by the control processor. Any difference in the isolation of the signals leads to small qubit signals that cannot be fixed during an operation thus resulting in inaccuracies in the states of qubits. Control signals shielding is complex since such signals must be passed via the apparatus that is used for isolating the quantum data plane from the environment. This could be done using vacuum, cooling, or through both required constraints. Signal crosstalk and qubit manufacturing errors gradually change with the configuration change in the system. Even if the underlying quantum system allows fast operations, the speed can still be limited by the time required to generate and send a precise pulse.

F. Control Processor Plane and Host Processor

This plane recognizes and invokes a series of quantum-gate operations to be performed by the control and measurement plane. These set of steps implement a quantum algorithm via the host processor. The application should be custom-built using specific functionalities of the quantum layer that are being offered by the software tool stack. One of the critical responsibilities of the control processor plane is to provide an algorithm for quantum error correction. Conventional data processing techniques are used to perform different quantum operations that are required for error correction according to computed results. This introduces a delay that may slow down the quantum computer processing. The overhead can be reduced if the error correction is done in a comparable time to that of the time needed for the quantum operations. As the computational task increases with the machine size, the control processor plane would inevitably consist of more elements for increasing computational load. However, it is quite challenging to develop a control plane for large-scale quantum machines.

One technique to solve these challenges is to split the plane into components. The first component being a regular processor can be tasked to run the quantum program, while the other component can be customized hardware to enable direct interaction with the measurement and control planes. It computes the next actions to be performed on the qubits by combining the controller's output of higher-level instructions with the syndrome measurements. The key challenge is to design customized hardware that is both fast and scalable with machine size, as well as appropriate for creating high-level instruction abstraction. A low abstraction level is used in the control processor plane. It converts the compiled code into control and measurement layer commands. The user will not be able to directly interact with the control processor plane. Subsequently, it will be attached to that computing machine to fasten the execution of a specific few applications. Such kind of architectures have been employed in current computers that have accelerators for graphics, ML, and networking. These accelerators typically require a direct connection with the host processors and shared access to a part of their memory, which could be exploited to program the controller.

G. Qubit Technologies

Shor's algorithm (47) opened the gate to possibilities for designing adequate systems that could implement quantum logic operations. There are two types of qubit technologies including trapped-ion qubits and superconducting qubits.

1) Trapped Ion Qubits: "The first quantum logic gate was developed in 1995 by utilizing trapped atomic ions" that were developed using a theoretical framework proposed in the same year (48). After its first demonstration, technical developments in qubit control have paved the way toward fully functional processors of quantum algorithms. The small-scale demonstration has shown promising results; however, trapped ions remain a considerable challenge. As opposed to Very Large Circuits Integration (VLSI), developing a trapped-ion based quantum computer requires the integration of a range of technologies including optical, radiofrequency, vacuum, laser, and coherent electronic controllers. However, the integration challenges associated with trapped-ion qubits must be thoroughly addressed before deploying a solution.

A data plane consists of ions and a mechanism to trap those into desired positions. The measurement and control plane contains different lasers to perform certain operations, e.g., a precise laser source is used for inflicting a specific ion to influence its quantum state. Measurements of the ions is captured through a laser, and the state of ions is detected through photon detectors.

2) Superconducting Qubits: Superconducting qubits share some common characteristics with today's silicon-based circuits. These qubits when cooled show quantitative energy-levels due to quantified states of electronic-charge. The fact that they operate at nanosecond-time scale, continuous improvement in coherence times, and ability to utilize lithographic scaling make them an efficient solution for quantum computing. Upon the convergence of these characteristics, superconducting qubits are considered both for quantum computation and quantum annealing.

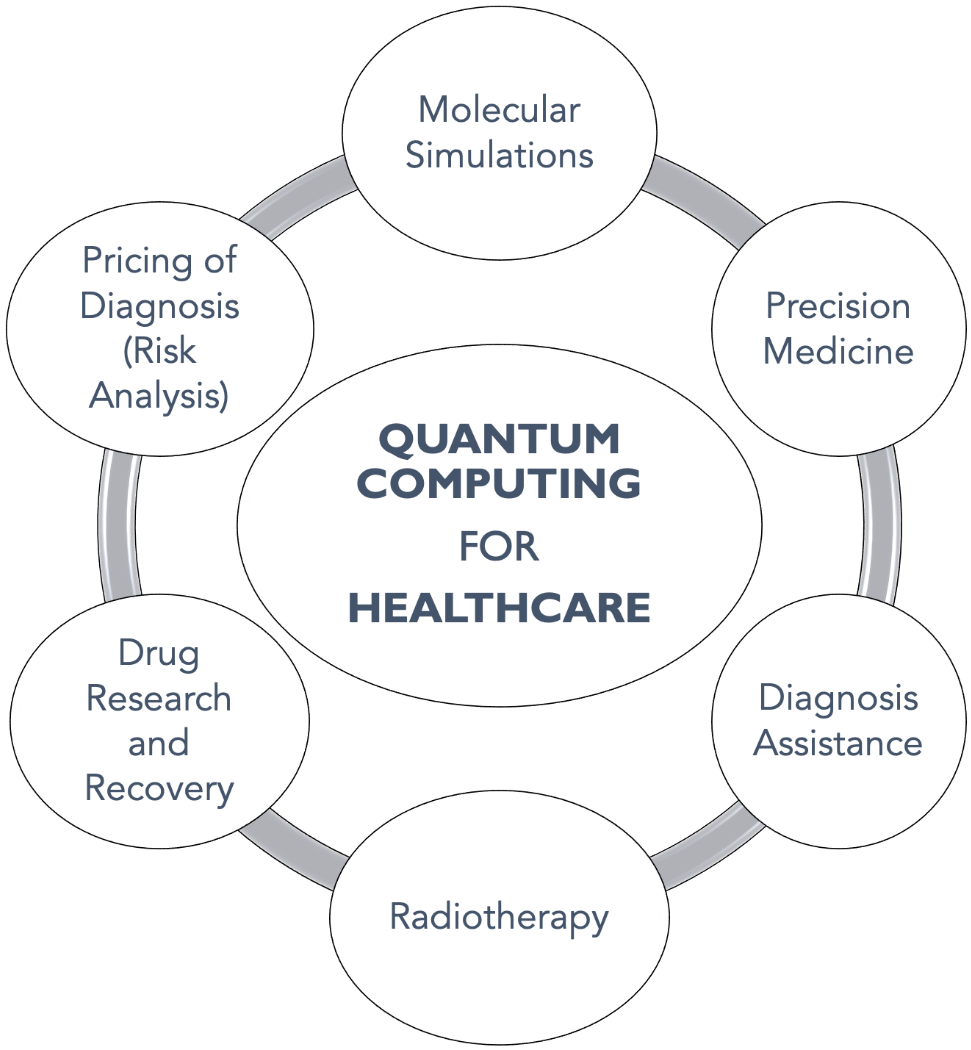

Fig. 4: Applications of *Quantum Computing for Healthcare*.

H. Lessons Learned: Summary and Insights

In this section, we discussed enabling technologies of quantum computing. We found that the key characteristics of a quantum data plane are the error rates of the single and two-qubit gates. Furthermore, qubit coherence times, interqubit connection, and the qubits within a single module are vital in the quantum data plane. We also explained that the quantum computer's speed is limited by the precise control signals that are required to perform quantum operations. The control processor plane and host computer run a traditional OS equipped with libraries for its operations that provides software development tools and services. It runs the software development tools that are essential for running the control process. These are different from the software that runs on today's conventional computers. These systems provide capabilities of networking and storage that a quantum application might require during execution. Thus connecting a quantum process to a traditional computer enables it to leverage its all features without getting started from scratch.

III. Applications of Quantum Computing for Healthcare

Recent research shows that quantum computing has a clear advantage over classical computing systems. Quantum computing provides an incremental speedup of disease diagnosis and treatment, and in some use cases can drastically reduce the computation times from years to minutes. It provokes innovative ways of realizing a higher level of skills for certain tasks, new architectures, and strategies. Therefore, quantum computing has an immense potential to be employed for a wide variety of use cases in the health sector in general and for healthcare service providers in particular, especially in the areas of accelerated diagnoses, personalized medicine, and price optimization. Literature survey shows that there is a visible increase in the use of classical modeling and quantum-based approaches, primarily due to the improvement in access to worldwide health-relevant data sources and availability. This section brings forward some potential use cases for the applications of quantum computing in healthcare, an illustration of these use cases is presented in Figure 4.

A. Molecular Simulations

Quantum computers tend to process data in a fundamentally novel way using quantum bits as compared to classical computing where integrated circuits determine the processing speed. Quantum computers unlike storing information in terms of 0s and 1s, use the phenomena of quantum entanglement, which paves the way for the quantum algorithms countering classical computing which is not designed to benefit from this phenomenon. In the healthcare industry, quantum computers can exploit ML, optimization, and Artificial Intelligence (AI) to perform complex simulations. Processes in healthcare often consist of complex correlations and well-connected structures of molecules with interacting electrons. The computational requirements for simulations and other operations in this domain naturally grow exponentially with the problem size, while time always being the limiting factor. Therefore we argue, that quantum computing based systems are a natural fit for the use case.

B. Precision Medicine

The domain of precision medicine focuses on providing prevention and treatment methodologies for individuals' healthcare needs. Due to the complexity of the human biological system, personalized medicine will be required in the future that will go beyond standard medical treatments. Classical ML has shown effectiveness in predicting the risk of future diseases using EHRs. However, there are still limitations in using classical ML approaches due to quality and noise, feature size, and the complexity of relations among features. It provokes the idea of using quantum-enhanced ML, which could facilitate more accurate and granular early disease discovery. Healthcare workers may then use tools to discover the impact of risks on individuals in a given condition changes by continual virtual diagnosis based on continuous data streams. Drug sensitivity is an ongoing research topic at a cellular level considering genomes features of cancer cells. Ongoing research discovers the chemical properties of drug models that could be used for predicting cancer efficiency at a granular level. Quantum-enhanced ML could expedite breakthroughs in the healthcare domain mainly by enabling drugs inference models.

Precision medicine has the goal of identifying and explaining relationships among causes and treatments and predicting the next course of action at an individual level. Traditional diagnosis based on the patient's reported symptoms results in umbrella diagnosis where the related treatments tend to fail sometimes. Quantum computing could help in utilizing continuous data streams using personalized interventions in predicting diseases and allowing relevant treatments. Quantum-enhanced predictive medicine optimizes and personalizes healthcare services using continuous care. Patient adherence and engagement at the individual-level treatments could be supported by quantum-enhanced modeling. A use case of quantum computing-based precision medicine is illustrated in Figure 5.

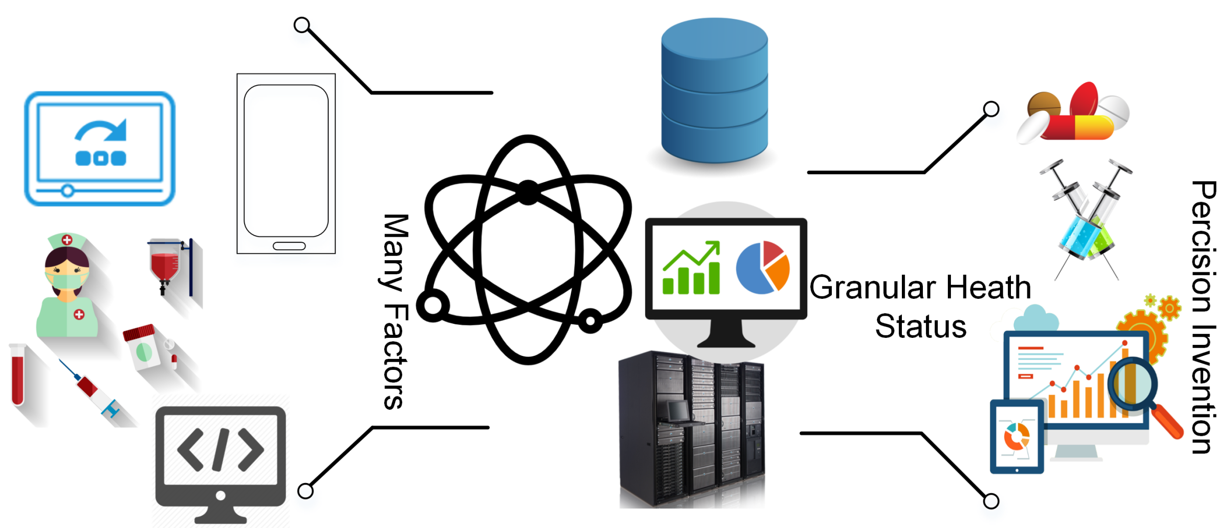

Fig. 5: *Precision medicine* using quantum computing.

C. Diagnosis Assistance

Early diagnosis of the diseases could render better prognosis, treatment, and lower the healthcare cost. For instance, it has been shown in the literature that the treatment cost lowers by a factor of 4 whereas the survival rate could be decreased "by a factor of 9 when the colon cancer is diagnosed at an early stage" (49). In the meantime, the current diagnostics and treatment for most of the diseases are costly and slow having deviations in the diagnosis of around 15-20% (50). The use of X-rays, CT scans, and MRIs has become critical over the past few years with computer-aided diagnostics developing at a faster pace. In this situation, diagnoses and treatment suffer from noise, data quality, and replicability issues. In this regard, quantum-assisted diagnosis has the potential to analyze medical images and oversee the processing steps such as edge detection in medical images, which improves the image-aided diagnosis.

The current techniques use single-cell methods for diagnosis, while analytical methods are needed in single-cell sequencing data and flow cytometry. These techniques further require advanced data analytic methods particularly combining datasets from different techniques. In this context, cell classification on the basis of biochemical and physical attributes is regarded as one of the main challenges. While this classification is vital for critical diagnoses such as cancerous cells integration from healthy cells, it requires an extended feature space where the predictor variable becomes considerably larger. Quantum ML techniques such as quantum vector machines (QVM) enable such classifications and enable single-cell diagnostic methods. The discovery and characterization of biomarkers pave the way for the study of intricate omics datasets such as metabolomics, transcriptomics, proteomics, and genomics. These processes could lead to increased feature space provoking complex patterns and correlations which are near-impossible to be analyzed using classical computational methodologies.

During the diagnosis process, quantum computing may help to support the diagnostics insights eliminating the need for repetitive diagnosis and treatment. This paradigm helps in providing continuous monitoring and analysis of individuals' health. It also helps in performing meta-analysis for cell-level diagnosis to determine the best possible procedure at a specific time. This could help to reduce the cost and allow extended data-driven diagnosis, bringing value for both the medical practitioners and individuals.

D. Radiotherapy

Radiation therapy has been employed for the treatment of cancers, which uses radiation beams to eliminate cancerous cells to stop them from multiplication. However, radiotherapy is a sensitive process, which requires highly precise computations to drop the beam on the cancer-causing tissues and avoid any impact on the surrounding healthy body cells. Radiography is performed using highly precise computers and involves a highly precise optimization problem to perform the precise radiography operation, which requires multiple precise and complex simulations to reach an optimal solution. Through Quantum computing running simultaneous simulations and figuring out a plan in an optimal time becomes possible, and hence the spectrum of opportunities is very vast if quantum concepts are employed for simulations.

E. Drug Research and Discovery

Quantum computing enables medical practitioners to model atomic-level molecular interactions, which is necessary for medical research. This will be particularly essential for diagnosis, treatment, drug discovery, and analytics. Due to the advancements in quantum computing, it is now possible to encode tens of thousands of proteins and simulate their interactions with drugs, which has not been possible before. Quantum computing helps process this information at orders of magnitude more effectively as compared to conventional computing capabilities. Quantum computing allows doctors to simultaneously compare large collections of data and their permutations to identify the best patterns. Detection of biomarkers specific to a disease in the blood is now possible through gold-nanoparticles by using known methods such as bio-barcode assay. In this situation, the goal could be to exploit the comparisons used to help the identification of a diagnosis.

F. Pricing of Diagnosis (Risk Analysis)

Creating pricing strategies is considered one of the key challenges that contribute to the complexities of the healthcare ecosystem. In pricing analysis, quantum computing helps in risk analysis by predicting the current health of patients and predicting whether the patient is prone to a particular disease. This is useful for optimizing insurance premiums and pricing (1). A population-level analysis of disease risks, and mapping that to the quantum-based risk models could help in computing financial risks and pricing models at a finer level. One of the key areas which could support pricing decisions is the detection of fraud where healthcare frauds cause billions of dollars of revenue. In this regard, traditional data mining techniques offer insights into detecting and reducing healthcare fraud. Quantum computing could provide higher classification and pattern detection performance thus uncovering malicious behavior attempting fraudulent medical claims. This could in turn help in better management of pricing models and lowering the costs associated with frauds. Quantum computing can substantially accelerate pricing computations as well, resulting in not only lowering the premiums but also in developing customized plans.

G. Lessons Learned: Summary and Insights

Different tests and systems, based on historical data, MRIs, CT scans etc could possibly become one of the quantum computing applications. Quantum computing could help in performing DNA sequencing which takes 2-3 months using classical computing. It could also help perform cardiomyopathy analysis for DNA variants promptly. Although the growth of quantum computing brings novel benefits to healthcare, the broad use of novel quantum techniques may provoke security challenges. Therefore, there is a need to invest in quantum computing for better healthcare services provisioning. Furthermore, vaccine research could be automated more efficiently. Moreover, there is a need to allocate the distributed quantum computing where a quantum supercomputer distributes its resources using the cloud.

TABLE III: A summary of key requirements of quantum computing for healthcare services provisioning along with different challenges and solutions.

Requirements	Challenges	Solutions
Computational power	• Lower computational power of traditional systems. • Higher computational complexity. • Large problem sizes. • Complex implementation.	• Multi-dimensional spaces of quantum computers. • Efficient representation of larger problems. • Quantum wave interference. • Unprecedented speed of quantum computing.
High-Speed Connectivity (5G/6G Networks)	• Lack of security. • Lack of scalability. • Lack of confidentiality. • Lack of integrity.	• Quantum walks-based universal computing model. • Inherent cryptographic features of quantum computing. • Cryptographic protocols. • Qantum-based authentication.
Higher dimensional quantum computing	• Growing number of quantum states. • Lower capacity in traditional systems. • Lack of resources. • Increased processing requirements.	• Quantum Hilbert states. • Increased noise resilience. • Quantum channel implementation. • Parallel execution of tasks.
Scalability of quantum computing	• Lack of scalability. • Lack of resuability. • Lack of support for growing amount of processing. • Lack of emulation environments.	• Transfer learning methods. • Use of neural Boltzmann machines. • Physics-inspired transfer-learning protocols. • FPGA-based quantum computing applications.
Fault-tolerance.	• Lack of fault-tolerance. • Quantum entangled states. • Errors in qubits. • Lack of quantum correction code.	• Monitoring qubits using ancillary qubit. • Logical errors detection. • Error-identification code. • Limiting error propagation.
Quantum Availability of the Healthcare Systems	• Far away processing systems. • Errors in the communication systems. • Lack of computing infrastructure. • Lack of service distribution.	• Communication infrastructure improvement. • Fault correction mechanisms • Development of quantum services. • Improvement in traditional computing systems.
Deployment of Quantum Gates	• No cloning restriction. • Challenges with coupling topology. • Combinatorial optimization problems. • Lack of error correction code.	• Use of gate-model quantum computers. • Programming gated-models. • Shor's factoring algorithm. • Performance of factorization process.
Use of Distributed Topologies	• Physical distances among quantum states. • Latency on quantum bus execution. • Requirement of coordinated infrastructure. • Lack of system area network.	• Development of distributed quantum technologies. • Efficient quantum bus implementation. • Feed forward quantum neural networks. • Dipole-dipole interaction.
Requirements for Physical Implementation	• Higher implementation cost. • Lack of resources. • Lack of expertise. • Lower revenue.	• Physical systems development. • Cost-effective solutions. • Manpower training. • Cost-effective solutions.
Quantum ML	• Extended execution time. • Lack of resources. • Higher complexity. • More implementation overhead.	• Quantum computing based solutions. • Lower computational complexity. • Higher responsiveness. • Efficient implementation.

IV. Requirements of Quantum Computing for Healthcare

Quantum-enhanced computing can decrease processing time in various healthcare applications. However, the requirements of quantum computing for healthcare could not be generalized across different applications. For instance, drug discovery requirements are different from vaccination development systems. Therefore, quantum computing applications in healthcare require consideration of multiple factors for effective implementation. Table III outlines the requirements of quantum computing for a successful operation of healthcare systems and are elaborated below.

A. Computational Power

Low computational time is one of the major requirements of any healthcare application. The classical computers having CPUs and GPUs are not capable of solving certain complex healthcare problems, e.g., simulating molecular structures. This motivates the need for using quantum computing that can exploit vast amounts of multidimensional spaces to represent large problems. A prominent example illustrating the power of quantum computing can be seen in Grover's Search algorithm (51), which used to search from a list of items. For instance, if we want to search a specific item in N number of items, we have to search $\frac{N}{2}$ items on average or in the worst case check all N items. Grover's search algorithm searches all these items by checking $\sqrt{n}$ items. This demonstrates remarkable efficiency in computational power. Let's assume we want to search from 1 trillion items and every item takes 1 microsecond to check, it will take only 1 second for a quantum computer.

B. High-Speed Connectivity (5G/6G Networks)

Fifth-generation (5G) has become an essential technology connecting smart medical objects. It provides extremely robust integrity, lower latency, higher bandwidth, and has an extremely large capacity. IoT objects work by transferring data to edge/cloud infrastructure for processing. Cloud storage suffers from security issues from users' perspective thus raising novel challenges associated with the availability, integrity, and confidentiality of data. Quantum computing can gain benefits from 5G/6G networks to provide novel services. Quantum walks deliver a universal processing model and inherent cryptographic features to deliver efficient solutions for the healthcare paradigm. Quantum walks are the mechanical counterpart of traditional random walk that allows to develop novel quantum algorithms and protocols using high-speed 5G/6G network.

A few examples of using quantum walks for designing secure quantum applications include pseudo-random number generators, substituting boxes, quantum-based authentication, and image encryption protocols. This could help in providing secure ways to store and transmit data using high-speed networks. A cryptography mandate for secure transmission of information, the entity's data is encrypted before sending it over the cloud. In this context, key management, encryption, decryption, and access control are taken care of by the entities. This could be novel research exploiting quantum technologies using 5G healthcare to enhance performance and resist attacks from classical and quantum scenarios.

C. Quantum Communications Networks

Quantum communication (QC) is a quantum technologies subbranch that concerns the distribution of quantum states of light for accomplishing a particular communication task (52; 53). The potential use of QC in commercial applications has been gaining popularity recently. Two leading technologies of QC include Quantum key distribution (QKD) and quantum random-number generation (QRNG). QKD enables private communication by allowing remote entities to share a secret key and together these promise to enable the perfect secrecy protocol to provide resistance to external attacks. The goal of the quantum internet (54; 55) is to develop a quantum communication network that connects quantum computers together to achieve quantum-enhanced network security, synchronization, and computing. Qirg is an IETF quantum internet research group that is responsible for The standardization process of the quantum internet.

D. Higher Dimensional Quantum Communication

Quantum information has been strongly influenced by modern technological paradigms. Literature shows that high-dimensional quantum states are of increasing interest, especially with respect to quantum communication. Hilbert space provides numerous benefits such as large information capacity and noise resilience (56). Moreover, the authors in (56), explored "multiple photonic degrees of freedom for generating high-dimensional quantum states" using both integrated photonics and bulk optics. Different channels were spun up for propagation of the quantum states, e.g., single-mode, free-space links, aquatic channels, and multicore and multimode fibers.

E. Scalability of Quantum Computing

Highly connected quantum states that are continuously interacting are challenging to simulate considering their many-body Hilbert vector space that increases with the growing number of particles. One of the promising methods to improve scalability is using the methods of transfer learning. It dictates reusing the capability of ML models to solve potentially similar but different class of problems. By reusing features of the neural network quantum states, we can exploit physics-inspired transfer learning protocols.

It has been verified that even simple neural networks (i.e. Boltzmann machines (57)) can precisely imitate the state of many-body quantum systems. Transfer learning uses the same trained model to be used for another task that is trained from a similar system with a larger size. In this regard, various physics-inspired protocols can be used for transfer learning to achieve scalability. FPGAs can also be used to emulate quantum computing algorithms providing higher speed as compared to software-based simulations. However, required hardware resources to emulate quantum systems become a critical challenge. In this regard, scalable FPGA-based solutions could provide more scalability.

F. Fault-Tolerance

Fault tolerance in quantum computers is extremely necessary as the components are connected in a fragile entangled state. It makes quantum computers robust and introduces ways to solve quantum problems leading to the high fidelity of quantum computations. This allows quantum computers to perform computations that were challenging to process in traditional computing. However, during processing, any error in qubit or in the mechanism of measuring the qubit will bring devastating consequences for the systems depending on those computations. The system of correcting errors itself suffers from major issues. A feasible way of monitoring these systems is to monitor qubits using ancillary qubits, which constantly analyze the logical errors for corrections and detection. Ancillary qubits have already shown promising results but errors themselves in ancillary qubits may lead to errors in qubits thereby inflicting more errors in the operation. Error correction code could be embedded among the qubits allowing the system to correct the code when some bits are wrong. It helps in faulty error propagation by ensuring that a single faulty gate or time stamp produces a single faulty gate.

G. Quantum Availability of the Healthcare Systems

In traditional systems, computing is performed in the close proximity of the devices. However, quantum computers are located far away from users' locality. If you want to share a virtual machine hosted on a quantum computer, it's challenging to access such a virtual machine, therefore, the availability requirements of quantum computers should be addressed carefully.

H. Deployment of Quantum Gates

One of the requirements in layered quantum computing is the deployment of quantum gates. In this scenario, each quantum gate has the responsibility to perform specific operations on the quantum systems. Quantum gates are applied in multiple quantum computing applications due to ”hardware restrictions such as the no-cloning theorem makes it challenging for a given quantum system to coordinate in greater than one quantum gate simultaneously” (58). In this paradigm, the requirement of coupling topology arises, qubit-to-qubit coupling is one such example where the circuit-depth relies on the fidelity of the involved gates.

Paler et al. (59) proposed Quantum Approximate Optimization Algorithm (QAOA), which solves the challenge of combinatorial optimization problems. In this technique, the working mechanism depends on the positive integer, which is directly related to the quality of the approximation. Farhi et al. (60) applied QAOA using a set of linear equations containing exactly three Boolean variables. This algorithm brings different advantages over traditional algorithms, and efficiently solves the input problem. In (61), the authors used gate-model quantum computers for QAOA. This algorithm converges to a combinatorial optimization problem as input and provides a string output satisfying a higher ”fraction of the maximum number of clauses”. Farhi et al. (62) proposed QAOA for fixed qubit architectures that provides a method for programming gate-model without considering requirements of error correction and compilation. The proposed method uses a sequence of unitaries that reside on the qubit-layout generating states. Meter et al. (63) developed a blueprint of a multi-computer using Shor's factoring algorithm (64). A quantum-based multicomputer is designed using a quantum bus and nodes. The primary metric was the performance of the factorization process. Several optimization methods make this technique suitable for reducing latency and the circuit path.

I. Use of Distributed Topologies

Large-scale quantum computers could be realized by distributed topologies due to physical distances among quantum states. A quantum bus is deployed for the communication of quantum computers where quantum algorithms (i.e. error correction) are run in a distributed topology. It requires a coordinated infrastructure and a communication protocol for distributed computation, communication, and quantum error correction for quantum applications. A system area networks model is required to have arbitrary quantum hardware handled by communication protocols.

Van Meter et al. (65) performed an experimental evaluation of different quantum error correction models for scalable quantum computing. Ahsan et al. (66) proposed a million qubit quantum computer suggesting the need ”for large-scale integration of components and reliability of hardware technology using” simulation and modeling tools. In (67), the authors proposed quantum generalization for feedforward neural networks showing that the classical neurons could be generalized with the quantum case with reversibility. The authors demonstrate that the neuron module can be implemented photonically thus making the practical implementation of the model feasible. In (68), the authors present an idea of using quantum dots for implementing neural networks through dipole-dipole interactions and showed that the implementation is versatile and feasible.

J. Requirements for Physical Implementation

The current implementation of quantum computers can be grouped into four generations (65). The first-generation quantum computers could be implemented by ion traps where KhZ represents physical speed and Hz shows the logical speed having footprints in the range of mm-cm (66; 69; 70; 71; 72; 73; 74). Second-generation quantum computers can be implemented by distributed-diamonds, superconducting quantum circuits, and linear optical strategies. The physical speed of these computers ranges from MhZ whereas logical speed constitutes in kHz range having a footprint size of $-mm$. The third generation quantum computers are based on monolithic-diamonds, donor, and quantum dot technologies. Their logical speed corresponds to MHz while physical speed ranges in GHz having a footprint size of $-um$. Topological quantum computing is used in fourth-generation quantum computers in the evolutionary stage. This generation of quantum computers does not need any quantum error correction having natural protection of decoherence. In order to address an open problem of enabling distributed quantum-computing via anionic particles, Monz et al. (75) propose a practical realization of the scalable Shor algorithm on quantum computers. This work does not discuss the algorithm's scalability and mainly demonstrates various implementations of factorization algorithm on multiple architectures.

K. Quantum Machine Learning

Quantum AI and quantum ML are emerging fields; therefore, requirements analysis of both fields from the perspective of experimental quantum information processing is necessary. Lamata (76) studied the implementation of basic protocols using superconducting quantum circuits. Superconducting quantum circuits are implemented for realizing computations and quantum information processing. In (77), the authors proposed a quantum recommendation system, which efficiently samples from a preference-matrix, that does not need a matrix reconstruction. Benedetti et al. (78) proposed a classical quantum DL architecture for near-term industrial devices. The authors presented a hybrid quantum-classical framework to tackle high-dimensional real-world ML datasets on continuous variables. In their proposed approach, DL is utilized for low dimensional binary data. This scheme is well-suited for small-scale quantum processors, and mainly for training unsupervised models.

L. Lessons Learned: Summary and Insights

In this section, we present novel requirements of healthcare systems implementation using quantum computing. Quantum computing for healthcare requires consideration of the diverse requirements of different infrastructures. Therefore, an effective realization of quantum healthcare systems requires healthcare infrastructure to be upgraded to coordinate with the high computational power provided by quantum computing.

V. Quantum Computing Architectures for Healthcare

This section presents an overview of existing literature focused on developing quantum computing architecture for healthcare applications. We start this section by first providing a brief overview of general quantum computing architecture.

A. Quantum Computing Architecture: A Brief Overview

Different components of quantum computing are integrated to form a quantum computing architecture. The basic elements of a classical quantum computer are its quantum states (i.e., qubits), the architecture used for fault tolerance and error correction, the use of quantum gates and circuits, the use of quantum teleportation, and the use of solid-state electronics (79), etc. The design and analysis of these components and their different architectural combinations have been widely studied in the literature. For instance, most of the proposed/developed quantum computing architectures are layered architecture (80; 81), which is a conventional approach to the design of complex information engineering architectures. So far many researchers have provided different perspectives and guidelines to design quantum computer architectures (82; 83). For instance, the fundamental criteria for viable quantum computing were introduced in (84) and the need for a quantum error correction mechanism within the quantum computer architecture is emphasized in (85; 86). (87) presents a comparative analysis of IBM Quantum vs fully connected trapped-ions.

TABLE IV: A comparison of the existing quantum computing literature on healthcare using different performance parameters.

Technique	Healthcare	Security	Performance	Sacalability	IoT	Key Feature
Liu et al. (88)	✓	×	✓	×	×	Logistic regression
Janani et al. (89)	✓	✓	✓	×	✓	Blockchain
Qiu et al. (90)	×	✓	✓	✓	×	Digital signature
Helgeson et al. (91)	✓	×	×	×	×	Survey
Latif et al. (92)	✓	✓	✓	✓	×	Quantum walks
Bhavin et al. (93)	✓	✓	×	✓	✓	Blockchain
Javidi (94)	✓	×	✓	×	×	3D images visualization
Childs (95)	✓	×	✓	×	×	Cloud computing
Perumal et al. (96)	✓	✓	×	×	×	Qubits quantum
Latif et al. (97)	✓	✓	×	×	×	Quantum watermarking
Hastings (98)	✓	×	×	×	×	Literature review
Grady et al. (99)	×	×	×	×	×	Quantum leadership
Datta et al. (100)	✓	×	✓	×	✓	Smartphone app
Koyama et al. (101)	✓	×	✓	✓	✓	High-speed wavelet
Narseh et al. (102)	✓	×	✓	✓	✓	DH extension

B. Quantum Computing for Healthcare

Different quantum computing based approaches can be noted in the literature. For instance, Liu et al. (88) proposed a logistic regression health assessment model using quantum optimal swarm optimization to detect different diseases at an early stage. Javidi (94) studies various research works that use 3D approaches for image- visualization and quantum imaging under photon-starved conditions and proposes a visualization. Childs et al. (95) proposed a study using cloud-based quantum computers exploiting natural language processing on electronic healthcare data. Datta et al. (100) proposed "Aptamers for Detection and Diagnostics (ADD) and developed a mobile app acquiring optical data from conjugated quantum nanodots to identify molecules indicating" the presence of the SARS-CoV-2 virus. Koyama et al. (101) proposed a mid-infrared spectroscopic system using a pulsed quantum cascade laser and high-speed wavelength-swept for healthcare applications, e.g., blood glucose measurement. Naresh et al. (102) proposed a quantum DH extension to dynamic quantum group key agreement for multi-agent systems-based e-healthcare applications in smart cities.

C. Secure Quantum Computing for Healthcare

Janani et al. (89) proposed quantum block-based scrambling and encryption for telehealth systems (image processing application), their proposed approach has two levels of security that works by selecting an initial seed value for encryption. The proposed system provides higher security against statistical and differential attacks. However, the proposed system produces immense overhead during complex computations of quantum cryptography. Qiu et al. (90) proposed a quantum digital signature for the access control of critical data in the big data paradigm that involves signing parties including the signer, the arbitrator, and the receiver. The authors did not propose a new quantum computer rather they implemented a quantum protocol that does not put more overhead on the network. However, this scheme does not consider sensitive data transferred from the source to the destination during the proposed quantum computing implementation. Al-Latif et al. (92) proposed a quantum walk-based cryptography application, which is composed of substitution and permutations.

In a recent study (93), a hybrid framework based on blockchain and quantum computing is proposed for an electronic health record protection system, where blockchain is used to assign roles to authorize entities in the network to access data securely. However, the performance of the proposed system suffers as the quantum computing and blockchain infrastructure pose immense network overhead. Therefore, the performance of the proposed system should be assessed intuitively before its actual deployment. Latif et al. (97) proposed two novel quantum information hiding techniques, i.e., a steganography approach and a quantum image watermarking approach. The quantum steganography methodology hides a quantum secret image into a cover image using a controlled-NOT gate to secure embedded data and the quantum watermarking approach hides a quantum watermarking gray image into a carrier image. Perumal et al. (96) propose a quantum key management scheme with negligible overhead. However, this scheme lacks a comparison with the available approaches to demonstrate its efficacy.

D. Actual Clinical Deployment of Quantum Computing

Helgeson et al. (91) explored the impact of clinician-awareness of quantum physics principles among patients and healthcare service providers and show that the principles of physics improve communication in the healthcare paradigm. However, this study is based on survey-based analysis, which did not provide an actual representation of the quantum healthcare implementation paradigm. An implementation level study should be conducted based on the findings of this research to identify its implications. Similarly, Hastings et al. (98) suggested that healthcare professionals must be aware of the fact that quantum computing involves extensive mathematical understanding to ensure efficient services of quantum computing in healthcare applications. Similarly, Grady et al. (99) suggested that leadership in the quantum age requires engaging with stakeholders and resonating with creativity, energy, and products of the work that results from the mutual efforts enforced by the leaders. On a similar note, we argue that the quantum computing architecture for healthcare applications should be developed by considering the important requirements that we have identified in this paper (which are discussed in detail in Section IV and are summarized in Table III).

E. Lessons Learned: Summary and Insights

In summary, this section discusses state-of-the-art quantum computing healthcare literature. Table IV shows a comparison of the available approaches in terms of different parameters. We defined key parameters based on quantum computing usage in the healthcare paradigm. Most of the existing studies do not consider IoT implementation in the quantum healthcare paradigm. Therefore, there is a need for IoT implementation in healthcare due to its greater implication in healthcare services provisioning.

VI. Security of Quantum Computing for Healthcare

As healthcare applications are essentially life-critical, therefore, ensuring their security is fundamentally important. However, a major challenge faced by healthcare researchers is the siloed nature of healthcare systems that impedes innovation, data sharing, and systematic progress (103). Furthermore, Chuck Brooks a leader in cybersecurity and chair in the Quantum Security Alliance, suggests that effective implementation of security should allow academia, industry, researchers, and governments to collaborate effectively (104). Security of a quantum computing system is also very important as it can enable exponential upgradation of computing capacities, which can put at risk current cryptographic-based approaches. Whereas, cryptography has been considered as the theoretical basis for healthcare information security. Quantum computing using cryptography exploits the combination of classical cryptography and quantum mechanics to offer unconditional security for both sides of the healthcare communication among healthcare services consumers. Quantum cryptography has become the first commercially available use case of quantum computing. Quantum cryptography is based on the fundamental laws of mechanics rather than unproven complex computational assumptions. A taxonomy of key security technologies that could help healthcare information security is presented in Figure 6 and described below.

A. Quantum Key Distribution

Quantum Key Distribution (QKD), is a protocol that is used to authorize two components by distributing a mutually agreed key to ensure secure transmission. QKD protocol uses certain quantum laws (which are generally based on complex characteristics of quantum computing) to detect information extraction attacks. Specifically, QKD leverages the footprints left when an adversary attempts to steal the information for attack detection. The QKD allows the generation of arbitrarily long keys and it will stop the keys generation process if an attack is detected. The first QKD technique known as BB84 was proposed by Gillies Brassed (105) and it is the widely used method in theoretical research on quantum computing. Shor et al. (106) presented the proof of the BB84 technique by relating the security to the entanglement purification protocol and the quantum error correction code. In the literature, substantial research has been conducted using the QKD security protocol and several novel improvements in the quantum computing security paradigm using QKD protocol have been made so far.

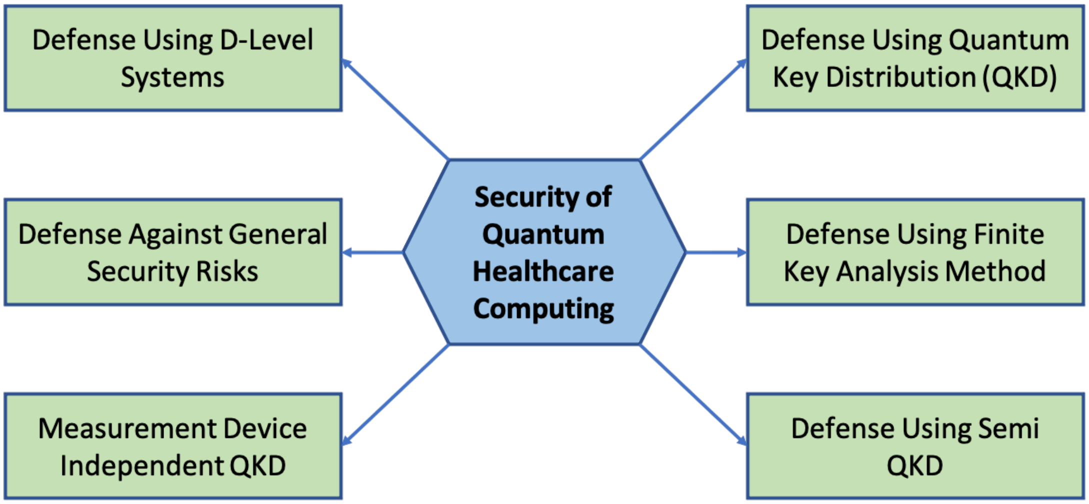

Fig. 6: Taxonomy of key technologies that can ensure security for healthcare information processing.

TABLE V: Summary of countermeasures and security protocols using *d-level systems*.

Author	Objective	Security Algorithm	Pros	Cons
Cerf et al. (107)	• Quantum cryptographic schemes	• Quantum states in a d-dimensional Hilbert space • Cryptosystem uses two mutually unbiased bases	• Enhanced accuracy • Efficient authentication	• Increased error rate
Waks et al. (108)	• Design flows in security and privacy	• Quantum key distribution with entangled photons • BB84 protocol	• Enhanced authentication • Increased accuracy • More practical paradigm	• Restricted to individual eavesdropping attacks • Lack of reliability • Lack of comparison
Hwang (109)	• Global secure communication	• Quantum key distribution • Decoy pulse method	• Coherent pulse sources • Generalization to any arbitrary case • Resource efficiency	• Higher computational cost • Require more resources • Prone to attacks
Iblisdir et al. (110)	• Security of quantum key distribution	• Coherent States and Homodyne Detection • Transmission of Gaussian-modulated coherent states	• Lowering down phase error rate • Securing against any attack	• Lack of robustness • Meager improvement
Biham et al. (111)	• Security of theoretical quantum key distribution	• Attackers reduced density matrices	• Securing against optimal attacks • Extensive usage of symmetry	• Lack of scalability • Complex computations
Acin et al. 2020 (112)	• Device-Independent security of quantum cryptography	• Quantum key cryptography • Authentication algorithm	• Security against collective attacks • Implementation efficiency	• Lower efficiency • Implementation issues
Mckague et al. 2019 (113)	• Secure against coherent attacks with memoryless measurement devices	• XOR • Device independent quantum key distribution	• Security againt overall attacks • Improved efficiency	• Limited evaluation • Low-level scope
Zhao et al. (114)	• Security analysis of an untrusted source	• Untrusted source scheme	• Does not require fast optical switching • Reduce cost	• False-positive rate • Limited efficiency

B. Defense Using D-Level Systems

In (107), the authors used d-level systems to protect against individual and concurrent attacks. They discussed two cryptosystems where the first system uses two mutually unbiased bases while the second utilizes d+1 concurrently unbiased bases. The proof of security for the protocols with entangled photons for individual attacks has been demonstrated by (108). However, the challenge with this approach was the increased error rate. In (109), the authors proposed the decoy pulse method for BB84 in high-loss rate scenarios. A privileged user replaces signal pulses with multiphoton pulses. The security proof of coherent-state protocol using Gaussian modulated coherent state and homodyne detection against arbitrary coherent attacks is provided in (110). In (111), authors proposed security against common types of attacks that could be inflicted on the quantum channels by eavesdroppers having vast computational power. The security of DI QKD against collective attacks has been analyzed in (112), which has been extended by (113) with a more general form of attacks. A passive approach for security using a beam divider to segregate each input pulse and demonstrate its effectiveness is presented in (114). Table V presents a taxonomy and summary of different approaches focused on using d-level systems as a defense strategy to withstand security attacks.

C. Defense Against General Security Risks

In this section, we present existing defense approaches to withstand different general attacks against quantum computing systems. For instance, Maroy et al. (115) proposed a defense strategy for BB84 that enforces security with random individual imperfections concurrently in the quantum sources and detectors. Similarly, Pawlowski et al. (117) proposed a semi-device independent defense scheme against individual attacks that provides security when the devices are assumed to devise quantum systems of a given dimension. In (118), authors presented a defensive scheme for a greater number of quantum protocols, where the key is generated by independent measurements. A comparative analysis of secret keys that violate Bell inequality is presented in (123). The authors suggested that any available information to the eavesdroppers should be consistent with the non-signaling principle.

TABLE VI: Summary of countermeasures and security protocols for *general security risks*.

Author	Objective	Security Algorithm	Pros	Cons
Maroy et al. (115)	• Security of quantum key distribution	• Quantum states in a d-dimensional • Arbitrary individual imperfections	• Enhanced accuracy • Efficient authentication	• Increased error rate using qudit systems
Sheridan et al. (116)	• Security proof for quantum key distribution	• Asymptotic regime • Higher-dimensional protocols	• Secret key rate for fixed noise • Increased accuracy • More practical paradigm	• Restricted to individual eavesdropping attacks • Lack of reliability • Lack of comparison
Pawlowski (117)	• Security of entanglement -based quantum key	• Semi-device-independent security • One-way quantum key distribution	• Coherent pulse sources • Generalization to any arbitrary case • Resource efficiency	• Higher computational cost • Require more resources • Prone to attacks
Masanes et al. (118)	• Secure device-independent quantum key	• Distribution with causally independent measurement devices • Quantum computing laws	• Lowering down phase error rate • Securing against any attack	• Lack of robustness • Meager improvement
Moroder et al. (119)	• Security of Distributed -Phase-Reference	• Variant of the COW protocol	• Generic method for security • Extensive usage of symmetry	• Lack of scalability • Complex computations
Beaudry et al. (120)	• Security of two-way quantum key distribution	• Entropic uncertainty relation • Authentication algorithm	• Security against collective attacks • Implementation efficiency	• Lower efficiency • Implementation issues
Leverrier et al. 2019 (121)	• Security of Continuous-Variable Quantum Key	• Phase-space symmetries of the protocols • Gaussian continuous-variable quantum	• Applicable to relevant finite-size regime • Improved efficiency	• Limited evaluation • Low-level scope
Prionio et al. (122)	• Security of quantum key cryptography	• Untrusted source scheme	• Does not require fast optical switching • Reduce cost	• False-positive rate • Limited efficiency
Masnes et al. (123)	• Full security of quantum key distribution	• Secret key from correlations	• Does not require fast optical switching • Reduce cost	• False-positive rate • Limited efficiency
Vazirani et al. (124)	• Fully device independent quantum key distribution	• Entanglement-based protocol building	• Does not require fast optical switching • Reduce cost	• False-positive rate • Limited efficiency
Zhang et al. (125)	• Security analysis of orthogonal	• Continuous-variable quantum key distribution	• Does not require fast optical switching • Reduce cost	• False-positive rate • Limited efficiency
Lupo et al. (126)	• Continuous-variable measurement-device independent quantum	• Security against collective Gaussian attacks	• Does not require fast optical switching • Reduce cost	• False-positive rate • Limited efficiency

TABLE VII: Summary of countermeasures and security protocols using *Finite Key Analysis*.

Author	Objective	Security Algorithm	Pros	Cons
Cai et al. (127)	• Finite-key unconditional security	• Entanglement-based implementations • Finite-key bound for prepare-and-measure	• Enhanced accuracy • Efficient authentication	• Increased error rate using qudit systems
Song et al. (128)	• Imperfect detectors to learn a large part of the secret key	• Asymptotic regime • Chernoff bound	• Secret key rate for fixed noise • Increased accuracy • More practical paradigm	• Restricted to individual eavesdropping attacks • Lack of reliability • Lack of comparison
Curty et al. (129)	• Finite-key analysis for device-independent measurement	• Semi-device-independent security • One-way quantum key distribution	• Coherent pulse sources • Generalization to any arbitrary case • Resource efficiency	• Higher computational cost • Require more resources • Prone to attacks
Zhou et al. (130)	• Semi-device-independent QKD protocol	• Distribution with causally independent measurement devices • Quantum computing laws	• Lowering down phase error rate • Securing against any attack	• Lack of robustness • Meager improvement

Leverrier et al. (121) evaluated ”the security of Gaussian continuous variable QKD with coherent states against arbitrary attacks in the finite-size scheme”. In a similar study, Morder et al. (119) presented a method to evaluate the security aspects of a practical distributed phase reference QKD against general attacks. A framework for the continuous-variable QKD is presented in (125), which is based on an orthogonal frequency division multiplexing scheme. A comprehensive security analysis of continuous variable MDI QKD in a finite-sized scenario is presented in (126) and defense against generic DI QKD protocols is presented in (122). In (120), the authors presented a method ”to prove the security of two-way QKD protocols against the most general quantum attack on an eavesdropper, which is based on an entropic uncertainty” relation. In (124), authors particularly defined the perspective of Eckert’s original entanglement protocol against a general class of attacks. A taxonomy summarizing different defenses against general security attacks is presented in Table VI.

D. Defense using Finite Key Analysis Method

During the past few years, the finite key analysis method has become a popular security scheme for QKD, which has been integrated into the composable unconditional security proof. In (127), the authors attempt to address the security constraints of finite length keys in different practical environments of BB84 that include prepare and measure implementation without decoy state and entanglement-based techniques. Similarly, the finite-key analysis of MDI QKD presented in (128) works by removing the major detector channels and generating different novel schemes of the key rate that is greater than that of a full-device-independent QKD. The security proof against the general form of attacks in the finite-key regime is presented in (129). The authors present the feasibility of long-distance implementations of MDI QKD within a specific signal transmission time frame. A practical prepare and measure partial device-independent BB84 protocol having finite resources is presented in (130). A security analysis performed against discretionary communication exposure from the preparation process is presented in (131). Table VII presents the taxonomy and summary of the finite key analysis security schemes.

TABLE VIII: Summary of countermeasures and security protocols using *measurement-device-independent quantum key distribution*.

Author	Objective	Security Algorithm	Pros	Cons
Acin et al. (112)	• Device-independent cryptography against collective attacks	• Holevo information • Bell-type inequality	• Generate secret key • Freedom and secrecy	• Leakage of information
Barret et al. (132)	• Security from memory attacks	• Device-independent protocols • Quantum cryptography	• Secret key rate for fixed noise • Securely destroying or isolating devices • More practical paradigm	• Restricted to individual eavesdropping attacks • Leaking secret data. • Costly and often impractical
Qi et al. (133)	• Security against time-shift attack	• Signal pulse synchronization pulse • Time-multiplexing technique	• Simple and feasible • Generalization to any arbitrary case • Resource efficiency	• Higher computational cost • Require more resources • Final key they share is insecure
Fung et al. (134)	• Phase-remapping	• Unconditionally secure against Measurement devices • Eavesdroppers with unlimited	• Lowering down phase error rate • Securing against any attack	• Lack of robustness • Meager improvement
Lydersen et al. (135)	• Relevant quantum property of single photons	• Commercially available QKD systems • Acquire the full secret key	• Lowering down phase error rate • Securing against any attack	• Lack of robustness • Meager improvement
Li et al. (136)	• Attacking practical quantum key	• Wavelength dependent beam splitter • Multi-wavelength sources	• Widespread scope • Securing against any attack	• Higher error rate • Higher implementation cost
Lim et al. (137)	• Local Bell test	• Device-independent quantum key • Multi-wavelength sources	• Casually independent devices • Losses in the channel is avoided.	• Implementation loopholes • Side-channel attacks
Broadbent et al. (138)	• Device independent quantum key distribution	• Generalized two-mode Schrodinger • Multi-wavelength sources	• Coherent attacks • Low error rate.	• Lack of accuracy • Attack vulnerabilities
Cao et al. (139)	• Long-distance free-space measurement	• Based on two-photon interference • Multi-wavelength sources • Fiber-based implementations	• Way to quantum experiments • Low error rate.	• Long-distance interference • Security attacks
Li et al. (140)	• Continuous-variable measurement	• Quantum catalysis • discrete-variable • Zero-photon catalysis	• Defense against attacks • Simulation results.	• Lack of accuracy • Attack vulnerabilities
Ma et al. (141)	• Measurement-device independent quantum	• Quantum catalysis • High-security quantum information • Gaussian-modulated coherent states	• Continuous-variable entanglement • Losses in current telecom components.	• More overhead. • Lack of accuracy
Zhou et al. (142)	• Biased decoy-state measurement	• Finite secret key rates • Efficient decoy-state information • Single-photon yield	• Simulation results • Increased efficiency	• More overhead. • Lack of accuracy
Tamaki et al. (143)	• Phase encoding schemes	• Basis-dependent flaw • Phase encoding schemes • Single-photon yield	• Non-phase-randomized coherent pulses • Increased efficiency	• More overhead. • Lack of accuracy
Zhao et al. (144)	• Phase encoding schemes	• Post selection using untrusted measurement • Virtual photon subtraction • Single-photon yield • Non-Gaussian post-selection	• Non-phase-randomized coherent pulses • Increased efficiency	• Reduced reliability • Increased complexity
Ma et al. (145)	• Continuous-variable measurement-device	• Independent quantum key distribution via quantum catalysis • Single-photon yield • A noiseless attenuation process	• Single-photon subtraction coherent pulses • Improving performance	• A higher secret key rate • Limitation of transmission distance
Li et al. (146)	• Fault-tolerant measurement	• Decoherence-free subspace • Collective-rotation noise • Collective-dephasing noises	• Reducing experiment difficulty • Enhanced security	• Lack of general noise cases • Lack of improving overall efficiency

E. Measurement-Device-Independent Quantum Key Distribution

DI QKD (112) aims to fulfill the gap among practical realization of the QKD without considering the working mechanism of the underlying quantum device. It requires a violation of the Bell inequality between both ends of the communication and can provide higher security than classical schemes through reduced security assumptions. Alternatively, information receivers on both ends need to identify the infringement of Bell inequality. DI attributes to the fact that there is no need to acquire information on the underlying devices. In this case, the device may correspond to adversaries. Therefore, the identification of elements is necessary as compared to considering how quantum security is implemented (132). In this context, DI QKD is capable of defending against different kinds of security vulnerabilities including time-shift attacks (133), phase remapping attacks (134), binding attacks (135), and wavelength-dependent attacks (136). Additionally, security vulnerability identification generated by quantum communication channels can be defended using the technique presented in (137). Furthermore, Broadbent et al. proposed generalized two-mode Schrodinger cat states DI QKD protocol (138). The taxonomy and summary of the device-independent quantum key distribution is presented in Table VIII.

Lo et al. proposed a device-independent measurement scheme (139), which is a step forward to achieve information theory security for the key sharing among two legitimate remote users. Comparatively, MDI-QKD incorporates different added advantages as compared to DI-QKD. The actual key rate of MDI-QKD achieves a higher rating as compared to DI-QKD by successfully eliminating the detector channel vulnerabilities. Moreover, both ends of communication do not require to execute any kind of measurements where they only need to transmit quantum signals that could be measured. In this case, both ends of the communication do not need to hold any measurement devices treating them as black boxes. This could help in eliminating the requirement to validate detectors in the QKD standardization mechanism. In this regard, bit strings designated to both ends of the communication would not be secured from the detector side channels due to the non-availability of detectors. Though they need to characterize the quantum states they transfer using channels, which occurs in a secure paradigm. This paradigm is relatively secure from the adversary who may exploit the encoding and decoding modules without focusing on polarization maintenance. Li et al. proposed an untrusted third-party attack detection using a continuous-variable MDI protocol (140). Similarly, Ma et al. (141) proposed MDI-based scheme using Gaussian-modulated coherent states. The

TABLE IX: Summary of countermeasures and security protocols using *Semi-Quantum Key Distribution*.

Author	Objective	Security Algorithm	Pros	Cons
Boyer et al. (147)	• Semi-quantum key distribution protocol	• Nonzero information acquired • Measure-resend SQKD protocol	• Robust approach • Eliminating information leak	• Prone to PNS attacks • Lack of scope.
Boyer 2017 et al. (148)	• Semi-quantum key distribution	• SQKD protocols • Classical Alice with a controllable mirror	• Robust approach • Comprehensive security	• Lack of interoperability • Increased communication overhead
Lu 2008 et al. (149)	• Quantum key distribution with classical Alice	• Encoding key bits • Classical encoding	• Robust approach • Tolerable noise	• Higher complexity • More processing time
Zou et al. (150)	• Semi-quantum key distribution	• Photon pulses • Quantum state distribution	• Robust approach • Tolerable noise	• Increased latency • Higher processing time
Maitra et al. (151)	• Eavesdropping in semi-quantum key distribution protocol	• Eavesdropping in both directions • Disturbance and information leakage	• Extract more info on secret approach • One-way strategy application	• Increased latency • Higher processing time
Krawec et al. (152)	• Mediated semi-quantum key distribution	• Shared secret key • Fully quantum server	• More overhead • One-way strategy application	• Full quantum security • Higher processing time
Zou et al. (153)	• Semi-quantum key distribution	• Shared secret key • Fully quantum server	• Robust against joint attacks • More control over classical party	• Simple strategy prone to attacks • Lack of computational feasibility
Liu et al. (154)	• Mediated semi-quantum key distribution	• A shared secret key • Untrusted third party	• Security against known attacks • More secure than three-party SQKD protocol	• Higher quantum burden • Unable to combat the collective-rotation noise
Sun et al. (155)	• MSemi-quantum key distribution protocol using Bell state	• Privacy amplification protocols • Untrusted third party	• Security against known attacks • More secure than three-party SQKD protocol	• Higher quantum burden • Unable to combat the collective-rotation noise • Higher computational complexity
Jian et al. (156)	• Semi-quantum key distribution using entangled states	• Maximally entangled states • Quantum Alice shares a secret key with classical Bob	• Increased qubit efficiency • Security against eavesdropping	• Challenges in implementing semi-quantum • Increased computation overhead • Higher computational complexity
Yu et al. (157)	• Authenticated semi-quantum key distribution	• Pre-sharing a master secret key • Transmitting a working key	• Increased impersonation attack security • Security against eavesdropping	• Prone to Trojan horse attacks • Increased computation overhead • Higher computational complexity
Li et al. (158)	• Semi-quantum key distribution using secure delegated quantum computation	• Establishing a secret key • Secure delegated quantum computation	• Enhanced efficiency • More security	• Quantum implementation challenges • Network overhead • Higher resource consumption
Li et al. (158)	• Long-distance free-space quantum Key distribution	• Establishing a secret key • Secure delegated quantum computation	• Satellite quantum • Long-distance security	• Noise accumulation • Communication restrictions • Higher resource consumption
He et al. (159)	• Measurement-device-independent semi-quantum key distribution	• Quantum key distribution • Key distribution	• Higher security • Increased reliability	• More latency • Secret key leakage • Side-channel attacks
Zhu et al. (159)	• Semi-quantum key distribution protocols with GHZ States	• Strong quantum capability • Achieve quantum key distribution	• Higher security • Increased reliability	• More latency • Secret key leakage • Side-channel attacks

authors in (142), proposed a decoy-state protocol. In this scheme, a measurement basis is chosen to have a biased probability and intensities of various types of states and an optimized strategy is used to achieve a finite secret key rate. In (143) authors proposed two techniques for phase encoding including phase-locking and conversion of BB84 standard encoding pulses into polarization modes. Zhao et al. (144) improved the performance of coherent-state continuous variable MDI protocol by virtual photon subtraction. In a similar study (145), the authors used photon subtraction to improve the efficiency of the continuous variable MDI protocol.

F. Semi-Quantum Key Distribution

SQKD exploits novel quantum capabilities of at least one party in the communication. It eliminates computational overhead and alleviates the computational cost. SQKD ensures that both ends of the communication achieve QKD. In this mechanism, only the sender should be quantum-capable whereas the receiver may have classical capabilities. Specifically, the sender performs various operations including preparation of quantum states, performing quantum measurements, and storage of quantum states. In this paradigm, the receiver performs multiple operations including preparation of novel qubits, measurement of qubits, order arrangement of qubits, and transmitting qubits without disturbing quantum channels. Boyer et al. (160) propose the first SQKD in 2007. In this scheme, they used single photons to determine the robustness of the protocol. In the later state, they extended this work by generalizing the underlying conditions. They analyzed these conditions and prove that complete robustness could only be achieved when the qubits are transmitted individually but are attacked collectively. In their later work, Boyer et al. (147) also proposed a feasible protocol using four-level systems. Lu et al. (149) proposed classical sender-based protocol. The sender can send encoded key bits on a Z basis. Zou et al. (150) proposed a robust SQKD protocol that transfers fewer than four quantum states. Maitra et al. (151) analyzed a two-way eavesdropping scheme against an SQKD protocol. Karawec et al. (152) proposed a secret key-sharing scheme between two classical users. In (153), the authors avoided measurement capabilities of the sender and ensure that it is robust against joint attacks thus showing that the measurement capability of the classical users is not essential for the implementation of SQKD. Liu et al. (154) used an untrusted quantum server that tries to steal session keys. Currently, various quantum states and technologies are used to devise novel protocols (155; 156; 157; 158; 159; 161). Additionally, a few researchers have analyzed the security vulnerabilities of SQKD (162; 163; 164). The taxonomy and summary of research studies focused on leveraging SQKD is presented in Table IX.

G. Lessons Learned: Summary and Insights

In this section, we outlined all the security solutions developed using the quantum mechanics concept. Security of healthcare is critical as healthcare systems store a large amount of private information of the patients. Therefore, quantum cryptography provides extended benefits to deal with the security issues faced by healthcare systems.

VII. Open Issues and Future Research Directions

This section discusses the various open issues related to quantum computing for healthcare. We present a taxonomy of those challenges, their causes, and some future research directions to solve those challenges.

A. Quantum Computing for Big Data Processing

Due to its natural ability to boost computational processing, quantum computing is a good fit for big data analytics. Previous research has shown the great promise of using big data for revolutionizing healthcare by enabling personalized services and better diagnostics and prognostics (165; 103). In particular, big data for healthcare can leverage data science and advancements in ML/DL to enable descriptive, predictive, and prescriptive analytics.

B. Quantum AI/ML Applications

Quantum computing promises to provide additional computational capabilities that can be used to train more advanced AI/ML models, which can drive revolutionary breakthroughs in healthcare (166). Of the various kinds of quantum algorithms that are relevant to healthcare, quantum-enhanced AI/ML stands out for the breadth of their applications. Quantum approaches are particularly well suited for ML algorithms, many of which rely on operations with large matrices, which can be enhanced significantly using quantum computing (1). AI/ML is a powerful and diverse method that supports a variety of applications. There are multiple traditional learning models such as the conjugate gradient method that use traditional hardware accelerators. Quantum computing could provide support for AI/ML tasks during the machine design phase for overall enhancement the of the inference model. A popular design using the Boltzmann machine (167) provides an early example. The Boltzmann machine consists of hidden artificial neurons having weighted edges between them. Neurons are characterized by energy function that depends on the interaction with their connected neighbors. Hence, quantum AI could speed up the ML training process and increase the accuracy of the training models.

Some of these systems deal with real-time decision making such as driving a vehicle, stock selection to maximize the portfolio, or computing recommendations to select the right product. Most AI applications develop an inference model for informed decision-making. These inference models work based on rule-based analysis, pattern recognition, and sequence identification. Rule-based inference models accompany pre-configured responses in the design of the system. However, these applications rely on the imagination of the application creator. An alternative method is to use patterns and associations using a large amount of existing data. A smaller amount of error in the inference models could bring the accuracy of predictions down. Error reduction in inference models is akin to a search problem.

C. Large-Scale Optimization

Optimization techniques are used routinely in various fields. Many optimization problems suffer from intractability and from a combinatorial explosion when dealing with large instances. For instance, the Traveling Salesman Problem (TSP) is a famous optimization problem that aims at identifying the shortest possible distance between cities by hitting each city once and then returning to the initial point. The TSP problem is NP-Hard and an optimal solution to this problem becomes intractable when the number of cities becomes very large. In such cases, heuristics are resorted to as solving such problems on traditional computing systems simply takes an impractically long time. Quantum computing provides two probable solutions to these problems including quantum annealing and universal quantum computers. Furthermore, quantum annealing is an optimization heuristic that can overcome the challenges of traditional computing systems in solving optimization problems. Specialized quantum annealers could be implemented that is considered easier to implement as compared to a universal quantum computer. However, their efficacy over traditional computers is yet to be explored. Lightweight digital annealers can simulate quantum annealers features on classical computing systems, resulting in cost-effective solutions. Universal annealers are fully capable of solving quantum computing problems but their commercial implementations are rare.

D. Quantum Computers for Simulation

Richard Feynman is reported to have said that "*nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical.*" Quantum computing offers great promise in developing realistic simulators for complex tasks that are difficult to predict using traditional methods. Quantum computers can be used to simulate chaotic systems such as the weather. They can also be used to model the evolution of complex biological systems and social contagions such as the evolution of an epidemic or a pandemic. Furthermore, quantum computers also hold promise for simulating metabolism within a call and for investigating drug interaction at a cellular and molecular level. This can enable and facilitate the development of new vaccines and medications. Quantum computers can also be used to develop digital twins of human organs and cells. Quantum computing will also enable fine-grained and potentially intrusive applications and it is necessary to consider and address the various ethical issues that may emerge (168; 169)

E. Quantum Web and Cloud Services

Bringing quantum computing services to commodity hardware is a critical challenge to reap the benefits of the extended functionalities provided by quantum computing. Due to the large number of resources required for quantum computing implementations, it becomes challenging to access quantum computing for general-purpose problem-solving. Amazon web services provide an example implementation scenario that can be used to implement quantum web services. Amazon Braket (170) is one example of implementing quantum web services. It provides an efficient platform for researchers and experts to analyze and evaluate quantum computing models in a real-time testing environment. Amazon Braket provides an experimental environment to design, test, and evaluate quantum computing algorithms on a simulated quantum environment and runs them on quantum hardware. It uses D-wave's quantum annealing and gate-based hardware under the hood. These gate-based quantum computers include ion-trap devices from IonQ, and systems built on superconducting qubits from Rigetti (171). Apart from the Amazon web services environment, other quantum computing solutions are required to provide quantum web services to the users. Software-Development Kits (SDK) could be implemented, which can be used to simulate the developed quantum computing algorithm.

F. Quantum Game Theory

Quantum computing is likely to impact future game theory applications. The complementary aspect of quantum computing overlaps game theory applications. In the game theory, every player is maximizing individual payoffs. A prime example is the Prisoner's Dilemma (172) where each player faces criminal charges. Pareto (173) calls for players to cooperate whereas Nash equilibrium (174) implies that both the players must defeat. Thus, there are apparent contradictions among different game theory applications. Quantum game theory is a novel extension of the traditional game theory involving quantum information resources. Quantum computing resources have already been providing better solutions for the Prisoner's Dilemma. Furthermore, players can achieve Pareto optimal solution provided the circumstances that they are allowed to share a mutually entangled state.

G. Quantum Security Applications

Cyberspace has been under a constant threat of an increasing number of attackers (175) (169). Necessary security frameworks have been developed to protect cyberspace against these attacks. However, this process becomes daunting for classical computing systems. Quantum computing using ML helps develop security schemes for traditional computing systems. Quantum computing supports quantum cryptography, which provides efficient solutions to protect data against privacy-breaching attacks. However, the unprecedented computing power of quantum computing also raises security risks and undermines traditional encryption schemes. This motivates the need for quantum-resisting encryption techniques to mitigate the threats of quantum computing. The National Institute of Standards and Technology (NIST) is developing such a solution to cope with encryption problems. Encryption techniques should be carefully developed to ensure that they are quantum-ready. Moreover, traditional password management schemes could become insufficient in the quantum environment. For example, passwords that may require extended time for decryption can be guessed in a shorter period using quantum computing applications. Therefore, novel techniques need to be developed to enforce strong encryption schemes to protect sophisticated data. Quantum services are also currently being offered via the cloud, it is important to acknowledge and mitigate the various security risks that emerge from using cloud services especially when quantum machine learning services are being offered via the cloud (176).

H. Developing Quantum Market Place

One of the vital challenges in quantum computing implementations is the pricing and resource allocation of quantum services to the service subscribers. Similar to web services, a quantum computing marketplace could be developed providing a platform for the subscribers to utilize a pay-per-use pricing model for the services. Users can subscribe to the services that they want and based on the consumed services, the price should be determined. However, such a distributed quantum marketplace development requires a coordinated quantum strategy, which can be used to distribute quantum services and develop pricing models. Such a system also requires experts from different domains to have expertise in quantum systems and can develop financial models, services distributed mechanisms, and control strategies for quantum resource distribution. Recently D-Wave announced plans to launch D-Wave's Leap quantum cloud service on the Amazon AWS cloud for the first time (177).

VIII. Conclusions

Quantum computing has revolutionized traditional computational systems by bringing unimaginable speed, efficiency, and reliability. These key features of quantum computing can be leveraged to develop computationally efficient healthcare applications. To this end, we in this paper provide a comprehensive survey of existing literature focused on leveraging quantum computing for the development of healthcare solutions. Specifically, we discussed different potential healthcare applications that can get benefited from quantum computing. In addition, we elaborate upon the key requirements for the development of quantum computing empowered healthcare applications and have provided a taxonomy of existing quantum computing architectures for healthcare systems. Furthermore, we also discussed different security aspects for the use of quantum computing in healthcare applications and discussed different quantum technologies that can ensure the security of such applications. Finally, we discussed current challenges, their causes, and future research directions where quantum computing could provide immense benefits. This is a novel study, which underlines all the key areas of quantum computing implications in the healthcare paradigm and can provide a one-stop solution to the research community interested in utilizing and analyzing different prospects of quantum computing in various healthcare applications.

References

[1] F. Flöther, J. Murphy, J. Murtha, D. Sow, Exploring quantum computing use cases for healthcare (ibm expert insights) (2020).
URL https://www.ibm.com/downloads/cas/8QDGKDZJ

[2] A. Devi, V. Kalaivani, Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications, Personal and Ubiquitous Computing (2021) 1–11.

[3] S. Sadki, H. E. Bakkali, Towards negotiable privacy policies in mobile healthcare, in: Fifth International Conference on the Innovative Computing Technology (INTECH 2015), 2015, pp. 94–99.

[4] M. Zinner, F. Dahlhausen, P. Boehme, J. Ehlers, L. Bieske, L. Fehring, Toward the institutionalization of quantum computing in pharmaceutical research, Drug Discovery Today.

[5] L. Banchi, M. Fingerhuth, T. Babej, C. Ing, J. M. Arrazola, Molecular docking with gaussian boson sampling, Science advances 6 (23) (2020) eaax1950.

[6] R. Y. Li, R. Di Felice, R. Rohs, D. A. Lidar, Quantum annealing versus classical machine learning applied to a simplified computational biology problem, NPJ quantum information 4 (1) (2018) 1–10.

[7] V. V. Fedorov, S. L. Leonov, Combinatorial and model-based methods in structuring and optimizing cluster trials, in: Platform Trial Designs in Drug Development, Chapman and Hall/CRC, 2018, pp. 265–286.

[8] L. Gyongyosi, S. Imre, A survey on quantum computing technology, Computer Science Review 31 (2019) 51–71.

[9] T. M. Fernández-Caramés, From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things, IEEE Internet of Things Journal 7 (7) (2019) 6457–6480.

[10] L. Gyongyosi, S. Imre, H. V. Nguyen, A survey on quantum channel capacities, IEEE Communications Surveys & Tutorials 20 (2) (2018) 1149–1205.

[11] S. Arunachalam, R. de Wolf, Guest column: A survey of quantum learning theory, ACM SIGACT News 48 (2) (2017) 41–67.

[12] Y. Li, M. Tian, G. Liu, C. Peng, L. Jiao, Quantum optimization and quantum learning: A survey, IEEE Access 8 (2020) 23568–23593.

[13] T. A. Shaikh, R. Ali, Quantum computing in big data analytics: A survey, in: 2016 IEEE International Conference on Computer and Information Technology (CIT), IEEE, 2016, pp. 112–115.

[14] D. J. Egger, C. Gambella, J. Marecek, S. McFaddin, M. Mevissen, R. Raymond, A. Simonetto, S. Woerner, E. Yndurain, Quantum computing for finance: state of the art and future prospects, IEEE Transactions on Quantum Engineering.

[15] M. Savchuk, A. Fesenko, Quantum computing: Survey and analysis, Cybernetics and Systems Analysis 55 (1) (2019) 10–21.

[16] H. Zhang, Z. Ji, H. Wang, W. Wu, Survey on quantum information security, China Communications 16 (10) (2019) 1–36.

[17] C. C. McGeoch, R. Harris, S. P. Reinhardt, P. I. Bunyk, Practical annealing-based quantum computing, Computer 52 (6) (2019) 38–46.

[18] K. Shannon, E. Towe, O. K. Tonguz, On the use of quantum entanglement in secure communications: a survey, arXiv preprint arXiv:2003.07907.

[19] S. Duan, S. Cong, Y. Song, A survey on quantum positioning system, International Journal of Modelling and Simulation (2020) 1–19.

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

[21] M. Roetteler, K. M. Svore, Quantum computing: Codebreaking and beyond, IEEE Security & Privacy 16 (5) (2018) 22–36.

[22] S. Uprety, D. Gkoumas, D. Song, A survey of quantum theory inspired approaches to information retrieval, ACM Computing Surveys (CSUR) 53 (5) (2020) 1–39.

[23] E. Rowell, Z. Wang, Mathematics of topological quantum computing, Bulletin of the American Mathematical Society 55 (2) (2018) 183–238.
[24] V. Padamvathi, B. V. Vardhan, A. Krishna, Quantum cryptography and quantum key distribution protocols: a survey, in: 2016 IEEE 6th International Conference on Advanced Computing (IACC), IEEE, 2016, pp. 556–562.
[25] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, R. Cammarota, Post-quantum lattice-based cryptography implementations: A survey, ACM Computing Surveys (CSUR) 51 (6) (2019) 1–41.
[26] D. Cuomo, M. Caleffi, A. S. Cacciapuoti, Towards a distributed quantum computing ecosystem, IET Quantum Communication 1 (1) (2020) 3–8.
[27] M. Fingerhuth, T. Babej, P. Wittek, Open source software in quantum computing, PloS one 13 (12) (2018) e0208561.
[28] A. Huang, S. Barz, E. Andersson, V. Makarov, Implementation vulnerabilities in general quantum cryptography, New Journal of Physics 20 (10) (2018) 103016.
[29] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, L. Hanzo, Quantum search algorithms for wireless communications, IEEE Communications Surveys & Tutorials 21 (2) (2018) 1209–1242.
[30] S. B. Ramezani, A. Sommers, H. K. Manchukonda, S. Rahimi, A. Amirlatifi, Machine learning algorithms in quantum computing: A survey, in: 2020 International Joint Conference on Neural Networks (IJCNN), IEEE, 2020, pp. 1–8.
[31] K. Bharti, T. Haug, V. Vedral, L.-C. Kwek, Machine learning meets quantum foundations: A brief survey, AVS Quantum Science 2 (3) (2020) 034101.
[32] A. Abbott, Quantum computers to explore precision oncology, Nature biotechnology 39 (11) (2021) 1324–1325.
[33] Y. Kumar, A. Koul, P. S. Sisodia, J. Shafi, V. Kavita, M. Gheisari, M. B. Davoodi, Heart failure detection using quantum-enhanced machine learning and traditional machine learning techniques for internet of artificially intelligent medical things, Wireless Communications and Mobile Computing 2021.
[34] S. Olgiati, N. Heidari, D. Meloni, F. Pirovano, A. Noorani, M. Slevin, L. Azamfirei, A quantum-enhanced precision medicine application to support data-driven clinical decisions for the personalized treatment of advanced knee osteoarthritis: development and preliminary validation of precisionknee qnn, medRxiv.
[35] S. Gupta, S. Modgil, P. C. Bhatt, C. J. C. Jabbour, S. Kamble, Quantum computing led innovation for achieving a more sustainable covid-19 healthcare industry, Technovation (2022) 102544.
[36] A. Kumar, B. Bhushan, S. Shriti, P. Nand, Quantum computing for health care: A review on implementation trends and recent advances, Multimedia Technologies in the Internet of Things Environment, Volume 3 (2022) 23–40.
[37] N. A. Sinitsyn, Computing with a single qubit faster than the computation quantum speed limit, Physics Letters A 382 (7) (2018) 477–481.
[38] D. Hanneke, J. Home, J. D. Jost, J. M. Amini, D. Leibfried, D. J. Wineland, Realization of a programmable two-qubit quantum processor, Nature Physics 6 (1) (2010) 13–16.
[39] S. Balaganur, Man's race to quantum supremacy: The complete timeline, Analytics India Magazine, Accessed: 22-02-2022.
URL https://analyticsindiamag.com/race-quantum-supremacy-complete-timeline/
[40] P. Ball, et al., First quantum computer to pack 100 qubits enters crowded race, Nature 599 (7886) (2021) 542–542.
[41] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, H. Neven, Characterizing quantum supremacy in near-term devices, Nature Physics 14 (6) (2018) 595–600.
[42] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, et al., Quantum computational advantage using photons, Science 370 (6523) (2020) 1460–1463.
[43] X.-M. Hu, C.-X. Huang, Y.-B. Sheng, L. Zhou, B.-H. Liu, Y. Guo, C. Zhang, W.-B. Xing, Y.-F. Huang, C.-F. Li, et al., Long-distance entanglement purification for quantum communication, Physical Review Letters 126 (1) (2021) 010503.
[44] J. Porter, Google confirms 'quantum supremacy' breakthrough (Date Accessed: June 16, 2021).
URL https://www.theverge.com/2019/10/23/20928294/google-quantum-supremacy-sycamore-computer-qubit-milestone
[45] J. Preskill, Fault-tolerant quantum computation, in: Introduction to quantum computation and information, World Scientific, 1998, pp. 213–269.
[46] J. K. Moser, Lectures on Hamiltonian systems, CRC Press, 2020.
[47] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. James, A. Gilchrist, A. G. White, Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement, Physical Review Letters 99 (25) (2007) 250505.
[48] National Academies of Sciences, Engineering, and Medicine, Quantum Computing: Progress and Prospects, The National Academies Press, Washington, DC, 2019. `doi:10.17226/25196`.
URL https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects
[49] M. Birtwistle, Saving lives and averting costs? the case for earlier diagnosis just got stronger, cancer research uk. (September 22, 2014).
URL https://tinyurl.com/r3ypjvsp
[50] H. Singh, A. N. Meyer, E. J. Thomas, The frequency of diagnostic errors in outpatient care: estimations from three large observational studies involving us adult populations, BMJ quality & safety 23 (9) (2014) 727–731.

[51] P. Kwiat, J. Mitchell, P. Schwindt, A. White, Grover's search algorithm: an optical approach, Journal of Modern Optics 47 (2-3) (2000) 257–266.

[52] F. Bouchard, D. England, P. J. Bustard, K. Heshami, B. Sussman, Quantum communication with ultrafast time-bin qubits, PRX Quantum 3 (1) (2022) 010332.

[53] A. Stanco, F. B. Santagiustina, L. Calderaro, M. Avesani, T. Bertapelle, D. Dequal, G. Vallone, P. Villoresi, Versatile and concurrent fpga-based architecture for practical quantum communication systems, IEEE Transactions on Quantum Engineering 3 (2022) 1–8.

[54] S. Wehner, D. Elkouss, R. Hanson, Quantum internet: A vision for the road ahead, Science 362 (6412) (2018) eaam9288.

[55] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, G. Bianchi, Quantum internet: networking challenges in distributed quantum computing, IEEE Network 34 (1) (2019) 137–143.

[56] N. Young, An introduction to Hilbert space, Cambridge University Press, 1988.

[57] R. Salakhutdinov, G. Hinton, Deep Boltzmann Machines, in: Artificial intelligence and statistics, PMLR, 2009, pp. 448–455.

[58] H. Neven, V. S. Denchev, G. Rose, W. G. Macready, Training a large scale classifier with the quantum adiabatic algorithm, arXiv preprint arXiv:0912.0779.

[59] A. Paler, I. Polian, K. Nemoto, S. J. Devitt, Fault-tolerant, high-level quantum circuits: form, compilation and description, Quantum Science and Technology 2 (2) (2017) 025003.

[60] E. Farhi, J. Goldstone, S. Gutmann, A quantum approximate optimization algorithm, arXiv preprint arXiv:1411.4028.

[61] L. Gyongyosi, Quantum state optimization and computational pathway evaluation for gate-model quantum computers, Scientific reports 10 (1) (2020) 1–12.

[62] E. Farhi, J. Goldstone, S. Gutmann, H. Neven, Quantum algorithms for fixed qubit architectures, arXiv preprint arXiv:1703.06199.

[63] R. D. Van Meter, Architecture of a quantum multicomputer optimized for Shor's factoring algorithm, arXiv preprint quant-ph/0607065.

[64] A. Ekert, R. Jozsa, Quantum computation and Shor's factoring algorithm, Reviews of Modern Physics 68 (3) (1996) 733.

[65] R. Van Meter, S. J. Devitt, Local and distributed quantum computation, arXiv preprint arXiv:1605.06951.

[66] M. Ahsan, R. V. Meter, J. Kim, Designing a million-qubit quantum computer using a resource performance simulator, ACM Journal on Emerging Technologies in Computing Systems (JETC) 12 (4) (2015) 1–25.

[67] K. H. Wan, O. Dahlsten, H. Kristjánsson, R. Gardner, M. Kim, Quantum generalisation of feedforward neural networks, NPJ Quantum information 3 (1) (2017) 1–8.

[68] M. V. Altaisky, N. N. Zolnikova, N. E. Kaputkina, V. A. Krylov, Y. E. Lozovik, N. S. Dattani, Towards a feasible implementation of quantum neural networks using quantum dots, Applied Physics Letters 108 (10) (2016) 103108.

[69] R. Blakestad, C. Ospelkaus, A. VanDevender, J. Amini, J. Britton, D. Leibfried, D. J. Wineland, High-fidelity transport of trapped-ion qubits through an X-junction trap array, Physical review letters 102 (15) (2009) 153002.

[70] K. R. Brown, J. Kim, C. Monroe, Co-designing a scalable quantum computer with trapped atomic ions, NPJ Quantum Information 2 (1) (2016) 1–10.

[71] J. I. Cirac, P. Zoller, Quantum computations with cold trapped ions, Physical review letters 74 (20) (1995) 4091.

[72] L.-M. Duan, M. Madsen, D. Moehring, P. Maunz, R. Kohn Jr, C. Monroe, Probabilistic quantum gates between remote atoms through interference of optical frequency qubits, Physical Review A 73 (6) (2006) 062324.

[73] W. Hensinger, S. Olmschenk, D. Stick, D. Hucul, M. Yeo, M. Acton, L. Deslauriers, C. Monroe, J. Rabchuk, T-junction ion trap array for two-dimensional ion shuttling, storage, and manipulation, Applied Physics Letters 88 (3) (2006) 034101.

[74] D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark, C. Monroe, Modular entanglement of atomic qubits using photons and phonons, Nature Physics 11 (1) (2015) 37–42.

[75] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, R. Blatt, Realization of a scalable shor algorithm, Science 351 (6277) (2016) 1068–1070.

[76] L. Lamata, Basic protocols in quantum reinforcement learning with superconducting circuits, Scientific reports 7 (1) (2017) 1–10.

[77] I. Kerenidis, A. Prakash, Quantum recommendation systems, arXiv preprint arXiv:1603.08675.

[78] M. Benedetti, J. Realpe-Gómez, A. Perdomo-Ortiz, Quantum-assisted helmholtz machines: A quantum–classical deep learning framework for industrial datasets in near-term devices, Quantum Science and Technology 3 (3) (2018) 034007.

[79] D. Copsey, M. Oskin, F. Impens, T. Metodiev, A. Cross, F. T. Chong, I. L. Chuang, J. Kubiatowicz, Toward a scalable, silicon-based quantum computing architecture, IEEE Journal of selected topics in quantum electronics 9 (6) (2003) 1552–1569.

[80] N. C. Jones, R. Van Meter, A. G. Fowler, P. L. McMahon, J. Kim, T. D. Ladd, Y. Yamamoto, Layered architecture for quantum computing, Physical Review X 2 (3) (2012) 031007.

[81] K. M. Svore, A. V. Aho, A. W. Cross, I. Chuang, I. L. Markov, A layered software architecture for quantum computing

design tools, Computer 39 (1) (2006) 74–83.

[82] T. P. Spiller, W. J. Munro, S. D. Barrett, P. Kok, An introduction to quantum information processing: applications and realizations, Contemporary Physics 46 (6) (2005) 407–436.

[83] R. v. Meter, M. Oskin, Architectural implications of quantum computing technologies, ACM Journal on Emerging Technologies in Computing Systems (JETC) 2 (1) (2006) 31–63.

[84] D. P. DiVincenzo, The physical implementation of quantum computation, Fortschritte der Physik: Progress of Physics 48 (9-11) (2000) 771–783.

[85] A. M. Steane, Quantum computer architecture for fast entropy extraction, arXiv preprint quant-ph/0203047.

[86] A. M. Steane, How to build a 300 bit, 1 giga-operation quantum computer, arXiv preprint quant-ph/0412165.

[87] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, C. Monroe, Experimental comparison of two quantum computing architectures, Proceedings of the National Academy of Sciences 114 (13) (2017) 3305–3310.

[88] Z. Liu, X. Liang, M. Huang, Design of logistic regression health assessment model using novel quantum PSO, in: 2018 IEEE 3rd International Conference on Cloud Computing and Internet of Things (CCIOT), IEEE, 2018, pp. 39–42.

[89] T. Janani, M. Brindha, A secure medical image transmission scheme aided by quantum representation, Journal of Information Security and Applications 59 (2021) 102832.

[90] L. Qiu, F. Cai, G. Xu, Quantum digital signature for the access control of sensitive data in the big data era, Future Generation Computer Systems 86 (2018) 372–379.

[91] H. L. Helgeson, C. K. Peyerl, M. Solheim-Witt, Quantum physics principles and communication in the acute healthcare setting: a pilot study, EXPLORE: The Journal of Science & Healing 12 (6) (2016) 408–415.

[92] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, S. E. Venegas-Andraca, Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things, Optics & Laser Technology 124 (2020) 105942.

[93] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, N. Kumar, Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications, Journal of Information Security and Applications 56 (2021) 102673.

[94] B. Javidi, 3D imaging with applications to displays, quantum imaging, optical security, and healthcare, in: 2015 14th Workshop on Information Optics (WIO), IEEE, 2015, pp. 1–3.

[95] H. Childs, Applications of cloud-based quantum computers with cognitive computing algorithms in automated, evidence-based virginia geriatric healthcare, Auctus: The Journal of Undergraduate Research and Creativity.

[96] A. M. Perumal, E. R. S. Nadar, Architectural framework and simulation of quantum key optimization techniques in healthcare networks for data security, Journal of Ambient Intelligence and Humanized Computing (2020) 1–8.

[97] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, B. B. Gupta, Efficient quantum information hiding for remote medical image sharing, IEEE Access 6 (2018) 21075–21083.

[98] J. Hastings, Modern nursing and modern physics: does quantum theory contain useful insights for nursing practice and healthcare management?, Nursing Philosophy 3 (3) (2002) 205–212.

[99] T. Porter-O'Grady, Quantum mechanics and the future of healthcare leadership, The Journal of Nursing Administration 27 (1) (1997) 15–20.

[100] S. Datta, B. Newell, J. Lamb, Y. Tang, P. Schoettker, C. Santucci, T. G. Pachta10, S. Joshi11, O. Geman12, D. C. Vanegas13, et al., Aptamers for Detection and Diagnostics (ADD) is a proposed mobile app acquiring optical data from conjugated quantum nanodots to identify molecules indicating presence of SARS-CoV-2 virus: Why public health and healthcare need smartphone sensors as a platform for early detection and prevention, ChemRxiv.

[101] T. Koyama, N. Shibata, S. Kino, A. Sugiyama, N. Akikusa, Y. Matsuura, A compact mid-infrared spectroscopy system for healthcare applications based on a wavelength-swept, pulsed quantum cascade laser, Sensors 20 (12) (2020) 3438.

[102] V. S. Naresh, M. M. Nasralla, S. Reddi, I. García-Magariño, Quantum Diffie–Hellman Extended to Dynamic Quantum Group Key Agreement for e-Healthcare Multi-Agent Systems in Smart Cities, Sensors 20 (14) (2020) 3940.

[103] S. Latif, J. Qadir, S. Farooq, M. A. Imran, How 5G wireless (and concomitant technologies) will revolutionize healthcare?, Future Internet 9 (4) (2017) 93.

[104] C. Brooks, Quantum trends and the internet of things (Date Accessed: June 16, 2021). URL https://www.forbes.com/sites/cognitiveworld/2019/12/05/quantum-trends-and-the-internet-of-things/?sh=595bb3443eb0

[105] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, arXiv preprint arXiv:2003.06557.

[106] P. W. Shor, J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Physical review letters 85 (2) (2000) 441.

[107] N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Security of quantum key distribution using d-level systems, Physical review letters 88 (12) (2002) 127902.

[108] E. Waks, A. Zeevi, Y. Yamamoto, Security of quantum key distribution with entangled photons against individual attacks, Physical Review A 65 (5) (2002) 052310.

[109] W.-Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Physical Review Letters

91 (5) (2003) 057901.

[110] S. Iblisdir, G. Van Assche, N. Cerf, Security of quantum key distribution with coherent states and homodyne detection, Physical review letters 93 (17) (2004) 170502.

[111] E. Biham, M. Boyer, P. O. Boykin, T. Mor, V. Roychowdhury, A proof of the security of quantum key distribution, Journal of cryptology 19 (4) (2006) 381–439.

[112] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Device-independent security of quantum cryptography against collective attacks, Physical Review Letters 98 (23) (2007) 230501.

[113] M. McKague, Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices, New Journal of Physics 11 (10) (2009) 103037.

[114] Y. Zhao, B. Qi, H.-K. Lo, L. Qian, Security analysis of an untrusted source for quantum key distribution: passive approach, New Journal of Physics 12 (2) (2010) 023024.

[115] Ø. Marøy, L. Lydersen, J. Skaar, Security of quantum key distribution with arbitrary individual imperfections, Physical Review A 82 (3) (2010) 032337.

[116] L. Sheridan, V. Scarani, Security proof for quantum key distribution using qudit systems, Physical Review A 82 (3) (2010) 030301.

[117] M. Pawłowski, N. Brunner, Semi-device-independent security of one-way quantum key distribution, Physical Review A 84 (1) (2011) 010302.

[118] L. Masanes, S. Pironio, A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices, Nature communications 2 (1) (2011) 1–7.

[119] T. Moroder, M. Curty, C. C. W. Lim, H. Zbinden, N. Gisin, et al., Security of distributed-phase-reference quantum key distribution, Physical review letters 109 (26) (2012) 260501.

[120] N. J. Beaudry, M. Lucamarini, S. Mancini, R. Renner, Security of two-way quantum key distribution, Physical Review A 88 (6) (2013) 062302.

[121] A. Leverrier, R. García-Patrón, R. Renner, N. J. Cerf, Security of continuous-variable quantum key distribution against general attacks, Physical review letters 110 (3) (2013) 030502.

[122] S. Pironio, L. Masanes, A. Leverrier, A. Acín, Security of device-independent quantum key distribution in the bounded-quantum-storage model, Physical Review X 3 (3) (2013) 031007.

[123] L. Masanes, R. Renner, M. Christandl, A. Winter, J. Barrett, Full security of quantum key distribution from no-signaling constraints, IEEE Transactions on Information Theory 60 (8) (2014) 4973–4986.

[124] U. Vazirani, T. Vidick, Fully device independent quantum key distribution, Communications of the ACM 62 (4) (2019) 133–133.

[125] H. Zhang, Y. Mao, D. Huang, J. Li, L. Zhang, Y. Guo, Security analysis of orthogonal-frequency-division-multiplexing–based continuous-variable quantum key distribution with imperfect modulation, Physical Review A 97 (5) (2018) 052328.

[126] C. Lupo, C. Ottaviani, P. Papanastasiou, S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks, Physical Review A 97 (5) (2018) 052327.

[127] R. Y. Cai, V. Scarani, Finite-key analysis for practical implementations of quantum key distribution, New Journal of Physics 11 (4) (2009) 045024.

[128] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, X.-Q. Tan, Finite-key analysis for measurement-device-independent quantum key distribution, Physical Review A 86 (2) (2012) 022332.

[129] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nature communications 5 (1) (2014) 1–7.

[130] C. Zhou, P. Xu, W.-S. Bao, Y. Wang, Y. Zhang, M.-S. Jiang, H.-W. Li, Finite-key bound for semi-device-independent quantum key distribution, Optics express 25 (15) (2017) 16971–16980.

[131] W. Wang, K. Tamaki, M. Curty, Finite-key security analysis for quantum key distribution with leaky sources, New Journal of Physics 20 (8) (2018) 083027.

[132] J. Barrett, R. Colbeck, A. Kent, Memory attacks on device-independent quantum cryptography, Physical review letters 110 (1) (2013) 010503.

[133] B. Qi, C.-H. F. Fung, H.-K. Lo, X. Ma, Time-shift attack in practical quantum cryptosystems, arXiv preprint quant-ph/0512080.

[134] C.-H. F. Fung, B. Qi, K. Tamaki, H.-K. Lo, Phase-remapping attack in practical quantum-key-distribution systems, Physical Review A 75 (3) (2007) 032314.

[135] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nature photonics 4 (10) (2010) 686–689.

[136] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, et al., Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources, Physical Review A 84 (6) (2011) 062308.

[137] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, N. Gisin, Device-independent quantum key distribution with local Bell test, Physical Review X 3 (3) (2013) 031006.

[138] C. J. Broadbent, K. Marshall, C. Weedbrook, J. C. Howell, Device-independent quantum key distribution with generalized two-mode Schrödinger cat states, Physical Review A 92 (5) (2015) 052318.
[139] H.-K. Lo, M. Curty, B. Qi, Measurement-device-independent quantum key distribution, Physical review letters 108 (13) (2012) 130503.
[140] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, H. Guo, Continuous-variable measurement-device-independent quantum key distribution, Physical Review A 89 (5) (2014) 052301.
[141] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, L.-M. Liang, Gaussian-modulated coherent-state measurement-device-independent quantum key distribution, Physical Review A 89 (4) (2014) 042335.
[142] C. Zhou, W.-S. Bao, H.-l. Zhang, H.-W. Li, Y. Wang, Y. Li, X. Wang, Biased decoy-state measurement-device-independent quantum key distribution with finite resources, Physical Review A 91 (2) (2015) 022313.
[143] K. Tamaki, H.-K. Lo, C.-H. F. Fung, B. Qi, Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw, Physical Review A 85 (4) (2012) 042307.
[144] Y. Zhao, Y. Zhang, B. Xu, S. Yu, H. Guo, Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction, Physical Review A 97 (4) (2018) 042328.
[145] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, G.-H. Zeng, Continuous-variable measurement-device-independent quantum key distribution with photon subtraction, Physical Review A 97 (4) (2018) 042329.
[146] C.-Y. Li, Fault-tolerant measurement-device-independent quantum key distribution in a decoherence-free subspace, Quantum Information Processing 17 (10) (2018) 1–13.
[147] M. Boyer, R. Gelles, D. Kenigsberg, T. Mor, Semiquantum key distribution, Physical Review A 79 (3) (2009) 032341.
[148] M. Boyer, M. Katz, R. Liss, T. Mor, Experimentally feasible protocol for semiquantum key distribution, Physical Review A 96 (6) (2017) 062335.
[149] H. Lu, Q.-Y. Cai, Quantum key distribution with classical Alice, International Journal of Quantum Information 6 (06) (2008) 1195–1202.
[150] X. Zou, D. Qiu, L. Li, L. Wu, L. Li, Semiquantum-key distribution using less than four quantum states, Physical Review A 79 (5) (2009) 052312.
[151] A. Maitra, G. Paul, Eavesdropping in semiquantum key distribution protocol, Information Processing Letters 113 (12) (2013) 418–422.
[152] W. O. Krawec, Mediated semiquantum key distribution, Physical Review A 91 (3) (2015) 032323.
[153] X. Zou, D. Qiu, S. Zhang, P. Mateus, Semiquantum key distribution without invoking the classical party's measurement capability, Quantum Information Processing 14 (8) (2015) 2981–2996.
[154] Z.-R. Liu, T. Hwang, Mediated semi-quantum key distribution without invoking quantum measurement, Annalen der Physik 530 (4) (2018) 1700206.
[155] Z. Sun, R. Du, D. Long, Semi-quantum key distribution protocol using Bell state, arXiv preprint arXiv:1106.2910.
[156] W. Jian, Z. Sheng, Z. Quan, T. Chao-Jing, Semiquantum key distribution using entangled states, Chinese Physics Letters 28 (10) (2011) 100301.
[157] K.-F. Yu, C.-W. Yang, C.-H. Liao, T. Hwang, Authenticated semi-quantum key distribution protocol using Bell states, Quantum Information Processing 13 (6) (2014) 1457–1465.
[158] Q. Li, W. H. Chan, S. Zhang, Semiquantum key distribution with secure delegated quantum computation, Scientific reports 6 (1) (2016) 1–6.
[159] J. He, Q. Li, C. Wu, W. H. Chan, S. Zhang, Measurement-device-independent semiquantum key distribution, International Journal of Quantum Information 16 (02) (2018) 1850012.
[160] M. Boyer, D. Kenigsberg, T. Mor, Quantum key distribution with classical Bob, in: 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07), IEEE, 2007, pp. 10–10.
[161] K.-N. Zhu, N.-R. Zhou, Y.-Q. Wang, X.-J. Wen, Semi-quantum key distribution protocols with ghz states, International Journal of Theoretical Physics 57 (12) (2018) 3621–3631.
[162] W. O. Krawec, Restricted attacks on semi-quantum key distribution protocols, Quantum Information Processing 13 (11) (2014) 2417–2436.
[163] Y.-G. Yang, S.-J. Sun, Q.-Q. Zhao, Trojan-horse attacks on quantum key distribution with classical Bob, Quantum Information Processing 14 (2) (2015) 681–686.
[164] W. O. Krawec, Security of a semi-quantum protocol where reflections contribute to the secret key, Quantum Information Processing 15 (5) (2016) 2067–2090.
[165] S. Shafqat, S. Kishwer, R. U. Rasool, J. Qadir, T. Amjad, H. F. Ahmad, Big data analytics enhanced healthcare systems: a review, The Journal of Supercomputing 76 (3) (2020) 1754–1799.
[166] D. Solenov, J. Brieler, J. F. Scherrer, The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine, Missouri medicine 115 (5) (2018) 463.
[167] I. Sutskever, G. E. Hinton, G. W. Taylor, The recurrent temporal restricted Boltzmann machine, in: Advances in neural information processing systems, 2009, pp. 1601–1608.
[168] K. Bruynseels, F. Santoni de Sio, J. van den Hoven, Digital twins in health care: ethical implications of an emerging

engineering paradigm, Frontiers in genetics 9 (2018) 31.

[169] K. Rasheed, A. Qayyum, M. Ghaly, A. Al-Fuqaha, A. Razi, J. Qadir, Explainable, trustworthy, and ethical machine learning for healthcare: A survey.

[170] C. Gonzalez, Cloud based QC with Amazon Braket, Digitale Welt 5 (2) (2021) 14–17.

[171] C. Rigetti, A. Blais, M. Devoret, Protocol for universal gates in optimally biased superconducting qubits, Physical review letters 94 (24) (2005) 240502.

[172] R. Axelrod, Effective choice in the prisoner's dilemma, Journal of conflict resolution 24 (1) (1980) 3–25.

[173] P. M. Pardalos, A. Migdalas, L. Pitsoulis, Pareto optimality, game theory and equilibria, Vol. 17, Springer Science & Business Media, 2008.

[174] G. J. Mailath, Do people play Nash equilibrium? lessons from evolutionary game theory, Journal of Economic Literature 36 (3) (1998) 1347–1374.

[175] A. Qayyum, J. Qadir, M. Bilal, A. Al-Fuqaha, Secure and robust machine learning for healthcare: A survey, IEEE Reviews in Biomedical Engineering.

[176] A. Qayyum, A. Ijaz, M. Usama, W. Iqbal, J. Qadir, Y. Elkhatib, A. Al-Fuqaha, Securing machine learning in the cloud: A systematic review of cloud machine learning security, Frontiers in big Data 3.

[177] Business Wire, D-wave launches in aws marketplace (Accessed on October 23, 2022).
URL https://www.barrons.com/articles/d-wave-launches-in-aws-marketplace-01666353918