# Quantum Computing for Healthcare: A Review

Adnan Qayyum [1]

[1]Information Technology University of the Punjab

October 30, 2023

**Abstract**

Quantum computing is an emerging field of research that can provide a "quantum leap" in terms of computing performance and thereby enable many new exciting healthcare applications such as rapid DNA sequencing, drug research and discovery, personalized medicine, molecular simulations, diagnosis assistance, efficient radiotherapy. In this paper, we provide a taxonomy of existing literature on quantum healthcare systems and identify the key requirements of quantum computing implementations in the healthcare paradigm. We also provide a through exploration of the application areas where quantum computing could transform traditional healthcare systems. Finally, we perform an extensive study of quantum cryptography from the perspective of healthcare systems to identify security vulnerabilities in traditional cryptography systems.

# Quantum Computing for Healthcare: A Review

Raihan Ur Rasool[1], Hafiz Farooq Ahmad[2], Wajid Rafique[3], Adnan Qayyum[4], and Junaid Qadir[5,4]
[1] Victoria University, Melbourne, Australia
[2] King Faisal University, Al-Ahsa, Saudi Arabia
[3] University of Montreal, Montreal, QC H3C 3J7, Canada
[4] Information Technology University (ITU), Punjab, Lahore, Pakistan
[5] Qatar University, Doha, Qatar

***Abstract*—Quantum computing uses fundamentally different ways of information processing compared to traditional computing systems, e.g., using quantum bits and quantum properties of subatomic particles such as superposition, entanglement, and interference to extend the computational capabilities to unprecedented levels. Although quantum computing systems promise to provide exponential performance benefits in processing, it is still in infancy with active ongoing research and development. The efficacy of quantum computing for important verticals such as healthcare—where quantum computing can enable important breakthroughs such as developing drugs, quick DNA sequencing and performing other compute-intensive tasks—is not yet fully explored. Keeping in view, this article explores this area and analyzes the potential of quantum computing for healthcare systems. We explore application areas where quantum computing could transform traditional healthcare systems by providing higher computational speed to perform complex healthcare computations. We identify the key requirements of quantum computing implementations in the healthcare paradigm. We provide a taxonomy of existing literature on quantum healthcare systems. Moreover, we perform an extensive study of quantum cryptography from the perspective of healthcare systems to identify security vulnerabilities in traditional cryptography systems. Finally, we explore current challenges, their causes, and future research directions in implementing quantum computing systems in healthcare.**

***Index Terms*—Internet of Things, quantum computing, healthcare services, qubits.**

## I. Introduction

### A. Introduction to Quantum Computing

The roots of quantum computing lie in quantum mechanics. Quantum computing uses physical quantum phenomena such as quantum superposition and quantum entanglement. Quantum computer takes the advantage of an unusual observation in quantum physics, which represents a single bit in both '1' and '0' that is known as a quantum bit or a qubit. Using this phenomenon, quantum computing essentially creates a powerful computing infrastructure, which is capable of processing multiple pieces of data simultaneously. This enables processing of gigantic amount of information 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.

We refer the reader to Figure 1 for a comparison of classical and quantum computing paradigms 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"*. The behavior of qubits relate 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 [1].

- 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. Superposition is the trick that enables quantum computers to tick and quantum computers can use a group of qubits in superposition to shortcut through calculations and speed up computing. Since a qubit can exist in two states, the computing capacity of a q-bit quantum computer grows exponentially in the form of $2^q$.
- The *quantum entanglement* property refers to the non-intuitive fact—described by Einstein as "spooky action at a distance"—due to which an entangled pair of electrons always spin in opposite directions and influence each other through time and space even when not physically connected. This process makes quantum algorithms much more powerful than conventional ones.
- Finally, the *quantum interference* property describes how an individual particle—such as a photon (light particle)—can cross its own trajectory and interfere with its path's direction. The technology for building qubits is advancing rapidly.

Quantum computing has applications in various disciplines including communication, image processing, information theory, electronics, and cryptography as well as other related areas of life. Practical quantum algorithms are emerging with the increasing availability of quantum computers. Quantum computing posses significant potential to bring a revolution to several verticals such as cryptography, financial modeling, weather precision, physics, and transportation (an illustration of salient verticals is presented in Figure 2). Quantum computing has already been used to improve different non-quantum algorithms being used in 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.

Corresponding author: Junaid Qadir (junaid.qadir@itu.edu.pk)

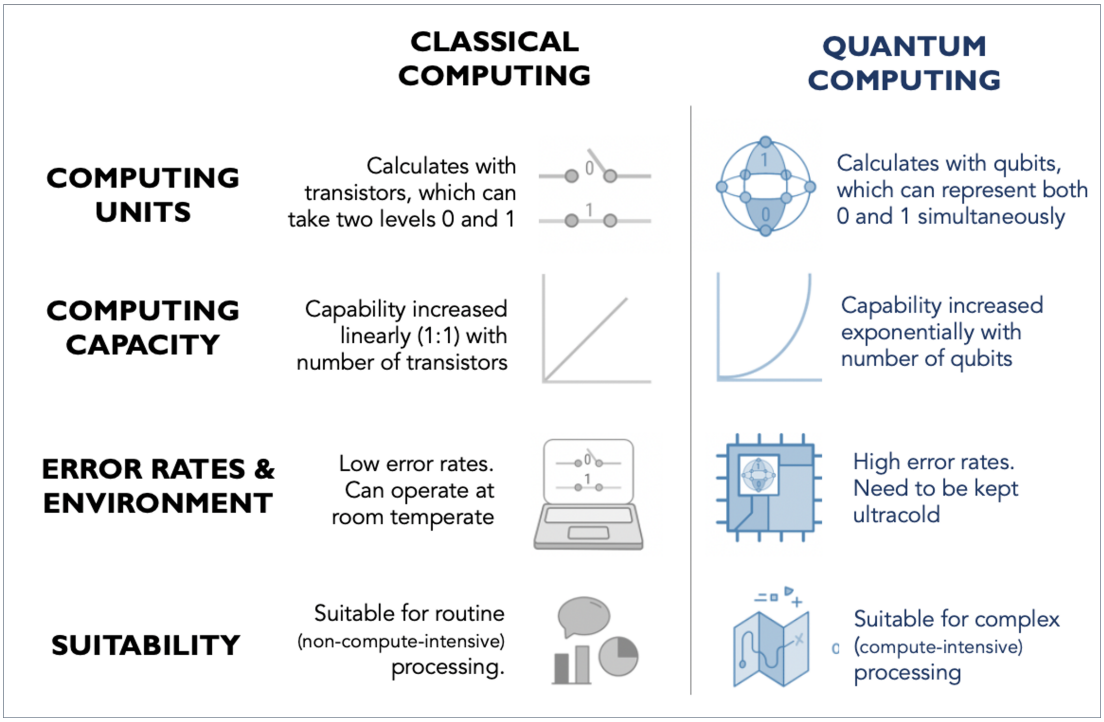


Fig. 1: Comparison of *Classical Computing vs. Quantum Computing*.

Even though quantum computing has a rich intellectual history (as depicted in the timeline of major events in Figure 3), with the term "quantum computing" coined by Richard Feynman in 1981, the field is still in its infancy. However, the field is developing rapidly. Currently popular techniques include the use of superconducting circuits or individual atoms that are levitated inside electromagnetic fields [2]. An important reason inhibiting the commoditization of quantum computing is the fact that controlling quantum effects is a delicate process and stray heat or noise can flip 0s or 1s and disrupt quantum effects such as superposition. This requires qubits to be carefully shielded and operated under special conditions such as very cold temperatures, sometimes very close to absolute zero. This also motivates research into fault tolerant quantum computing [3]. Even though quantum computing chips have not yet reached desktops or handhelds, service providers have begun offering niche quantum computing products as well as quantum cloud computing services (e.g., 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 [4]. Considering this fast-paced development of quantum computing, there is a need to find ways that could benefit traditional healthcare systems.

### *B. Quantum Computing for Healthcare*

Quantum computing is particularly well suited to numerous compute-intensive applications of healthcare [5]—especially in the current highly connected digital healthcare paradigm [6] [7], where encompasses interconnected medical devices that may be connected to the Internet or the cloud. The revenue of connected medical things was around 44.5 USD billion in 2018 and has been expected to reach 254.2 USD billion by 2025 [8]. The connected objects include medical sensors, healthcare infrastructures, machines, patients, doctors, and medical staff, etc. In this heterogeneous connected paradigm, one of the prime challenges is to monitor and ensure the efficient Quality of Services (QoS) across all the connected infrastructures. As IoT devices lack computational resources, cloud computing provides an impetus to provide resources at the edge of Internet of things (IoT).

To understand the limitations of the current healthcare systems, there is a strong need to analyze the connectivity challenges of sensors and actuators. These devices use short range communication protocols such as Bluetooth, 6LoWPAN, Zigbee, and Wi-Fi for communication. However, these devices are most of the time connected to the more powerful communication infrastructure (e.g., cloud, cellular, etc) where quantum computing is expected to be deployed in future. Whereas the long term architectures mostly connect actual remote devices (e.g., sensors and actuators) that are based on proprietary solutions, alliances, or standardized Third-Generation Partnership Project (3GPP) based cellular solutions. In this paradigm, the former two communication protocols work over the license exempt spectrum and therefore, they cannot provide QoS assurance, which is critically required in the healthcare or tactile Internet applications [9], [10]. Smart healthcare devices strive to connect healthcare objects with the Internet to provide healthcare services everywhere and all the time [7]. In such a setting, smart nodes comprising devices, things, sensors, and applications can seamlessly connect and communicate in real-time [9].

The massive increase in computational capacity can allow quantum computers to enable fundamental breakthroughs in

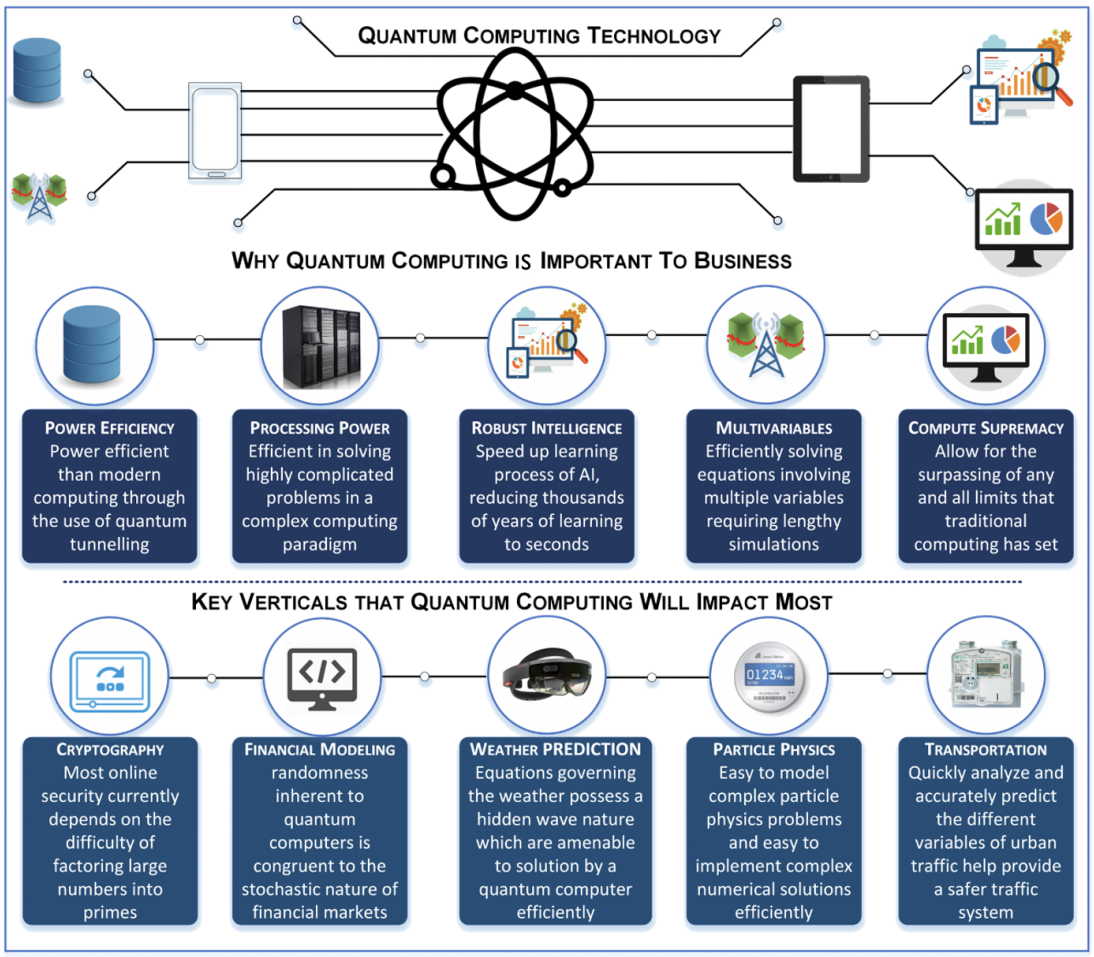


Fig. 2: *Why use quantum computing* and which *key verticals* will it disrupt?

healthcare. When we leap from bits to qubits, it could upgrade the whole healthcare paradigm as quantum computing could help realize supersonic drug design and in silico clinical trials simulated over virtual human beings. Some potential applications are listed next for an illustration. A quantum computer can do quick DNA sequencing, which opens up the possibility for personalized medicine. A quantum computer can enable the development of new therapies and medicines through more detailed modeling. A quantum computer can create efficient imaging systems that can provide clinicians more fine-grained clarity in real-time. Quantum computing can solve complex optimization problems involved in devising an optimal radiation plan that is targeted at killing the cancerous cells without damaging the surrounding healthy tissues and body parts. Quantum computing can also enable the study of complex molecular interactions at the atomic level, which will be very useful for drug discovery and medical research. Whole genome sequencing is a time-consuming and tedious task, with the help of qubits, whole-genome sequencing and analytics could be implemented in a limited amount of time. Furthermore, bringing the hospital's infrastructure to the cloud, predicting chronic diseases, and the security of medical data using fast processing of quantum computing could bring wonders in the current healthcare systems.

### C. Challenges in Efficient Healthcare Services

Healthcare infrastructure relies on the web-enabled exchange of data supporting enhanced connectivity and state-of-the-art service delivery. Smart healthcare leverages the concept of connectivity among physical and virtual worlds to provide services ubiquitously. Considering this paradigm, the security of healthcare devices becomes critically important where services could be attacked in a variety of ways [11], [12], [13]. The popularity of smart devices has been tremendously increased during the past few years, it has been envisioned that the number of IoT devices will be more than 75 billion by 2025 [14]. This gigantic growth of smart devices requires the development of standardized security and privacy protocols and architectures to provide services to the underlying IoT devices.

The sophisticated nature of healthcare infrastructure also poses challenges to security. Most of the public-key cryptography systems have become essential due to the ability to provide higher security to web services, e-mail systems, military communications, and financial transactions. In this regard, public-key cryptosystems such as Elliptic Curve Cryptography (ECC), Diffie-Hellman (DH), or Rivest-Shamir Adleman (RSA) have gained tremendous popularity. These systems are key components of different Internet standards

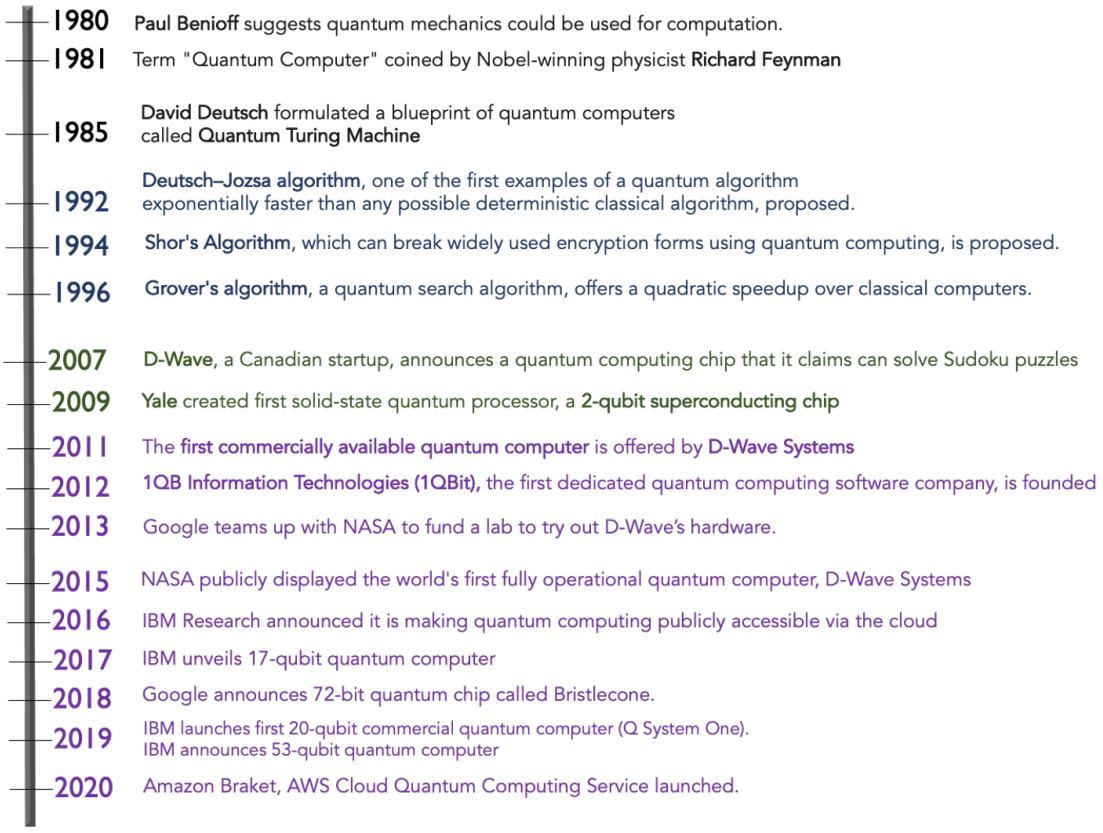


Fig. 3: *Timeline* of developments in quantum computing technology.

such as Transport Layer Security (TLS) used by conventional computers and IoT systems. However, the advancements in computing and communication technologies have made it easier to reach the computational efforts duly required to break certain asymmetric systems, which paves the way to enhancing the recommended minimum key size. Quantum computers have emerged to provide solutions to the problems that traditional computing has been unable to solve. This has been made possible by the tremendous combinatorial speed of the quantum computers acting as superposition states where the state could be one and zero simultaneously. Due to the reason that the current insurmountable combinatorial complexity, adversaries holding quantum-related characteristics, pose a significant threat to the healthcare infrastructure. Conventional Information Technology (IT) systems are expected to be patched in the future; however, patching billions of embedded IoT devices is quite challenging. Therefore, the security aspects of the current and future healthcare systems in such an attack-prone paradigm should be carefully addressed.

### *D. Motivation of this Survey*

The motivation of this survey derives from the analysis of the complex and essential requirements of the current healthcare systems such as smart pills, ingestible devices, and healthcare monitoring systems that rely on traditional computational systems. These systems comprise of computing infrastructure that is unable to fulfill the demands of future healthcare systems. Furthermore, the analysis of the challenges faced by the current healthcare systems also provides motivation for this survey. One such example is the situation experienced during the COVID-19 pandemic where the world is observing novel variants of coronavirus every few months. This poses significant challenges for the healthcare professionals working on genome sequencing of the virus. Therefore, if the variants of the coronavirus change, the whole effort using traditional computing will be exhausted. Therefore, there is a need to explore novel ways, which can speed up genome sequencing thereby paving ways to deal with the outbreaks like coronavirus. In the future, there will be a prime need to use novel ways to deal with such pandemic situations. Considering the current situation, we in this paper, provide a comprehensive survey on using quantum computing in the healthcare paradigm. To the best of our knowledge, this is the first survey that deals with the challenges of quantum computing and its applicability in the healthcare paradigm.

### *E. Comparison with Related Surveys*

Multiple surveys on quantum computing have been already presented in the literature. For instance, Gyongyosi et al. [15] 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. [16] survey the resource limitations of IoT and propose a survey of quantum cryptography solutions for IoT. They

TABLE I: A comparison of this survey with already available surveys.

| References | Year | Healthcare Focus | Security | Privacy | Architectures | Quantum Requirements | Machine/Deep Learning | Applications |
|---|---|---|---|---|---|---|---|---|
| Gyongyosi et al. [15] | 2019 | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Fernandez et al. [16] | 2019 | ✓ | ✓ | ✓ | | | ✓ | |
| Gyongyosi et al. [17] | 2018 | | | ✓ | | | ✓ | |
| Arunachalam et al. [18] | 2017 | | | | | ✓ | | |
| Li et al. [19] | 2020 | | | | | ✓ | | ✓ |
| Shaikh et al. [20] | 2016 | | | ✓ | ✓ | ✓ | ✓ | |
| Egger et al. [21] | 2020 | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Savchuk et al. [22] | 2019 | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Zhang et al. [23] | 2019 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mcgeoch et al. [24] | 2019 | | | ✓ | ✓ | | ✓ | ✓ |
| Shanon et al [25] | 2020 | ✓ | ✓ | | | | | |
| Duan et al. [26] | 2020 | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Preskill et al. [27] | 2018 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Roetteler et al. [28] | 2018 | ✓ | ✓ | ✓ | | ✓ | ✓ | |
| Upretyet al. [29] | 2020 | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Rowell et al. [30] | 2018 | | | ✓ | ✓ | ✓ | | |
| Padamvathi et al. [31] | 2016 | ✓ | ✓ | | ✓ | ✓ | | |
| Nejatollahi et al. [32] | 2019 | ✓ | ✓ | | ✓ | ✓ | | |
| Cuomo et al. [33] | 2020 | | | | ✓ | ✓ | | |
| Fingeruth et al. [34] | 2018 | | | | ✓ | ✓ | | |
| Huang et al. [35] | 2018 | | ✓ | ✓ | ✓ | ✓ | | |
| Botsinis et al. [36] | 2018 | | ✓ | ✓ | ✓ | ✓ | | |
| Ramezani et al. [37] | 2020 | | | | ✓ | ✓ | ✓ | |
| Bharti et al. [38] | 2020 | | | | ✓ | ✓ | ✓ | ✓ |
| **Our Survey** | 2021 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

developed an edge computing-based security solution for the IoT where management software deals with the security vulnerabilities of IoT. However, this is a domain-specific survey that only deals with security challenges. Gyongyosi et al. [17] discuss quantum channel capacities, which ease the quantum computing implementation for information processing. It deals with the quantum channel capacities for conventional information processing. Various other quantum-computing related surveys have been proposed in the literature such as quantum learning theories [18], [19], quantum data analytics [20], [29], quantum Machine Learning (ML) [37], [38], and quantum information security [23], [25], [28], [31]. However, these surveys consider specific aspects of quantum computing applications. Furthermore, these surveys analyzed the impacts of quantum computing implementation. Huang et al. [35] analyzed the implementation vulnerabilities in quantum cryptography systems. Botsinis et al. [36] discuss quantum search algorithms for wireless communication. Cuomo et al. [33] survey existing challenges and solutions for quantum distributed solutions and proposed a layered abstraction to deal with communication challenges. Although these surveys include different aspects of quantum computing, they lack discussion of an overall life-cycle of quantum computing. *To the best of our knowledge, this is a pioneering survey that discusses the overall implementation life-cycle of quantum computing in the healthcare domain*, covering the various critical aspects of quantum computing starting from its evolution and its applications. We discuss the quantum computing applications from different perspectives and how they could help in future problem-solving. In particular, we focus on the challenges that are being faced by the traditional systems and discuss how we could use quantum computing solutions in healthcare. Table I presents a comparison of this survey with the existing surveys.

### *F. Contributions of this Survey*

This survey systematically discusses the evolution of quantum computing and its enabling technologies. It explores the core application areas of quantum computing and analyzes the critical importance of quantum computing in the healthcare domain. We have categorically outlined the requirements of quantum computing for the implementation of high-performance healthcare systems. We highlight different aspects of quantum computing that could be used to solve real-world security problems of healthcare systems. We discuss the security implications of quantum computing for seamless healthcare services provisioning. We particularly focus on the challenges that are being faced by traditional computing systems and the perspectives of quantum computing in healthcare. We outline the taxonomies of the available literature on quantum healthcare computing solutions. In summary, the salient contributions of this survey are:

1) We provide 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 towards 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.

### G. Organization of this Survey

Table II shows acronyms and their definition. This paper has been organized as follows. 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.

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 |

## II. Quantum Computing for Healthcare: Enabling Technologies

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

### A. Hardware Structure

Since the application of quantum computer deals with user data and network components related to the conventional computing systems. Therefore, a quantum computing system should be capable enough to efficiently utilize traditional computing systems. Qubits systems require carefully orchestrated control for efficient performance; this can be managed using conventional computing principles. To understand necessary hardware components, for an analog gate-based quantum computer, the hardware could be modeled in different layers including quantum data plane, control plane, and measurement plane that are responsible for pefroming different quantum operations. The control processor plane uses measurement outcomes to determine the sequence of operations and measurements that is required by the algorithm. It also supports the host processor, which handles access to networks, large-scale storage arrays, and user interfaces.

### B. 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 [39]. Control signals that are routed to the selected qubits set the Hamiltonian path thereby controlling the gate operations for a digital quantum computer. For the gate-based systems, sometimes it requires two qubits, where the quantum data plane should provide a programmable wiring network that supports interaction of two or more qubits. Analog systems require richer communication among qubits supported by 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.

In contrast to conventional computing systems in which control and data plane are based on silicon technology. Control of quantum data plane needs different technology as compared to qubits, which is performed externally by separating control and measurement layers. Analog qubits information should be sent to the specific qubits. In some of the systems, control information is transmitted electronically using wires that are part of the quantum data plane. 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 characteristic of the quantum data plane.

### C. Quantum Control and Measurement Plane

The role of quantum plane is to convert digital signals received from the control processor. It defines a set of quantum operations that are performed on the qubits in the quantum data plane. It efficiently translates the data plane's analogue output of qubits to classical binary data that the control processor can easily handle. Any difference in the isolation of the signals leads to small qubit signals that can not be fixed during an operation thus resulting in small errors in their respective qubit state. Proper shielding of the control signals is complex since they 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 of the required constraints. Signal crosstalk and qubit manufacturing errors are systematic and they gradually change with the configuration

of the system. Even if the underlying quantum system allows fast operations, the time required to generate and transmit an exquisitely precise control pulse will limit the speed.

### D. Control Processor Plane and Host Processor

This plane recognizes and invokes a proper Hamiltonian or sequence of quantum gate operations and steps to be performed by the control and measurement plane. These sequences run the application offered by the host processor to implement a quantum algorithm. 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 the quantum error correction. Conventional data processing techniques are used to perform different quantum operations that are required for error correction according to computed results. The inferred delay may slow down the quantum computer processing. The overhead can be reduced if the error correction can be done in a comparable time to that of the time needed for the quantum operations. As the computational task increases with the machine size, this control processor plane would inevitably consist of multiple interconnected processing elements to handle increasing computational needs. However, it is quite challenging to develop a control processor plane for large size quantum machines.

One technique to solve these challenges is to split the plane into two components. The first component is a regular processor that ”runs” the quantum program, while the other component is customized (scalable) hardware that directly interacts with the control and measurement plane. 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, this plane will be attached to that computer and to fasten the execution of a few specific applications. Such kind of architecture has been employed in current computers that have accelerators for graphics, ML, and networking. These accelerators typically require a high bandwidth connection with the host processors through shared access having access to a part of their memory, which could be exploited to program the control processor that can execute the data it will be using during the process.

### E. Qubit Technologies

Since the discovery of Shor's algorithm in 1994 [40], efforts were put forward to design adequate physical 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 [41]. After its first demonstration, technical developments in qubit control have paved the way towards fully functional processors of a broad range 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) supported by the Integrated Circuits (IC), developing a quantum computer using trapped-ion qubits require the integration of a wide range of technologies including vacuum, optical, radiofrequency, laser, and coherent electronic controllers. However, the integration challenges associated with trapped-ion qubits must be thoroughly addressed before deploying a solution.

The trapped ion data plane consists of the ions that act as qubits and a trap that integrates them in the desired locations. The control and measurement plane contains different laser to perform certain operations, e.g., a precise laser source is used inflict on a specific ion to influence its quantum state. It also contain a laser to cool and capture measurements of the ions, a set of photon detectors is used to measure the state of the ions by detecting scattered photons by them.

*2) Superconducting Qubits:* Similar to the definition of the current silicon-based circuits, superconducting qubits are defined as electronic circuits. These superconducting qubits when cooled to millikelvin temperatures, show quantitative energy levels due to quantified states of electronic charge. These are sometimes called artificial atoms. Their compatibility with microwave control electronics, operating 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 placed among the forefront of the qubit modalities that are considered both for quantum computation and quantum annealing.

### F. Lessons Learned: Summary and Insights

In this section, we discuss enabling technologies of quantum computing. We found that the key characteristics of a quantum data plane are the error rates of the single-qubit and two-qubit gates. Furthermore, qubit coherence times, interqubit connectivity, and the number of qubits that reside within a single module are vital in the quantum data plane. We discussed that the speed of a quantum computer could not be faster than the precise control signals required to perform quantum operations. The control processor plane and host computer run a traditional operating system equipped with standard supporting 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 the scratch.

## III. Quantum Healthcare Applications

Quantum computing has been used in a variety of ways in the healthcare paradigm. Healthcare data has been increasing tremendously including clinical trials, registries of disease, Electronic Health Records (EHRs), and medical devices' observations. A recent estimate shows that this data has been increasing with a compound annual growth rate of 36% [42]. This increase in healthcare data supports in addressing the challenges related to the quadruple aim of providing better healthcare to the patients, lowering down the cost, better patient management, and improving the healthcare professionals' experience. In the meantime, healthcare decision-makers need to make continuous decisions based on data provided using complex systems. Current research has proved that there is a huge amount of progress in delivering the right information and powerful insights to healthcare individuals. Advancements in the industry are creating a digital experience by enforcing healthy and preventive behaviors. Alternatively, this novel data is expanding the capabilities of classical computing systems.

Recent research shows that quantum computing has an advantage over traditional computing systems. Quantum computing provides an incremental speedup of disease diagnosis and treatment. It provides an exponential increase in the computing speeds, which will enhance the computational speed from years to minutes. It provokes novel ways of realizing a higher level of skills for certain tasks, distinct IT architectures, and new corporate strategies. Moreover, quantum computing has novel characteristics for the security of healthcare given the high level of requirements of data privacy for healthcare. In healthcare, quantum computing could enable an extended range of use cases for healthcare service providers providing healthcare plans, accelerating diagnoses, medicine personalizing, and price optimization. Furthermore, due to the increase in access to health-relevant data sources, there is an increase in the use of quantum computing and classical modeling approaches to save human lives.

Although healthcare is likely to benefit extraordinarily from quantum computing, most of the early intellectual property in quantum computing is proprietary, which raises the urgency of developing quantum strategies and engage with partners and the ecosystem. In healthcare, quantum computing is going to provide exponential benefits that are challenging for traditional computer systems. Following are some of the key use cases of the applications of quantum computing in the healthcare domain. These use cases are also illustrated in Figure 4.

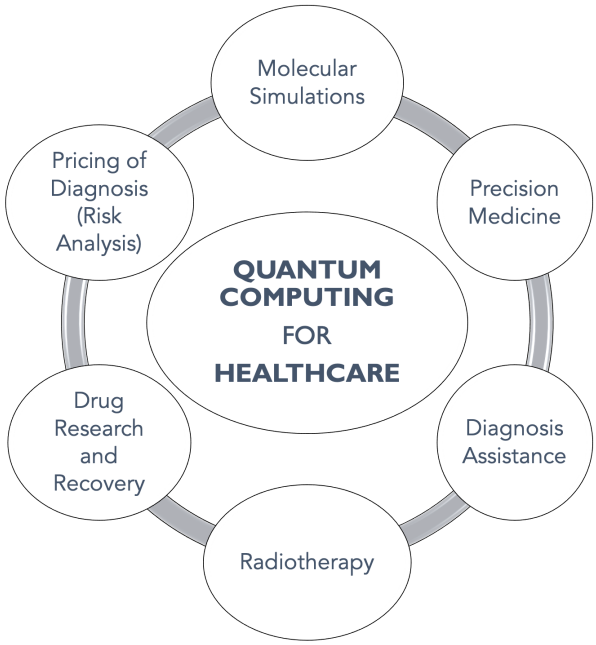


Fig. 4: Applications of *Quantum Computing for Healthcare*.

### 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 are not able to leverage quantum phenomena. In the healthcare industry, quantum computers can exploit ML, optimization, and Artificial Intelligence (AI) for complex simulations. Quantum computing helps to improve ML processes, which paves the way towards quantum advances. The modeling of complex correlations and dependencies among different highly connected elements such as molecular structures where many electrons may interact provides an efficient way of analyzing healthcare processes. The complex simulations where inherent scaling limits of relevant classical algorithms could be performed such as resource requirements of these algorithms might increase exponentially with the size of problem at hand, which could be easily managed using quantum computing.

### B. Precision Medicine

Precision medicine aims at providing prevention and treatment approaches for individuals' healthcare needs. Due to the complexity of human biological system, personalized medicine will be required in the future that will go beyond standard medical treatments. Precisely, healthcare contributes 10-20% to the outcomes, other costs includesocioeconomic factors, environmental aspects, and health-related behaviors that account for the rest of 80-90 % of the cost. Computationally, the dependencies and correlations among diverse contributors create a challenging task to optimizing the effectiveness of treatment. Therefore, many prevailing therapies are unable to achieve the intended effectiveness to the variability in individuality. For instance, only one third of individuals respond to drug-based therapies and in Europe alone more than 200,000 people die each year due to adverse drug reactions [43]. Early treatment and using preventive interventions can enhance healthcare outcomes and lower costs.

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 the level of noise and quality, size of relevant features, and the complexity of relations among features. This provokes the idea of using

quantum-enhanced ML, which could facilitate more accurate early discovery of disease in a more granular way. 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 the cancer cells. Moreover, ongoing research discovers the chemical properties of drug models that could be used to predict the efficiency of cancer at a granular level. Quantum-enhanced ML could support further breakthroughs in this area and finally enable causal inference models of drugs.

Precision medicine has the goal of identifying and explaining relationships among causes and treatments and predicting the next course of actions at an individual level. Traditional diagnosis based on 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 the diseases and allowing relevant treatments. Quantum-enhanced predictive medicine optimizes and personalizes healthcare services using continuous care. Patient's adherence and engagement at the individual-level treatments could be supported by quantum-enhanced modeling. Figure 5 shows a use case of precision medicine using the quantum computing paradigm.

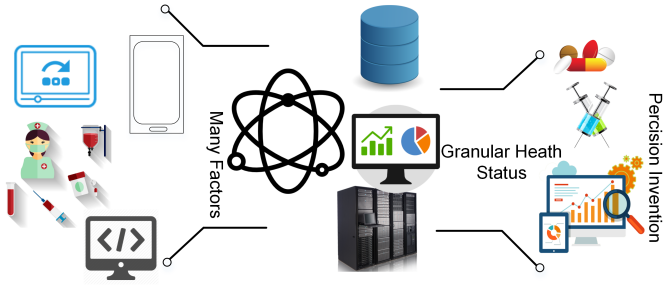


Fig. 5: *Precision medicine* using quantum computing.

### C. Diagnosis Assistance

Diagnosis performed at an earlier stage could render better diagnosis, treatment, and lower down the healthcare cost. For instance, the treatment cost lower downs 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 [44]. 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% [45]. The use of X-rays, CT scans, and MRIs have become a critical diagnosis tool over the past few years where computer-aided diagnosis has been developing at a faster pace. In this situation, treatment diagnoses suffer from noise, data quality, and replicability issues. In this regard, one of the challenges is to adhere to safety procedures. 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.

Moreover, the current techniques, use single-cell methods for diagnosis, where flow cytometry and single-cell sequencing data require analytical methods. These techniques further require advanced data analytic methods particularly combining datasets from different techniques. In this context, one challenge is the classification of cells based on the physical and biochemical characteristics, requiring an extended feature space where the predictor variable becomes considerably larger. This classification is vital for critical diagnosis such as cancerous cells integration from normal cells where quantum-enhanced ML techniques such as quantum-supported vector machines enable such classification and help in boosting single-cell diagnostic methods. Furthermore, discovering and characterizing biomarkers pave the way for the analysis of complex, omics datasets, such as genomics, transcriptomics, proteomics, and metabolomics. These processes could lead to increased feature space provoking complex correlations and patterns that are difficult to analyze using traditional computational methods. Moreover, biomarkers insights for the individual level require more advanced modeling techniques where quantum computing could help biomarkers analysis at a granular level.

During the diagnosis process, quantum computing may help to support the diagnosis insights eliminating the need for repetitive diagnosis and treatment. This paradigm helps in providing continuous monitoring and analysis of individuals' health. In addition to healthcare during diagnosis, it helps in reducing cost by early diagnosis of the disease. This 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 provoke extended data-driven diagnosis by using health plans and governments for 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 avoiding 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. Using the concept of quantum computing, the spectrum of opportunities for simulations using quantum computing is broad, which allows multiple simulations simultaneously and to develop an optimal plan faster.

### E. Drug Research and Discovery

Quantum computing allows medical practitioners to model complex molecular interactions at an atomic level, 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 approximately 20,000 proteins in the human genome

and their interactions with existing drugs can be simulated, which have not possible yet. There is an evolving trend for applying AI techniques to aid patient diagnostics. Most of the existing ML techniques correspond to pattern recognition where different ML models are trained using a large scale collection of data collected from patients thus developing a computer aided diagnosis system. Such system also allows to compare the current cases with that of the previous ones that can help in accurate diagnosis and treatment.

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 its their permutations to identify the best patterns. Using methods of known bio-barcode assay, clinicians can detect disease-specific biomarkers in the blood using gold nanoparticles that are visible using Magnetic Resonance Imaging (MRI). In this situation, the goals could be to exploit the comparisons used to help the identification of a diagnosis.

### *F. Pricing of Diagnosis (Risk Analysis)*

Precision medicine aims at tailoring preventive medicine and treatment where the complexity of the biological diagnosis at an individual's level requires considering more aspects that could go beyond the standard medical procedures. Critically, the medical care contributes to approximately 10-20% of the medical outcomes whereas the rest of 80-90% incur based on socioeconomic factors, environmental constraints, and other overheads [46]. The diagnosis includes complex interdependencies including population health levels, disease risks, cost of treatment suitability, and the exposure of risks of a health plan that is feasible at a strategic level. Although ML has considerably improved health plans, ascertaining granular models with more accuracy and lower chances of uncertainties is still a complex challenge.

In pricing analysis, quantum computing helps in risk analysis by predicting the current health of patients and predicting whether the patient has the tendency to be impacted by a particular disease. This is useful for optimizing insurance premiums and pricing [5]. The analysis of disease risks at the population level and intermixing them with the quantum risk models could help in computing financial risks and pricing models at a finer level. Furthermore, 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 on detecting and reducing healthcare frauds. Quantum computing could help in supporting higher accuracy in classification and pattern detection uncovering malicious behavior to enable malicious medical claims. This could in turn help in better managing the pricing models and offering lower premiums by lowering downs the costs associated with frauds.

Moreover, quantum computing could significantly improve pricing computations, which will help in providing lower average premiums as well as developing customized premium options. The complexity of healthcare is reflected in the challenges associated with making pricing strategies easily understandable. Indeed the novel models require transparency and lower average healthcare costs, which will help in improving pricing models.

### *G. Lessons Learned: Summary and Insights*

Different tests and systems, based on historical data, MRIs, CT scans could help line up all the applications of quantum computing where quantum computing could help in performing DNA sequencing which takes 2-3 months using classical computing. For instance, quantum computing could 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 invests 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.

## IV. Requirements of Quantum Computing for Healthcare

Quantum-enhanced computing help decrease processing time in various aspects of healthcare. The requirements of quantum computing for healthcare could not be generalized as they are different in the domain where quantum computing is applied. 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.

### *A. Computational Power*

Quantum computing considerably enhances computational power. Quantum computers follow the phenomena of physics to solve certain problems. Classical powerful computers having large-scale CPUs and GPUs are not capable of solving certain problems. This motivates the need for quantum computing. Quantum computers exploiting vast amounts of multidimensional spaces to represent large problems. The immaculate computational speed of quantum computers suggests that they would also be having bigger sizes. However, current quantum computers have the size as big as a utility fridge. The algorithms exploiting quantum wave interference are exploited to find solutions in the healthcare domain.

A prominent example of the power of quantum computing can be seen in the Grover's Search algorithm [47] 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 checking all N items. Grover's search algorithm searches all these items by checking $\sqrt{n}$ items. This shows a remarkable efficiency in computational power. An example of this is if 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.

TABLE III: *Requirements* of quantum computing for healthcare services provisioning.

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

### *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' viewpoints posing novel challenges to the integrity, confidentiality, and availability of data in the cloud. Quantum computing is a rapidly developing technology gaining tremendous breakthroughs during the past few years. Quantum computing can gain benefits from 5G/6G networks to provide novel services. In this paradigm, quantum walks deliver a universal processing model and inherent cryptographic features that could be utilized to deliver efficient cryptographic solutions for the healthcare paradigm. Quantum walks is the mechanical counterpart of traditional random walk having the capability of developing novel quantum algorithms using high speed 5G/6G networks. It could be exploited to develop cryptography protocols as well as quantum networks.

The further use-case of quantum walks of discrete quantum walks for designing secure quantum applications include pseudo-random number generator, substituting boxes, image encryption protocols, and quantum-based authentication. This could help in providing secure ways to store and transmit data using high-speed networks. The prime concern of cryptography is to provide a secure and transparent way of storing and transmitting information. The entity's data is encrypted before sending it to the cloud. In this regard, key management, encryption, decryption, and access control are handled by the intended entities to ensure data security. This could be novel research exploiting quantum technologies using 5G-healthcare to enhance the performance and resisting attacks from classical and quantum scenarios.

### *C. Higher Dimensional Quantum Communication*

Quantum information has been a strongly influenced modern technological paradigm. There is a growing interest in high-dimensional quantum states and their impact on quantum communication. The availability of enlarged Hilbert space provides numerous advantages such as large information capacity and improved noise resilience [48]. Moreover, the authors in [48], explored multiple photonic degrees of freedom for generating high-dimensional quantum states using both integrated photonics and bulk optics. Different channels were used for propagation of the quantum states, e.g., single-mode, free-space links, aquatic channels, and multicore and multimode fibers.

### *D. Scalability of Quantum Computing*

Highly connected quantum states that are continuously interacting are challenging to simulate considering their many-body Hilbert vector space that grows exponentially with the

increasing number of particles. It restricts to fewer amount of particles; thus, restricting exact diagonalization methods to few particles in practice. One of the promising methods to improve scalability is using the methods of transfer learning. It designates protocols reusing the capability of ML models to solve potentially related but different problems. We exploit physics-inspired transfer learning protocols by reusing features of the neural network quantum states.

It has been verified that even simple neural networks such as Boltzmann machines [49] can be used to precisely describe the ground state of many-body quantum systems. Transfer-learning uses the same trained model to be used for another task that is it transfer neural network quantum state parameters trained from an initial system to a similar system of a larger size. In this regard, various physics-inspired protocols can be used for transfer learning to achieve scalability. However, a system having better efficiency and effectiveness as the system size grows to provide better 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 could provide more scalability.

### *E. 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 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. The proposed method reduces the chances of catastrophic failures of quantum computers and helps in making those systems robust and reliable.

### *F. Quantum Availability of the Healthcare Systems*

In traditional systems, computing is performed near the location 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 on a quantum computer. Therefore, the availability requirements of quantum computers should be addressed carefully.

### *G. 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. In this paradigm, the requirement of coupling topology arises, qubit-to-qubit coupling is one such example where the circuit depth depends on the fidelity of the involved gates [50] [51].

Paler et al. [52] propose 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. [53] apply QAOA using a set of linear equations containing exactly three Boolean variables. This algorithm efficiently solves the input problem and provides different other benefits over classical algorithms. In [54], the authors use 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. [55] propose QAOA for fixed qubit architectures. A method for programming gate-model without considering requirements of error correction and compilation. Here, a significant amount of logical qubits will be equal to the number of qubits on the device. The proposed method uses a sequence of parameterized unitaries that reside on the qubit layout generating quantum states. Van Meter et al. [56] develop an architecture of the multicomputer optimized using Shor's factoring algorithm [57]. A quantum multicomputer is realized using a large number of nodes communicating through a quantum bus. The primary metric was the performance of the factorization process. Several optimization methods make this technique suitable for reducing latency and the circuit path.

### *H. 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 and error-correction algorithms are also executed in a distributed manner. It requires a coordinated infrastructure and communication protocol is required 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. Moreover, quantum metropolitan area networks and quantum wide area networks could also be constructed.

Van et al. [58] performed a experimental evaluation of different quantum error correction models for scalable quantum computing. Ahsan et al. [59] propose 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 [60], the authors

distributed secure ML enabling classical clients delegating remote quantum ML executed on quantum machines. In [61], 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 show that the quantum neuron module can be implemented photonically thus making the practical implementation of the model feasible. In [62], the authors consider the implementation of the quantum neural networks using quantum dots using dipole-dipole interactions and show that the implementation is versatile and feasible.

### *I. Requirements for Physical Implementation*

The current implementation of quantum computers suggests that they can be categorized into four generations [58]. 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 [59], [63], [64], [65], [66], [67], [68]. Second-generation quantum computers could 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. An open problem in these computers is the realization of the distributed quantum computing among distant points via anionic particles.

Monz et al. [69] propose a practical realization of the scalable Shor algorithm on quantum computers. Since multiple implementations of the factorization algorithm have been demonstrated using different quantum computer architectures, the general scalability of the algorithm has not been discussed. In [70], the authors propose an improved operation of exchange-coupled semiconductor quantum dots.

### *J. 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 [71] studied the implementation of basic protocols using superconducting quantum circuits. Superconducting quantum circuits are implemented for the effective realization of quantum computations and quantum information processing. In [72], the authors proposed a quantum recommendation system, which samples efficiently from an approximation of a preference matrix, which does not require reconstruction of the overall matrix. Benedetti et al. [73] proposed a classical quantum DL framework for industrial near term devices. The authors defined a hybrid quantum-classical framework to tackling high-dimensional real-world ML datasets on continuous variables. Deep learning has been utilized for low-dimensional binary representation of data. This scheme is suitable for small-scale quantum processors assisting the training of an unsupervised generative model.

### *K. Lessons Learned: Summary and Insights*

In this section, we discussed 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

In this section, we present 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 together 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, the use of solid state electronics [74], etc. The design and analysis of these components and their different architectural combinations have been widely studied in the literature.

In the literature, most of the proposed/developed quantum computing architectures are layered architecture [75], [76], which is a conventional approach to design complex information engineering architectures. So far many researchers have provided different perspectives and guidelines to design quantum computer architectures [77], [78]. For instance, the fundamental criteria for viable quantum computing was introduced in [79] and the need of a quantum error correction mechanism within the quantum computer architecture is emphasized in [80], [81]. The experimental comparison of two quantum computing architectures (i.e., IBM Quantum and a fully connected trapped-ion) is presented in [82].

### *B. Quantum Computing for Healthcare*

Different quantum computing based approaches have been presented in the literature. For instance, Liu et al. [83] proposed a logistic regression health assessment model using quantum optimal swarm optimization to detect different diseases at an early stage. Javidi [88] overviews a variety of recent research using 3D approaches for image visualization as well as quantum imaging under photon starved conditions and proposed a visualization for 3D images under photon-starved conditions. Childs [89] proposed a study using cloud-based quantum computers exploiting natural language processing on the electronic healthcare data. Datta et al. [94] proposed Aptamers for Detection and Diagnostics (ADD) and developed

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. [83] | ✓ | × | ✓ | × | × | Logistic regression |
| Janani et al. [84] | ✓ | ✓ | ✓ | × | ✓ | Blockchain |
| Qiu et al. [85] | × | ✓ | ✓ | ✓ | × | Digital signature |
| Helgeson et al. [86] | ✓ | × | × | × | × | Survey |
| Latif et al. [87] | ✓ | ✓ | ✓ | ✓ | × | Quantum walks |
| Bhavin et al. [7] | ✓ | ✓ | × | ✓ | ✓ | Blockchain |
| Javidi [88] | ✓ | × | ✓ | × | × | 3D images visualization |
| Childs [89] | ✓ | × | ✓ | × | × | Cloud computing |
| Perumal et al. [90] | ✓ | ✓ | × | × | × | Qubits quantum |
| Latif et al. [91] | ✓ | ✓ | × | × | × | Quantum watermarking |
| Hastings [92] | ✓ | × | × | × | × | Literature review |
| Grady et al. [93] | × | × | × | × | × | Quantum leadership |
| Datta et al. [94] | ✓ | × | ✓ | × | ✓ | Smartphone app |
| Koyama et al. [95] | ✓ | × | ✓ | ✓ | ✓ | High-speed wavelet |
| Narseh et al. [96] | ✓ | × | ✓ | ✓ | ✓ | DH extension |

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. [95] 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. [96] 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. [84] proposed quantum block-based scrambling and encryption for telehealth systems (image processing application), their proposed approach have 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. [85] proposed quantum digital signature for the access control of critical data in the big data paradigm that involve signing parties including the signer, the arbitrator, and the receiver. The authors do not proposed 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. Latif et al. [87] proposed quantum walk-based cryptography application, which is composed of substitution and permutations.

In a recent study [7], a hybrid framework based on blockchain and quantum computing is proposed for 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. [91] proposed two novel quantum information hiding techniques, i.e., a steganography approach and a quantum image watermarking approach. The quantum steganography approach hides a quantum secret image into a quantum cover image using a controlled-NOT gate to secure embedded data and quantum watermarking approach hides a quantum watermarking gray image into a carrier image. Perumal et al. [90] propose a quantum key management scheme with negligible overhead. However, this scheme lacks comparison with the available approaches to demonstrate its efficacy.

### D. Actual Clinical Deployment of Quantum Computing

Helgeson et al. [86] explore the impact of clinician-awareness of quantum physics principles among patients and 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 [92] suggest that healthcare professionals must be aware of the fact that quantum computing involves extensive mathematics understanding to ensure efficient services of quantum computing in healthcare applications. Similarly, Grady et al. [93] suggest 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. In the 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 define 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 Healthcare Computing

Ensuring the security of healthcare applications is of utmost importance due to their life-critical nature. One major challenge faced by healthcare researchers is the siloed-nature of healthcare systems that impedes innovation, data sharing, and systematic progress [97]. 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 [98]. 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 mechanisms. At the same time, quantum computing also offers the potential for greater security by leveraging the counterintuitive physics of subatomic particles and the principles of quantum mechanics. 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 objects 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.

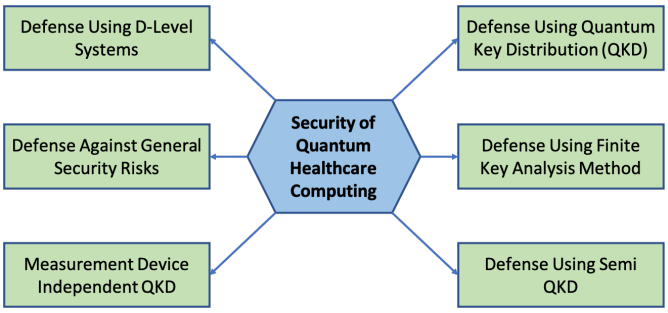


Fig. 6: Taxonomy of key technologies that can ensure security for healthcare information processing.

### A. Quantum Key Distribution

Quantum Key Distribution (QKD) authorize two components to distribute a mutually agreed upon key for the transmission security. The initial QKD technique was developed by Gilles Brassard known as BB84 [99]. In the QKD protocol, if an adversary attempts to steal information, it would be detected using the specific quantum laws. It is generally based on the complex characteristics of quantum computing, which is challenging to outperform. When the adversary attempts to steal the information, it will leave some footprints, which could be detected by QKD. The QKD allows for the generation of arbitrarily long keys whereas if the adversary tampers the communication channel, the protocol stops generating keys and identifies the attack. Moreover, to protect the quantum channel, there is a negligible chance that the QKD protocol stops working and the adversary could steal the information. The vast majority of theoretical research uses the BB84 protocol. The first proof of BB84 was provided by Shor et al. [100]. They related the security to the entanglement purification protocol and the quantum error correction code. In this paradigm, there is a substantial research conducted using QKD security protocol and several novel improvements in the security paradigm using QKD protocol have been made so far.

### B. Defense Using D-Level Systems

In [101], the authors used d-level systems to protect against individual and concurrent attacks. They discussed two cryptosystems where the first use two mutually unbiased bases and the second utilizes d+1 concurrently unbiased bases. The proof of security for the protocols with entangled photons for individual attacks have been demonstrated by [102]. However, the challenge with this approach was the increased error rate. In [103], the authors proposed the decoy pulse method for BB84 in the presence of a high loss rate. 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 [104]. In [105], 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 [106], which has been extended by [107] with a more general form of attacks. A passive approach for the security using a beam divider to segregate each input pulse and demonstrate its effectiveness is presented in [108]. Table V shows a taxonomy of the security of d-level systems.

### C. Defense Against General Security Risks

In this section, we present existing defense approaches to withstand different general attacks against quantum computing systems. Maroy et al. [109] proposed defense strategy for BB84 that enforces security with random individual imperfections concurrently in the quantum sources and detectors. A defense method using d-dimensional alphabets against coherent attacks is proposed in [110]. Pawlowski et al. [111] proposed a semi-device independent defense scheme against individual attacks. The proposed approach provides security when the devices are assumed to devise quantum systems of a given dimesion. Manses et al. [112], present a defensive scheme for a greater number of quantum protocols, where the key is generated by independent measurements. Morder et al. [113] presented a generic method to evaluate security aspects of a practical distributed phase reference QKD against general attacks. Leverrier et al. [115] demonstrated the security of Gaussian continuous variable QKD with coherent states against arbitrary attacks in the finite-size scheme, which is applicable in the practically relevant finite-sized mechanism. In [114], the authors provide the strategy 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. Defense against generic DI QKD protocols

TABLE V: Countermeasures and security protocols using *d-level systems*.

| Author | Objective | Security Algorithm | Pros | Cons |
|---|---|---|---|---|
| Cerf et al. [101] | • Quantum cryptographic schemes | • Quantum states in a d-dimensional Hilbert space<br>• Cryptosystem uses two mutually unbiased bases | • Enhanced accuracy<br>• Efficient authentication | • Increased error rate |
| Waks et al. [102] | • Design flows in security and privacy | • Quantum key distribution with entangled photons<br>• BB84 protocol | • Enhanced authentication<br>• Increased accuracy<br>• More practical paradigm | • Restricted to individual eavesdropping attacks<br>• Lack of reliability<br>• Lack of comparison |
| Hwang [103] | • Global secure communication | • Quantum key distribution<br>• Decoy pulse method | • Coherent pulse sources<br>• Generalization to any arbitrary case<br>• Resource efficiency | • Higher computational cost<br>• Require more resources<br>• Prone to attacks |
| Iblisdir et al. [104] | • Security of quantum key distribution | • Coherent States and Homodyne Detection<br>• Transmission of Gaussian-modulated coherent states | • Lowering down phase error rate<br>• Securing against any attack | • Lack of robustness<br>• Meager improvement |
| Biham et al. [105] | • Security of theoretical quantum key distribution | • Attackers reduced density matrices | • Securing against optimal attacks<br>• Extensive usage of symmetry | • Lack of scalability<br>• Complex computations |
| Acin et al. 2020 [106] | • Device-Independent security of quantum cryptography | • Quantum key cryptography<br>• Authentication algorithm | • Security against collective attacks<br>• Implementation efficiency | • Lower efficiency<br>• Implementation issues |
| Mckague et al. 2019 [107] | • Secure against coherent attacks with memoryless measurement devices | • XOR<br>• Device independent quantum key distribution | • Security againt overall attacks<br>• Improved efficiency | • Limited evaluation<br>• Low-level scope |
| Zhao et al. [108] | • Security analysis of an untrusted source | • Untrusted source scheme | • Does not require fast optical switching<br>• Reduce cost | • False-positive rate<br>• Limited efficiency |

TABLE VI: Countermeasures and security protocols for *general security risks*.

| Author | Objective | Security Algorithm | Pros | Cons |
|---|---|---|---|---|
| Maroy et al. [109] | • Security of quantum key distribution | • Quantum states in a d-dimensional<br>• Arbitrary individual imperfections | • Enhanced accuracy<br>• Efficient authentication | • Increased error rate using qudit systems |
| Sheridan et al. [110] | • Security proof for quantum key distribution | • Asymptotic regime<br>• Higher-dimensional protocols | • Secret key rate for fixed noise<br>• Increased accuracy<br>• More practical paradigm | • Restricted to individual eavesdropping attacks<br>• Lack of reliability<br>• Lack of comparison |
| Pawlowski [111] | • Security of entanglement -based quantum key | • Semi-device-independent security<br>• One-way quantum key distribution | • Coherent pulse sources<br>• Generalization to any arbitrary case<br>• Resource efficiency | • Higher computational cost<br>• Require more resources<br>• Prone to attacks |
| Masanes et al. [112] | • Secure device-independent quantum key | • Distribution with causally independent measurement devices<br>• Quantum computing laws | • Lowering down phase error rate<br>• Securing against any attack | • Lack of robustness<br>• Meager improvement |
| Moroder et al. [113] | • Security of Distributed -Phase-Reference | • Variant of the COW protocol | • Generic method for security<br>• Extensive usage of symmetry | • Lack of scalability<br>• Complex computations |
| Beaudry et al. [114] | • Security of two-way quantum key distribution | • Entropic uncertainty relation<br>• Authentication algorithm | • Security against collective attacks<br>• Implementation efficiency | • Lower efficiency<br>• Implementation issues |
| Leverrier et al. 2019 [115] | • Security of Continuous-Variable Quantum Key | • Phase-space symmetries of the protocols<br>• Gaussian continuous-variable quantum | • Applicable to relevant finite-size regime<br>• Improved efficiency | • Limited evaluation<br>• Low-level scope |
| Prionio et al. [116] | • Security of quantum key cryptography | • Untrusted source scheme | • Does not require fast optical switching<br>• Reduce cost | • False-positive rate<br>• Limited efficiency |
| Masnes et al. [117] | • Full security of quantum key distribution | • Secret key from correlations | • Does not require fast optical switching<br>• Reduce cost | • False-positive rate<br>• Limited efficiency |
| Vazirani et al. [118] | • Fully device independent quantum key distribution | • Entanglement-based protocol building | • Does not require fast optical switching<br>• Reduce cost | • False-positive rate<br>• Limited efficiency |
| Zhang et al. [119] | • Security analysis of orthogonal | • Continuous-variable quantum key distribution | • Does not require fast optical switching<br>• Reduce cost | • False-positive rate<br>• Limited efficiency |
| Lupo et al. [120] | • Continuous-variable measurement-device independent quantum | • Security against collective Gaussian attacks | • Does not require fast optical switching<br>• Reduce cost | • False-positive rate<br>• Limited efficiency |

is presented in [116]. A comparative analysis of secret keys that violate Bell inequality is presented in [117]. The authors suggested that any available information to the eavesdroppers should be consistent with the non-signaling principle. The authors in [118] particularly define the perspective of Eckert's original entanglement protocol against a general class of attacks. A framework for the continuous-variable QKD is presented in [119], which is based on orthogonal frequency division multiplexing scheme. An comprehensive security analysis of continuous variable MDI QKD in a finite-sized scenario is presented in [120]. Table VI presents the taxonomy of defenses against general security attacks.

### *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 [121], 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 is presented in [122], that 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 [123]. The authors demonstrated the feasibility of long-distance implementations of MDI QKD within a reasonable time frame of signal transmission. A practical prepare and measure partial device-independent BB84 protocol having finite resources is presented in [124]. A security analysis performed against discretionary communication exposure from the preparation process is presented in [125]. Table VII presents the taxonomy of the finite key analysis security

TABLE VII: Countermeasures and security protocols using security against *Finite Key Analysis*.

| Author | Objective | Security Algorithm | Pros | Cons |
|---|---|---|---|---|
| Cai et al. [121] | • Finite-key unconditional security | • Entanglement-based implementations<br>• Finite-key bound for prepare-and-measure | • Enhanced accuracy<br>• Efficient authentication | • Increased error rate using qudit systems |
| Song et al. [122] | • Imperfect detectors to learn a large part of the secret key | • Asymptotic regime<br>• Chernoff bound | • Secret key rate for fixed noise<br>• Increased accuracy<br>• More practical paradigm | • Restricted to individual eavesdropping attacks<br>• Lack of reliability<br>• Lack of comparison |
| Curty et al. [123] | • Finite-key analysis for device-independent measurement | • Semi-device-independent security<br>• One-way quantum key distribution | • Coherent pulse sources<br>• Generalization to any arbitrary case<br>• Resource efficiency | • Higher computational cost<br>• Require more resources<br>• Prone to attacks |
| Zhou et al. [124] | • Semi-device-independent QKD protocol | • Distribution with causally independent measurement devices<br>• Quantum computing laws | • Lowering down phase error rate<br>• Securing against any attack | • Lack of robustness<br>• Meager improvement |

schemes.

### *E. Measurement-Device-Independent Quantum Key Distribution*

DI QKD [106] aims to fulfill the gap among practical realization of the QKD without considering the working mechanism of the underlying quantum device. It requires violation of the bell inequality between both ends of the communication and can provide higher security than traditional schemes by reducing the number of required 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 of 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 [126]. In this context, DI QKD is capable of defending different kinds of security vulerablities including time-shift attacks [127], phase remapping attacks [128], binding attacks [129], and wavelength-dependent attacks [130]. Additionally, security vulnerabilities identification generated by quantum communication channels can be defended using the technique presented in [131]. Furthermore, Broadbent et al. proposed generalized two-mode Schrodinger cat states DI QKD protocol [132]. The taxonomy of the device-independent quantum key distribution is presented in Table VIII.

Lo et al. proposed a device-independent measurement scheme [133]. This schemes 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 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 nonavailability of detectors. Though they need to characterize the quantum states they transfer using channels, which occurs in a secure paradigm. This paradimg is secure from the adversary who exploits the simple encoding and decoding modules without concentrating on polarization maintenance. Li et al. propose an untrusted third-party attack detection using a continuous-variable MDI protocol [134]. Ma et al. [135] propose MDI-based scheme using Gaussian-modulated coherent states. The authors in [136], propose a decoy-state protocol. In this scheme, measurement basis is chosen having a biased probability and intensities of various types of states. An optimized strategy is used to achieve finite secret key rate.

The authors in [137] propose two techniques for phase encoding including phase-locking and conversion of BB84 standard encoding pulses into polarization modes. Zhao et al. [138] improves the performance of coherent-state continuous variable MDI protocol by virtual photon subtraction. The author in [139] improves the efficiency of the continuous variable MDI protocol by using photon subtraction.

### *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. [154] propose the first SQKD in 2007. In this scheme, they use single photons to determine the robustness of the protocol. In the later state, they extend this work by generalizing the underlying conditions. They analyze these conditions and prove that a complete robustness could only be achieved when the qubits are tranmitted individually but are attacked collectively . In their later work Boyer et al. [141] also propose a feasible protocol using four-level systems. Lu et al. [143] propose classical sender-based protocol. The sender can send encoded key bits on the Z basis. Zou et al. [144] propose a robust SQKD protocol which transfers fewer than four quantum states. Maitra et al. [145] analyze a two-way eavesdropping scheme against an SQKD protocol. Karawec et al. [146] propsoe a secret key sharing scheme between two classical users. The authors in [147] avoid measurement capabilities of the sender and ensures that it is robust against joint

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

| Author | Objective | Security Algorithm | Pros | Cons |
|---|---|---|---|---|
| Acin et al. [106] | • Device-independent cryptography against collective attacks | • Holevo information<br>• Bell-type inequality | • Generate secret key<br>• Freedom and secrecy | • Leakage of information |
| Barret et al. [126] | • Security from memory attacks | • Device-independent protocols<br>• Quantum cryptography | • Secret key rate for fixed noise<br>• Securely destroying or isolating devices<br>• More practical paradigm | • Restricted to individual eavesdropping attacks<br>• Leaking secret data.<br>• Costly and often impractical |
| Qi et al. [127] | • Security against time-shift attack | • Signal pulse synchronization pulse<br>• Time-multiplexing technique | • Simple and feasible<br>• Generalization to any arbitrary case<br>• Resource efficiency | • Higher computational cost<br>• Require more resources<br>• Final key they share is insecure |
| Fung et al. [128] | • Phase-remapping | • Unconditionally secure against Measurement devices<br>• Eavesdroppers with unlimited | • Lowering down phase error rate<br>• Securing against any attack | • Lack of robustness<br>• Meager improvement |
| Lydersen et al. [129] | • Relevant quantum property of single photons | • Commercially available QKD systems<br>• Acquire the full secret key | • Lowering down phase error rate<br>• Securing against any attack | • Lack of robustness<br>• Meager improvement |
| Li et al. [130] | • Attacking practical quantum key | • Wavelength dependent beam splitter<br>• Multi-wavelength sources | • Widespread scope<br>• Securing against any attack | • Higher error rate<br>• Higher implementation cost |
| Lim et al. [131] | • Local Bell test | • Device-independent quantum key<br>• Multi-wavelength sources | • Casually independent devices Losses in the channel is avoided. | • Implementation loopholes<br>• Side-channel attacks |
| Broadbent et al. [132] | • Device independent quantum key distribution | • Generalized two-mode Schrodinger<br>• Multi-wavelength sources | • Coherent attacks Low error rate. | • Lack of accuracy<br>• Attack vulnerabilities |
| Cao et al. [133] | • Long-distance free-space measurement | • Based on two-photon interference<br>• Multi-wavelength sources<br>• Fiber-based implementations | • Way to quantum experiments Low error rate. | • Long-distance interference<br>• Security attacks |
| Li et al. [134] | • Continuous-variable measurement | • Quantum catalysis<br>• discrete-variable<br>• Zero-photon catalysis | • Defense against attacks Simulation results. | • Lack of accuracy<br>• Attack vulnerabilities |
| Ma et al. [135] | • Measurement-device independent quantum | • Quantum catalysis<br>• High-security quantum information<br>• Gaussian-modulated coherent states | • Continuous-variable entanglement<br>• Losses in current telecom components. | • More overhead.<br>• Lack of accuracy |
| Zhou et al. [136] | • Biased decoy-state measurement | • Finite secret key rates<br>• Efficient decoy-state information<br>• Single-photon yield | • Simulation results Increased efficiency | • More overhead.<br>• Lack of accuracy |
| Tamaki et al. [137] | • Phase encoding schemes | • Basis-dependent flaw<br>• Phase encoding schemes<br>• Single-photon yield | • Non-phase-randomized coherent pulses Increased efficiency | • More overhead.<br>• Lack of accuracy |
| Zhao et al. [138] | • Phase encoding schemes | • Post selection using untrusted measurement<br>• Virtual photon subtraction<br>• Single-photon yield<br>• Non-Gaussian post-selection | • Non-phase-randomized coherent pulses Increased efficiency | • Reduced reliability<br>• Increased complexity |
| Ma et al. [139] | • Continuous-variable measurement-device | • Independent quantum key distribution via quantum catalysis<br>• Single-photon yield<br>• A noiseless attenuation process | • Single-photon subtraction coherent pulses<br>• Improving performance | • A higher secret key rate<br>• Limitation of transmission distance |
| Li et al. [140] | • Fault-tolerant measurement | • Decoherence-free subspace<br>• Collective-rotation noise<br>• Collective-dephasing noises | • Reducing experiment difficulty<br>• Enhanced security | • Lack of general noise cases<br>• Lack of improving overall efficiency |

attacks. This scheme shows that the measurement capability of the classical users is not essential for the implementation of SQKD. Liu et al. [148] use an untrusted quantum server that try to steal session keys. Currently, various quantum states and technologies are used and to devise novel protocoles [149], [150], [151], [152], [153], [155]. Additionally, some authors analyze the security vulnerabilities of SQKD [156], [157], [158]. Table IX shows the security taxonomy of the semi quantum key distribution.

### 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 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 big data for revolutionizing healthcare by enabling personalized services and better diagnostics and prognostics [159], [97]. In particular, big data for healthcare can leverage data science and machine learning to enable descriptive analytics (*what happened?*); diagnostic analytics (*why did it happen?*); predictive analytics (*what will happen?*); and prescriptive analytics (*how can we make it happen?*).

### 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 [160]. Of the various kinds of quantum algorithms that are relevant to healthcare, quantum-enhanced AI/ML stand out for the breadth of their application. Quantum approaches are particularly well suited for ML algorithms, many of which rely on operations with large matrices, which can be speeded significantly using quantum computing [5]. AI/ML is a powerful and diverse method that supports a

TABLE IX: Countermeasures and security protocols using *Semi-Quantum Key Distribution*.

| Author | Objective | Security Algorithm | Pros | Cons |
|---|---|---|---|---|
| Boyer et al. [141] | • Semi-quantum key distribution protocol | • Nonzero information acquired<br>• Measure-resend SQKD protocol | • Robust approach<br>• Eliminating information leak | • Prone to PNS attacks<br>• Lack of scope. |
| Boyer 2017 et al. [142] | • Semi-quantum key distribution | • SQKD protocols<br>• Classical Alice with a controllable mirror | • Robust approach<br>• Comprehensive security | • Lack of interoperability<br>• Increased communication overhead |
| Lu 2008 et al. [143] | • Quantum key distribution with classical Alice | • Encoding key bits<br>• Classical encoding | • Robust approach<br>• Tolerable noise | • Higher complexity<br>• More processing time |
| Zou et al. [144] | • Semi-quantum key distribution | • Photon pulses<br>• Quantum state distribution | • Robust approach<br>• Tolerable noise | • Increased latency<br>• Higher processing time |
| Maitra et al. [145] | • Eavesdropping in semi-quantum key distribution protocol | • Eavesdropping in both directions<br>• Disturbance and information leakage | • Extract more info on secret approach<br>• One-way strategy application | • Increased latency<br>• Higher processing time |
| Krawec et al. [146] | • Mediated semi-quantum key distribution | • Shared secret key<br>• Fully quantum server | • More overhead<br>• One-way strategy application | • Full quantum security<br>• Higher processing time |
| Zou et al. [147] | • Semi-quantum key distribution | • Shared secret key<br>• Fully quantum server | • Robust against joint attacks<br>• More control over classical party | • Simple strategy prone to attacks<br>• Lack of computational feasibility |
| Liu et al. [148] | • Mediated semi-quantum key distribution | • A shared secret key<br>• Untrusted third party | • Security against known attacks<br>• More secure than three-party SQKD protocol | • Higher quantum burden<br>• Unable to combat the collective-rotation noise |
| Sun et al. [149] | • MSemi-quantum key distribution protocol using Bell state | • Privacy amplification protocols<br>• Untrusted third party | • Security against known attacks<br>• More secure than three-party SQKD protocol | • Higher quantum burden<br>• Unable to combat the collective-rotation noise<br>• Higher computational complexity |
| Jian et al. [150] | • Semi-quantum key distribution using entangled states | • Maximally entangled states<br>• Quantum Alice shares a secret key with classical Bob | • Increased qubit efficiency<br>• Security against eavesdropping | • Challenges in implementing semi-quantum<br>• Increased computation overhead<br>• Higher computational complexity |
| Yu et al. [151] | • Authenticated semi-quantum key distribution | • Pre-sharing a master secret key<br>• Transmitting a working key | • Increased impersonation attack security<br>• Security against eavesdropping | • Prone to Trojan horse attacks<br>• Increased computation overhead<br>• Higher computational complexity |
| Li et al. [152] | • Semi-quantum key distribution using secure delegated quantum computation | • Establishing a secret key<br>• Secure delegated quantum computation | • Enhanced efficiency<br>• More security | • Quantum implementation challenges<br>• Network overhead<br>• Higher resource consumption |
| Li et al. [152] | • Long-distance free-space quantum Key distribution | • Establishing a secret key<br>• Secure delegated quantum computation | • Satellite quantum<br>• Long-distance security | • Noise accumulation<br>• Communication restrictions<br>• Higher resource consumption |
| He et al. [153] | • Measurement-device-independent semi-quantum key distribution | • Quantum key distribution<br>• Key distribution | • Higher security<br>• Increased reliability | • More latency<br>• Secret key leakage<br>• Side-channel attacks |
| Zhu et al. [153] | • Semi-quantum key distribution protocols with GHZ States | • Strong quantum capability<br>• Achieve quantum key distribution | • Higher security<br>• Increased reliability | • More latency<br>• Secret key leakage<br>• Side-channel attacks |

variety of applications. There are multiple traditional learning models such as the conjugate gradient method that use traditional hardware accelerators to quickly search through a tailored machine design. Quantum computing could provide support for AI/ML tasks during the machine design phase to enhance the overall robustness of the inference model. Moreover, for the fixed-machine design, inference model training can be achieved using quantum computing. A popular design using restricted Boltzmann machine [161] 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 increases 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 the informed decision-making. These inference models work on the basis of 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 suffer from a combinatorial explosion when dealing with large instances. For instance, the Traveling Salesman Problem (TSP) is a famous optimization problems that aims at identifying the shortest possible distance between the 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 for very large number of cities. In such cases, heuristics are resorted to in such cases as solving such problems on traditional computing systems simply takes an impractically long time. Quantum computing provides two probable solutions to solve these problems including quantum annealing and universal quantum computers. Furthermore, quantum annealing is an optimization heuristics that can overcome the challenges of traditional computing systems in solving optimization problems. Quantum annealing could be implemented on specialized quantum annealers that are easier to implement as compared to a universal quantum computer.

However, their efficacy over traditional computers is yet to be explored. Lightweight digital annealers simulate quantum annealers using classical computing and provide cost-effective solutions. Universal annealers are fully capable of solving quantum computing problems but their commercial implementations are rare thus pose more cost to solve optimization problems.

### *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 of 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 [162], [163]

### *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 [164] 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 computing hardware. It provides access to quantum annealing hardware from D-wave and two types of other gate-based quantum computers. These gate-based quantum computers include ion-trap devices from IonQ, and systems built on superconducting qubits from Rigetti [165]. 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 [166] where each player faces criminal charges. Pareto [167] calls for players to cooperate whereas Nash equilibrium [168] implies that both the players must defeat. Thus, there are apparent contradictions among different game theory applications. The best payoff comes from limitations of the game-abiding communication among the players. 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 Prisoner's Dilemma. Furthermore, players can achieve Pareto optimal solution provided the circumstances that they are allowed to share an entangled state between them. An extension to providing games offers online quantum resources can open a new type of gaming strategies and expand user payoffs.

### *G. Quantum Security Applications*

Cyberspace has been under a constant threat of an increasing number of attackers [169] [163]. 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 developing 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 the traditional encryption schemes. This motivates the need of quantum-resisting encryption techniques to mitigate the threats of quantum computing. 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 time span 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 [170].

### *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 to the subscribers to utilize a pay-per-use pricing model for the offered services. Users can subscribe to the services that they want and based on the consumed services, 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 having expertise in quantum systems and can develop financial models, services distributed mechanisms, and control strategies for the quantum resource distribution.

## VIII. Conclusions

Quantum computing has revolutionized traditional computational systems by bringing unimaginable speed, efficiency, and reliability. Healthcare systems can efficiently get benefits from the huge amount of computational power provided by quantum computing systems. In this research, we surveyed quantum computing solutions from the perspective of healthcare systems. We discussed novel application areas where quantum computing provides the benefits of complex computational processing. We discussed key requirements of quantum computing system implementations in the healthcare paradigm. We provided a taxonomy of existing quantum computing architectures for healthcare systems. Furthermore, we outlined quantum cryptography solutions for healthcare systems. 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.

## References


[1] 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*, vol. 126, no. 1, p. 010503, 2021.

[2] T. Simonite, "The wired guide to quantum computing." [Online]. Available: https://www.wired.com/story/wired-guide-to-quantum-computing/

[3] J. Preskill, "Fault-tolerant quantum computation," in *Introduction to quantum computation and information*. World Scientific, 1998, pp. 213–269.

[4] J. Porter, "Google confirms 'quantum supremacy' breakthrough," Date Accessed: June 16, 2021. [Online]. Available: https://www.theverge.com/2019/10/23/20928294/google-quantum-supremacy-sycamore-computer-qubit-milestone

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

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

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

[8] A. Steger, "How the Internet of Medical Things is impacting healthcare," Date Accessed: June 16, 2021. [Online]. Available: https://healthtechmagazine.net/article/2020/01/how-internet-medical-things-impacting-healthcare-perfcon0

[9] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing iot services through software defined networking and edge computing: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1761–1804, 2020.

[10] W. Rafique, M. Khan, and W. Dou, "Maintainable software solution development using collaboration between architecture and requirements in heterogeneous IoT paradigm (Short Paper)," in *International Conference on Collaborative Computing: Networking, Applications and Worksharing*. Springer, 2019, pp. 489–508.

[11] W. Rafique, X. He, Z. Liu, Y. Sun, and W. Dou, "CFADefense: A security solution to detect and mitigate crossfire attacks in software-defined IoT-edge infrastructure," in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2019, pp. 500–509.

[12] W. Rafique, M. Khan, N. Sarwar, and W. Dou, "A security framework to protect edge supported software defined Internet of Things infrastructure," in *International Conference on Collaborative Computing: Networking, Applications and Worksharing*. Springer, 2019, pp. 71–88.

[13] W. Rafique, M. Khan, X. Zhao, N. Sarwar, and W. Dou, "A blockchain-based framework for information security in intelligent transportation systems," in *International Conference on Intelligent Technologies and Applications*. Springer, 2019, pp. 53–66.

[14] K. Yunana, A. A. Alfa, S. Misra, R. Damasevicius, R. Maskeliunas, and J. Oluranti, "Internet of things: Applications, adoptions and components - a conceptual overview," in *Hybrid Intelligent Systems*, A. Abraham, T. Hanne, O. Castillo, N. Gandhi, T. Nogueira Rios, and T.-P. Hong, Eds. Cham: Springer International Publishing, 2021, pp. 494–504.

[15] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51–71, 2019.

[16] 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*, vol. 7, no. 7, pp. 6457–6480, 2019.

[17] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1149–1205, 2018.

[18] S. Arunachalam and R. de Wolf, "Guest column: A survey of quantum learning theory," *ACM SIGACT News*, vol. 48, no. 2, pp. 41–67, 2017.

[19] Y. Li, M. Tian, G. Liu, C. Peng, and L. Jiao, "Quantum optimization and quantum learning: A survey," *IEEE Access*, vol. 8, pp. 23 568–23 593, 2020.

[20] T. A. Shaikh and 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.

[21] D. J. Egger, C. Gambella, J. Marecek, S. McFaddin, M. Mevissen, R. Raymond, A. Simonetto, S. Woerner, and E. Yndurain, "Quantum computing for finance: state of the art and future prospects," *IEEE Transactions on Quantum Engineering*, 2020.

[22] M. Savchuk and A. Fesenko, "Quantum computing: Survey and analysis," *Cybernetics and Systems Analysis*, vol. 55, no. 1, pp. 10–21, 2019.

[23] H. Zhang, Z. Ji, H. Wang, and W. Wu, "Survey on quantum information security," *China Communications*, vol. 16, no. 10, pp. 1–36, 2019.

[24] C. C. McGeoch, R. Harris, S. P. Reinhardt, and P. I. Bunyk, "Practical annealing-based quantum computing," *Computer*, vol. 52, no. 6, pp. 38–46, 2019.

[25] K. Shannon, E. Towe, and O. K. Tonguz, "On the use of quantum entanglement in secure communications: a survey," *arXiv preprint arXiv:2003.07907*, 2020.

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

[27] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[28] M. Roetteler and K. M. Svore, "Quantum computing: Codebreaking and beyond," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 22–36, 2018.

[29] S. Uprety, D. Gkoumas, and D. Song, "A survey of quantum theory inspired approaches to information retrieval," *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–39, 2020.

[30] E. Rowell and Z. Wang, "Mathematics of topological quantum computing," *Bulletin of the American Mathematical Society*, vol. 55, no. 2, pp. 183–238, 2018.

[31] V. Padamvathi, B. V. Vardhan, and 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.

[32] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–41, 2019.

[33] D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem," *IET Quantum Communication*, vol. 1, no. 1, pp. 3–8, 2020.

[34] M. Fingerhuth, T. Babej, and P. Wittek, "Open source software in quantum computing," *PloS one*, vol. 13, no. 12, p. e0208561, 2018.

[35] A. Huang, S. Barz, E. Andersson, and V. Makarov, "Implementation vulnerabilities in general quantum cryptography," *New Journal of Physics*, vol. 20, no. 10, p. 103016, 2018.

[36] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum search algorithms for wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2018.

[37] S. B. Ramezani, A. Sommers, H. K. Manchukonda, S. Rahimi, and A. Amirlatifi, "Machine learning algorithms in quantum computing: A survey," in *2020 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2020, pp. 1–8.

[38] K. Bharti, T. Haug, V. Vedral, and L.-C. Kwek, "Machine learning meets quantum foundations: A brief survey," *AVS Quantum Science*, vol. 2, no. 3, p. 034101, 2020.

[39] J. K. Moser, *Lectures on Hamiltonian systems*. CRC Press, 2020.

[40] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. James, A. Gilchrist, and A. G. White, "Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement," *Physical Review Letters*, vol. 99, no. 25, p. 250505, 2007.

[41] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*, E. Grumbling and M. Horowitz, Eds. Washington, DC: The National Academies Press, 2019. [Online]. Available: https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects

[42] J. Kent, "Health it analytics: big-data-to-see-explosive-growth-challenging-healthcare organizations," December 3, 2018. [Online]. Available: https://healthitanalytics.com/news/

[43] I. Spilker, "A crash test dummy for medicine," March, 2018. [Online]. Available: https://tinyurl.com/3wxm7x7h

[44] M. Birtwistle, "Saving lives and averting costs? the case for earlier diagnosis just got stronger, cancer research uk." September 22, 2014. [Online]. Available: https://tinyurl.com/r3ypjvsp

[45] H. Singh, A. N. Meyer, and E. J. Thomas, "The frequency of diagnostic errors in outpatient care: estimations from three large observational studies involving us adult populations," *BMJ quality & safety*, vol. 23, no. 9, pp. 727–731, 2014.

[46] C. Hood, K. Gennuso, G. Swain, and B. Catlin, "County health rankings: relationships between determinant factors and health outcomes," *American journal of preventive medicine*, vol. 50, no. 2, pp. 129–135, 2016.

[47] P. Kwiat, J. Mitchell, P. Schwindt, and A. White, "Grover's search algorithm: an optical approach," *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 257–266, 2000.

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

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

[50] H. Neven, V. S. Denchev, G. Rose, and W. G. Macready, "Training a large scale classifier with the quantum adiabatic algorithm," *arXiv preprint arXiv:0912.0779*, 2009.

[51] ——, "Training a binary classifier with the quantum adiabatic algorithm," *arXiv preprint arXiv:0811.0416*, 2008.

[52] A. Paler, I. Polian, K. Nemoto, and S. J. Devitt, "Fault-tolerant, high-level quantum circuits: form, compilation and description," *Quantum Science and Technology*, vol. 2, no. 2, p. 025003, 2017.

[53] E. Farhi, J. Goldstone, and S. Gutmann, "A quantum approximate optimization algorithm," *arXiv preprint arXiv:1411.4028*, 2014.

[54] L. Gyongyosi, "Quantum state optimization and computational pathway evaluation for gate-model quantum computers," *Scientific reports*, vol. 10, no. 1, pp. 1–12, 2020.

[55] E. Farhi, J. Goldstone, S. Gutmann, and H. Neven, "Quantum algorithms for fixed qubit architectures," *arXiv preprint arXiv:1703.06199*, 2017.

[56] R. D. Van Meter, "Architecture of a quantum multicomputer optimized for Shor's factoring algorithm," *arXiv preprint quant-ph/0607065*, 2006.

[57] A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," *Reviews of Modern Physics*, vol. 68, no. 3, p. 733, 1996.

[58] R. Van Meter and S. J. Devitt, "Local and distributed quantum computation," *arXiv preprint arXiv:1605.06951*, 2016.

[59] M. Ahsan, R. V. Meter, and J. Kim, "Designing a million-qubit quantum computer using a resource performance simulator," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 12, no. 4, pp. 1–25, 2015.

[60] E. Farhi and A. W. Harrow, "Quantum supremacy through the quantum approximate optimization algorithm," *arXiv preprint arXiv:1602.07674*, 2016.

[61] K. H. Wan, O. Dahlsten, H. Kristjánsson, R. Gardner, and M. Kim, "Quantum generalisation of feedforward neural networks," *NPJ Quantum information*, vol. 3, no. 1, pp. 1–8, 2017.

[62] M. V. Altaisky, N. N. Zolnikova, N. E. Kaputkina, V. A. Krylov, Y. E. Lozovik, and N. S. Dattani, "Towards a feasible implementation of quantum neural networks using quantum dots," *Applied Physics Letters*, vol. 108, no. 10, p. 103108, 2016.

[63] R. Blakestad, C. Ospelkaus, A. VanDevender, J. Amini, J. Britton, D. Leibfried, and D. J. Wineland, "High-fidelity transport of trapped-ion qubits through an X-junction trap array," *Physical review letters*, vol. 102, no. 15, p. 153002, 2009.

[64] K. R. Brown, J. Kim, and C. Monroe, "Co-designing a scalable quantum computer with trapped atomic ions," *NPJ Quantum Information*, vol. 2, no. 1, pp. 1–10, 2016.

[65] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Physical review letters*, vol. 74, no. 20, p. 4091, 1995.

[66] L.-M. Duan, M. Madsen, D. Moehring, P. Maunz, R. Kohn Jr, and C. Monroe, "Probabilistic quantum gates between remote atoms through interference of optical frequency qubits," *Physical Review A*, vol. 73, no. 6, p. 062324, 2006.

[67] W. Hensinger, S. Olmschenk, D. Stick, D. Hucul, M. Yeo, M. Acton, L. Deslauriers, C. Monroe, and J. Rabchuk, "T-junction ion trap array for two-dimensional ion shuttling, storage, and manipulation," *Applied Physics Letters*, vol. 88, no. 3, p. 034101, 2006.

[68] D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark, and C. Monroe, "Modular entanglement of atomic qubits using photons and phonons," *Nature Physics*, vol. 11, no. 1, pp. 37–42, 2015.

[69] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, "Realization of a scalable shor algorithm," *Science*, vol. 351, no. 6277, pp. 1068–1070, 2016.

[70] M. Reed, B. Maune, R. Andrews, M. Borselli, K. Eng, M. Jura, A. Kiselev, T. Ladd, S. Merkel, I. Milosavljevic *et al.*, "Reduced sensitivity to charge noise in semiconductor spin qubits via symmetric operation," *Physical review letters*, vol. 116, no. 11, p. 110402, 2016.

[71] L. Lamata, "Basic protocols in quantum reinforcement learning with superconducting circuits," *Scientific reports*, vol. 7, no. 1, pp. 1–10, 2017.

[72] I. Kerenidis and A. Prakash, "Quantum recommendation systems," *arXiv preprint arXiv:1603.08675*, 2016.

[73] M. Benedetti, J. Realpe-Gómez, and A. Perdomo-Ortiz, "Quantum-assisted helmholtz machines: A quantum–classical deep learning framework for industrial datasets in near-term devices," *Quantum Science and Technology*, vol. 3, no. 3, p. 034007, 2018.

[74] D. Copsey, M. Oskin, F. Impens, T. Metodiev, A. Cross, F. T. Chong, I. L. Chuang, and J. Kubiatowicz, "Toward a scalable, silicon-based quantum computing architecture," *IEEE Journal of selected topics in quantum electronics*, vol. 9, no. 6, pp. 1552–1569, 2003.

[75] N. C. Jones, R. Van Meter, A. G. Fowler, P. L. McMahon, J. Kim, T. D. Ladd, and Y. Yamamoto, "Layered architecture for quantum computing," *Physical Review X*, vol. 2, no. 3, p. 031007, 2012.

[76] K. M. Svore, A. V. Aho, A. W. Cross, I. Chuang, and I. L. Markov, "A layered software architecture for quantum computing design tools," *Computer*, vol. 39, no. 1, pp. 74–83, 2006.

[77] T. P. Spiller, W. J. Munro, S. D. Barrett, and P. Kok, "An introduction to quantum information processing: applications and realizations," *Contemporary Physics*, vol. 46, no. 6, pp. 407–436, 2005.

[78] R. v. Meter and M. Oskin, "Architectural implications of quantum computing technologies," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 2, no. 1, pp. 31–63, 2006.

[79] D. P. DiVincenzo, "The physical implementation of quantum computation," *Fortschritte der Physik: Progress of Physics*, vol. 48, no. 9-11, pp. 771–783, 2000.

[80] A. M. Steane, "Quantum computer architecture for fast entropy extraction," *arXiv preprint quant-ph/0203047*, 2002.

[81] ——, "How to build a 300 bit, 1 giga-operation quantum computer," *arXiv preprint quant-ph/0412165*, 2004.

[82] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Experimental comparison of two quantum computing architectures," *Proceedings of the National Academy of Sciences*, vol. 114, no. 13, pp. 3305–3310, 2017.

[83] Z. Liu, X. Liang, and 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.

[84] T. Janani and M. Brindha, "A secure medical image transmission scheme aided by quantum representation," *Journal of Information Security and Applications*, vol. 59, p. 102832, 2021.

[85] L. Qiu, F. Cai, and G. Xu, "Quantum digital signature for the access control of sensitive data in the big data era," *Future Generation Computer Systems*, vol. 86, pp. 372–379, 2018.

[86] H. L. Helgeson, C. K. Peyerl, and M. Solheim-Witt, "Quantum physics principles and communication in the acute healthcare setting: a pilot study," *EXPLORE: The Journal of Science & Healing*, vol. 12, no. 6, pp. 408–415, 2016.

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

[88] 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.

[89] 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*, 2020.

[90] A. M. Perumal and 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*, pp. 1–8, 2020.

[91] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21 075–21 083, 2018.

[92] J. Hastings, "Modern nursing and modern physics: does quantum theory contain useful insights for nursing practice and healthcare management?" *Nursing Philosophy*, vol. 3, no. 3, pp. 205–212, 2002.

[93] T. Porter-O'Grady, "Quantum mechanics and the future of healthcare leadership," *JONA: The Journal of Nursing Administration*, vol. 27, no. 1, pp. 15–20, 1997.

[94] 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*, 2020.

[95] T. Koyama, N. Shibata, S. Kino, A. Sugiyama, N. Akikusa, and Y. Matsuura, "A compact mid-infrared spectroscopy system for healthcare applications based on a wavelength-swept, pulsed quantum cascade laser," *Sensors*, vol. 20, no. 12, p. 3438, 2020.

[96] V. S. Naresh, M. M. Nasralla, S. Reddi, and I. García-Magariño, "Quantum Diffie–Hellman Extended to Dynamic Quantum Group Key Agreement for e-Healthcare Multi-Agent Systems in Smart Cities," *Sensors*, vol. 20, no. 14, p. 3940, 2020.

[97] S. Latif, J. Qadir, S. Farooq, and M. A. Imran, "How 5G wireless (and concomitant technologies) will revolutionize healthcare?" *Future Internet*, vol. 9, no. 4, p. 93, 2017.

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

[99] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[100] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical review letters*, vol. 85, no. 2, p. 441, 2000.

[101] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Physical review letters*, vol. 88, no. 12, p. 127902, 2002.

[102] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," *Physical Review A*, vol. 65, no. 5, p. 052310, 2002.

[103] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[104] S. Iblisdir, G. Van Assche, and N. Cerf, "Security of quantum key distribution with coherent states and homodyne detection," *Physical review letters*, vol. 93, no. 17, p. 170502, 2004.

[105] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," *Journal of cryptology*, vol. 19, no. 4, pp. 381–439, 2006.

[106] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, no. 23, p. 230501, 2007.

[107] M. McKague, "Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices," *New Journal of Physics*, vol. 11, no. 10, p. 103037, 2009.

[108] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, "Security analysis of an untrusted source for quantum key distribution: passive approach," *New Journal of Physics*, vol. 12, no. 2, p. 023024, 2010.

[109] Ø. Marøy, L. Lydersen, and J. Skaar, "Security of quantum key distribution with arbitrary individual imperfections," *Physical Review A*, vol. 82, no. 3, p. 032337, 2010.

[110] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Physical Review A*, vol. 82, no. 3, p. 030301, 2010.

[111] M. Pawłowski and N. Brunner, "Semi-device-independent security of one-way quantum key distribution," *Physical Review A*, vol. 84, no. 1, p. 010302, 2011.

[112] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," *Nature communications*, vol. 2, no. 1, pp. 1–7, 2011.

[113] 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*, vol. 109, no. 26, p. 260501, 2012.

[114] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, "Security of two-way quantum key distribution," *Physical Review A*, vol. 88, no. 6, p. 062302, 2013.

[115] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, "Security of continuous-variable quantum key distribution against general attacks," *Physical review letters*, vol. 110, no. 3, p. 030502, 2013.

[116] S. Pironio, L. Masanes, A. Leverrier, and A. Acín, "Security of device-independent quantum key distribution in the bounded-quantum-storage model," *Physical Review X*, vol. 3, no. 3, p. 031007, 2013.

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

[118] U. Vazirani and T. Vidick, "Fully device independent quantum key distribution," *Communications of the ACM*, vol. 62, no. 4, pp. 133–133, 2019.

[119] H. Zhang, Y. Mao, D. Huang, J. Li, L. Zhang, and Y. Guo, "Security analysis of orthogonal-frequency-division-multiplexing–based continuous-variable quantum key distribution with imperfect modulation," *Physical Review A*, vol. 97, no. 5, p. 052328, 2018.

[120] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks," *Physical Review A*, vol. 97, no. 5, p. 052327, 2018.

[121] R. Y. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," *New Journal of Physics*, vol. 11, no. 4, p. 045024, 2009.

[122] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, "Finite-key analysis for measurement-device-independent quantum key distribution," *Physical Review A*, vol. 86, no. 2, p. 022332, 2012.

[123] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature communications*, vol. 5, no. 1, pp. 1–7, 2014.

[124] C. Zhou, P. Xu, W.-S. Bao, Y. Wang, Y. Zhang, M.-S. Jiang, and H.-W. Li, "Finite-key bound for semi-device-independent quantum key distribution," *Optics express*, vol. 25, no. 15, pp. 16 971–16 980, 2017.

[125] W. Wang, K. Tamaki, and M. Curty, "Finite-key security analysis for quantum key distribution with leaky sources," *New Journal of Physics*, vol. 20, no. 8, p. 083027, 2018.

[126] J. Barrett, R. Colbeck, and A. Kent, "Memory attacks on device-independent quantum cryptography," *Physical review letters*, vol. 110, no. 1, p. 010503, 2013.

[127] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *arXiv preprint quant-ph/0512080*, 2005.

[128] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Physical Review A*, vol. 75, no. 3, p. 032314, 2007.

[129] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by

tailored bright illumination," *Nature photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[130] 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*, vol. 84, no. 6, p. 062308, 2011.

[131] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, "Device-independent quantum key distribution with local Bell test," *Physical Review X*, vol. 3, no. 3, p. 031006, 2013.

[132] C. J. Broadbent, K. Marshall, C. Weedbrook, and J. C. Howell, "Device-independent quantum key distribution with generalized two-mode Schrödinger cat states," *Physical Review A*, vol. 92, no. 5, p. 052318, 2015.

[133] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[134] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution," *Physical Review A*, vol. 89, no. 5, p. 052301, 2014.

[135] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, "Gaussian-modulated coherent-state measurement-device-independent quantum key distribution," *Physical Review A*, vol. 89, no. 4, p. 042335, 2014.

[136] C. Zhou, W.-S. Bao, H.-l. Zhang, H.-W. Li, Y. Wang, Y. Li, and X. Wang, "Biased decoy-state measurement-device-independent quantum key distribution with finite resources," *Physical Review A*, vol. 91, no. 2, p. 022313, 2015.

[137] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw," *Physical Review A*, vol. 85, no. 4, p. 042307, 2012.

[138] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction," *Physical Review A*, vol. 97, no. 4, p. 042328, 2018.

[139] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, "Continuous-variable measurement-device-independent quantum key distribution with photon subtraction," *Physical Review A*, vol. 97, no. 4, p. 042329, 2018.

[140] C.-Y. Li, "Fault-tolerant measurement-device-independent quantum key distribution in a decoherence-free subspace," *Quantum Information Processing*, vol. 17, no. 10, pp. 1–13, 2018.

[141] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, "Semiquantum key distribution," *Physical Review A*, vol. 79, no. 3, p. 032341, 2009.

[142] M. Boyer, M. Katz, R. Liss, and T. Mor, "Experimentally feasible protocol for semiquantum key distribution," *Physical Review A*, vol. 96, no. 6, p. 062335, 2017.

[143] H. Lu and Q.-Y. Cai, "Quantum key distribution with classical Alice," *International Journal of Quantum Information*, vol. 6, no. 06, pp. 1195–1202, 2008.

[144] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, "Semiquantum-key distribution using less than four quantum states," *Physical Review A*, vol. 79, no. 5, p. 052312, 2009.

[145] A. Maitra and G. Paul, "Eavesdropping in semiquantum key distribution protocol," *Information Processing Letters*, vol. 113, no. 12, pp. 418–422, 2013.

[146] W. O. Krawec, "Mediated semiquantum key distribution," *Physical Review A*, vol. 91, no. 3, p. 032323, 2015.

[147] X. Zou, D. Qiu, S. Zhang, and P. Mateus, "Semiquantum key distribution without invoking the classical party's measurement capability," *Quantum Information Processing*, vol. 14, no. 8, pp. 2981–2996, 2015.

[148] Z.-R. Liu and T. Hwang, "Mediated semi-quantum key distribution without invoking quantum measurement," *Annalen der Physik*, vol. 530, no. 4, p. 1700206, 2018.

[149] Z. Sun, R. Du, and D. Long, "Semi-quantum key distribution protocol using Bell state," *arXiv preprint arXiv:1106.2910*, 2011.

[150] W. Jian, Z. Sheng, Z. Quan, and T. Chao-Jing, "Semiquantum key distribution using entangled states," *Chinese Physics Letters*, vol. 28, no. 10, p. 100301, 2011.

[151] K.-F. Yu, C.-W. Yang, C.-H. Liao, and T. Hwang, "Authenticated semi-quantum key distribution protocol using Bell states," *Quantum Information Processing*, vol. 13, no. 6, pp. 1457–1465, 2014.

[152] Q. Li, W. H. Chan, and S. Zhang, "Semiquantum key distribution with secure delegated quantum computation," *Scientific reports*, vol. 6, no. 1, pp. 1–6, 2016.

[153] J. He, Q. Li, C. Wu, W. H. Chan, and S. Zhang, "Measurement-device-independent semiquantum key distribution," *International Journal of Quantum Information*, vol. 16, no. 02, p. 1850012, 2018.

[154] M. Boyer, D. Kenigsberg, and 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.

[155] K.-N. Zhu, N.-R. Zhou, Y.-Q. Wang, and X.-J. Wen, "Semi-quantum key distribution protocols with ghz states," *International Journal of Theoretical Physics*, vol. 57, no. 12, pp. 3621–3631, 2018.

[156] W. O. Krawec, "Restricted attacks on semi-quantum key distribution protocols," *Quantum Information Processing*, vol. 13, no. 11, pp. 2417–2436, 2014.

[157] Y.-G. Yang, S.-J. Sun, and Q.-Q. Zhao, "Trojan-horse attacks on quantum key distribution with classical Bob," *Quantum Information Processing*, vol. 14, no. 2, pp. 681–686, 2015.

[158] W. O. Krawec, "Security of a semi-quantum protocol where reflections contribute to the secret key," *Quantum Information Processing*, vol. 15, no. 5, pp. 2067–2090, 2016.

[159] S. Shafqat, S. Kishwer, R. U. Rasool, J. Qadir, T. Amjad, and H. F. Ahmad, "Big data analytics enhanced healthcare systems: a review," *The Journal of Supercomputing*, vol. 76, no. 3, pp. 1754–1799, 2020.

[160] D. Solenov, J. Brieler, and J. F. Scherrer, "The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine," *Missouri medicine*, vol. 115, no. 5, p. 463, 2018.

[161] I. Sutskever, G. E. Hinton, and G. W. Taylor, "The recurrent temporal restricted Boltzmann machine," in *Advances in neural information processing systems*, 2009, pp. 1601–1608.

[162] K. Bruynseels, F. Santoni de Sio, and J. van den Hoven, "Digital twins in health care: ethical implications of an emerging engineering paradigm," *Frontiers in genetics*, vol. 9, p. 31, 2018.

[163] K. Rasheed, A. Qayyum, M. Ghaly, A. Al-Fuqaha, A. Razi, and J. Qadir, "Explainable, trustworthy, and ethical machine learning for healthcare: A survey," 2021.

[164] C. Gonzalez, "Cloud based QC with Amazon Braket," *Digitale Welt*, vol. 5, no. 2, pp. 14–17, 2021.

[165] C. Rigetti, A. Blais, and M. Devoret, "Protocol for universal gates in optimally biased superconducting qubits," *Physical review letters*, vol. 94, no. 24, p. 240502, 2005.

[166] R. Axelrod, "Effective choice in the prisoner's dilemma," *Journal of conflict resolution*, vol. 24, no. 1, pp. 3–25, 1980.

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

[168] G. J. Mailath, "Do people play Nash equilibrium? lessons from evolutionary game theory," *Journal of Economic Literature*, vol. 36, no. 3, pp. 1347–1374, 1998.

[169] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha, "Secure and robust machine learning for healthcare: A survey," *IEEE Reviews in Biomedical Engineering*, 2020.

[170] A. Qayyum, A. Ijaz, M. Usama, W. Iqbal, J. Qadir, Y. Elkhatib, and A. Al-Fuqaha, "Securing machine learning in the cloud: A systematic review of cloud machine learning security," *Frontiers in big Data*, vol. 3, 2020.