International Journal of Data Informatics and Intelligent computing (IJDIIC)
Vol. 2, No. 2, June 2023, pp. 55~62
DOI: 10.59461/ijdiic.v2i2.61

A Review of Significant Challenges with Quantum Communication and Computing

S.Subash Chandra Bose[1], V.Shafeeq Ahmed[1]
[1]Department of Computer Science, Islamiah College (Autonomous), Vaniyambadi, Tamil Nadu, India.

Article Info

Article history:

Received June 01, 2023
Revised June 18, 2023
Accepted June 20, 2023

Keywords:

Quantum Technology
Quantum Networking
Quantum Entanglement
Quantum Cryptography

ABSTRACT

Recent times have witnessed tremendous competition towards quantum optics in business as well as academia, motivated by rapid growth in quantum computing. Overall scalability of quant present invention relates generally has exceeded several orders of magnitude, whereas ubiquitous quantum computers has accommodated as many as hundreds of quantum bits (i.e., thousands of qubits). Robust machines are still being created. Therefore, ethnicity has motivated an immense amount of research papers and reports. For all those people who read would really like to learn further the concepts of quant communication and computing from the machine learning perspective, this article provides an introduction. It begins with such an informative approach until continuing well over key turning points and most recent developments in quantum computing. These core features of such a virtual network are broken down into four significant issues in this paper, each of which has been closely investigated. A, B, C, and D are quantum mechanics, networking, security, and algorithms, accordingly. The article wraps up with the major challenges, the significant research areas, as well as the latest developments.

Corresponding Author:

S. Subash Chandra Bose
Department of Computer Science
Islamiah College (Autonomous)
Vaniyambadi
Tamil Nadu, India.
Email: bose.milestone@gmail.com

1. INTRODUCTION

Information processing technology analyses and distributes information is utilized quantum states in science, also including entangled. As such, including for challenges of rises up, qubits could solve complex mathematical problems at the rate exceeding we initially assumed was unachievable (NP-Complete). Quantum computer allow humans to solve issues that are far too demanding for computational complexity to resolve (including such massive number decomposition and ruthlessness research).

Neither academic nor enterprise are witnessing the explosive growth of quantum technology (sometimes referred as that of the race of the quantum systems) [1]. For instance, scientific businesses and organizations across the world have created quantum equipment for just a key distribution system [2][3][4]. Heterogeneous techniques (including such quantum consistency from the scientist's viewpoint or high computational from a computation researcher's viewpoint) are also what contribute to recent advancement in quantum. One widely used measure to demonstrate the strength of someone using quantum technologies is the amount of quantum bits (i.e., quantum bits) in such a quantum algorithm. Regarding ubiquitous computing power and quantum annealers, this amount has now entered the region of a couple of orders of magnitude (hundreds of qubits) and triple magnitudes of an order (millions and millions of qubits).

Whereas the technologies perform multiple objectives, quantum annealers as well as intelligent machines are also both kinds of physical equipment. Machines were originally developed to simulate quantum entanglement; although, the concept was subsequently expanded to include the complete computer resources of such an Automaton [5]. This much more over is regularly alluded to as a global quantum algorithm. Generally, these are carried out using quantum digital logic (c.f., classical logic gates). Alternatively, classical annealed exploits computational probabilities to resolve scalability issue (for discovering a global optimum). In just this article, except as otherwise specified, the terminology "Computer Program" relates to all types of computational technology developed for different purposes.

A quantum computer requires several system performance in addition to the total number of quantum bits, including such relatively continuous basis to achieve (versus decoherence, for instance [6][7][8], equipment mass (to keep the physical dimensions suitably modest and preserving made great progress, such instance), and fault - tolerant (e.g., quantum error correction [9]). Both distance of a communications network and also the mechanism of transmission of data (wiring through fibres, such instance [10][11][12][13][14] or wireless via satellites, for instance [15][16][17]) were frequent parameters in a communication system.

In spite of the fact of quantum computing remains to be in its development, it's indeed significant as it has the ability to transform the conventional architecture. As per latest estimates, worldwide world's involvement in quantum computing could approach approximately $50 million by both the mid of 202. Quantum computing makes up one of the Best ten Significant Science and technology Trends for the coming year as per Forrester. Research predicted that there's going to be hype around quantum computing for the at least 5 - 10 additional years in its 2021, Trend on Computational Architecture report. A multiyear hyped might indicate that it's going to take at least 10 years for it to develop prior to being able to produce positive outcomes. And still, it was additionally projected that just by 2025; approximately 40% of huge companies will provide quantum virtual machines.

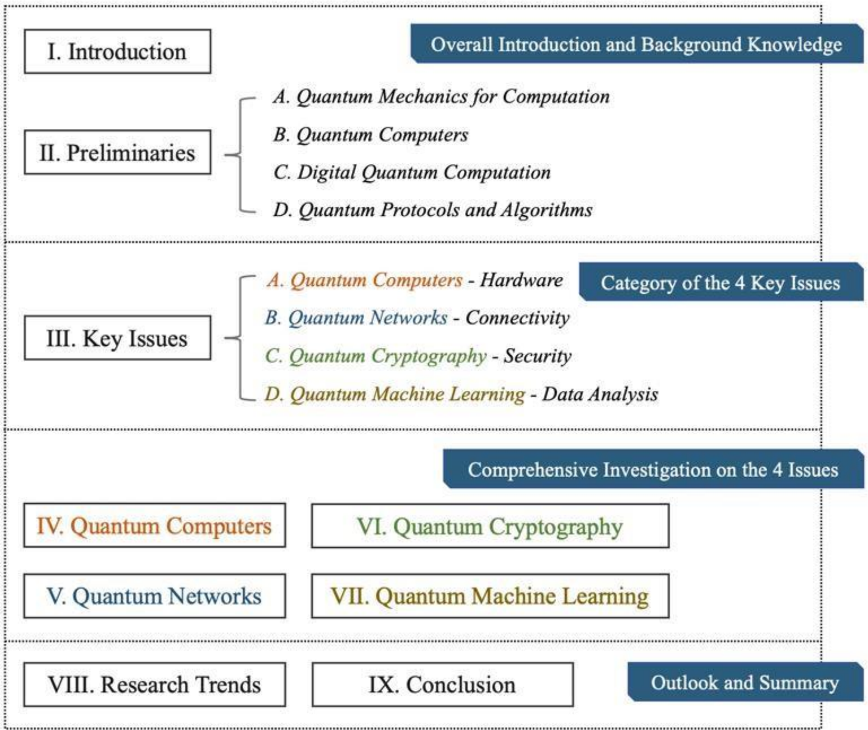

Figure 1. Connections and Outlines between components

Tech giants like IBM, Google, and Intel have demonstrated significant interest in quantum computing over the past few years. Quantum companies such as D-Wave, IonQ, and Rigetti have continuously announced their breakthroughs in quantum hardware and software development kits (SDKs). This uptick in hardware has stimulated the development of quantum applications, e.g., quantum as a service, quantum machine learning, and quantum key distribution (QKD) networks. Through quantum applications, we have seen new ways to exchange secret keys (e.g., QKD), new solutions for hyper- scale machine learning (e.g., quantum annealing), and different ways to access a quantum system (e.g., quantum simulators or remote quantum labs). Internet service providers such as Google's Aws and Intel's Azure offer beginning to do is provide clouds quant computing capabilities upon accessing the quantum region. Those advancements illustrate how well the forthcoming era of intellectual networked devices is influenced by quantum computing as well as communication.

In contrast to traditional technologies, quantum computing and communication systems have always had the ability to substantially improve the effectiveness of certain activities, hence the reason technologies are getting much more consideration. In figure 1 we compared with traditional processors, quantum computers become way more efficient in resolving various computations, optimizing, including local search. Quantum computers, that have now use in science and physical properties, would influence the behaviour of certain physical processes more effectively then general - purpose computers. An instance is indeed the wireless network, which could provide better trustworthy and safe interactions than distributed systems.

The significance and attention in quantum computing challenges throughout research has been one of the key drivers behind all this research. Researchers encourage engaged individuals to comprehend the core concepts underlying quantum computing. A beginner towards the subject can immediately easily become overwhelmed considering the enormous amount of information and data produced by the fast development of quantum technologies. Throughout this article, we explain major aspects (from the computing scientific perspective) prior applying these instead of presenting threatening terms and concepts explicitly.

Designers give viewers a practical approach that enable readers become comfortable to related concepts and standardized derivations. Instead of merely identifying the much more conventional technologies, we assess and evaluate key major turning periods including technological trends on quantum computing. Designers address the four major challenges that we have classified the top trending issues in quantum computing into: a) quantum machines, b) quantum communications, c) cryptographic algorithms, and d) quantum algorithms. Possible future research opportunities and phenomena were recognized and addressed.

2. QUANTUM PRELIMINARIES

Numerous areas of research, such quantum chemical, the theory of quantum fields, and information processing science, are founded on the concepts of quantum systems. Just at scale of subatomic particles and atoms, the concept establishes the laws of thermodynamics. There at convergence of science, maths (particularly Computational geometry and Predicate logic), with information technology resides quantum mechanics, otherwise referred to as quantum science. We primarily discuss computer technology from a computer engineering perspective throughout this section in Figure 2.

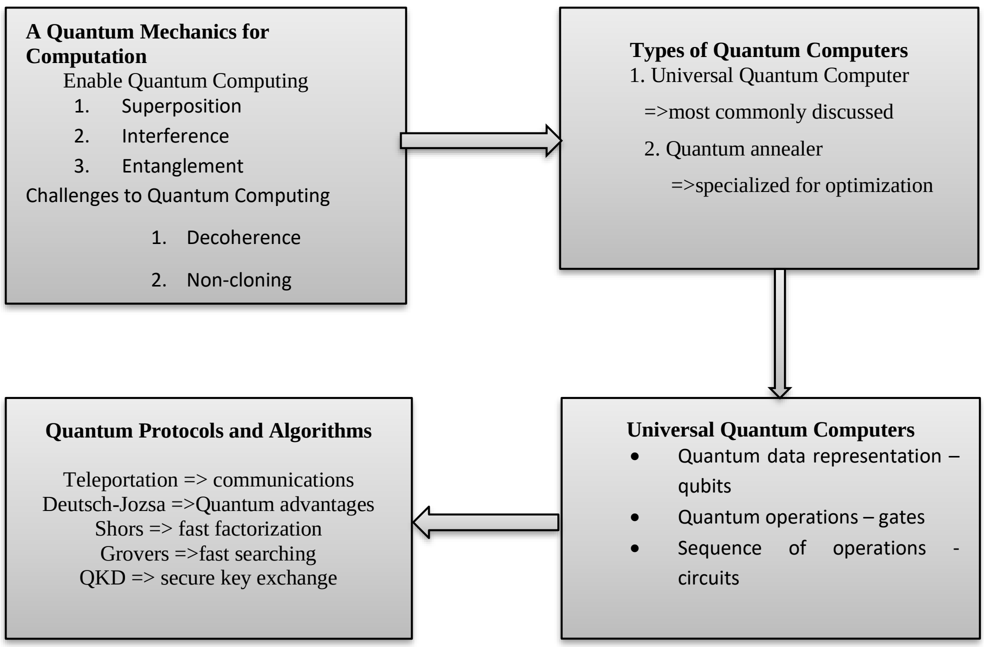

Figure. 2. The Primary ideas presented

Inside this portion, we start by explaining fundamental basic quantum systems that really are necessary for quantum computation, including such entanglement and superposition. The learner will understand better why quantum computation concepts come into being following the adoption of subatomic particles (for example, to relate to the role of semiconductors or transistors in classical computers). Secondly, we introduce three distinct kinds of quantum systems, namely universal quantum systems (also referred to as digital quantum computers), quantum annealers (often when known as analogous quantum systems), and electronic intelligent machines, together along with their underlying mathematical methods. The reference model, or "gateway design," employed in international quantum systems design currently being considered most commonly subsequently primarily introduced. Finally, in the interest of demonstrating why qubits are superior to classical approaches, we introduce a number of very well quantum algorithms and protocols. The connection between both the concepts that this subsection addresses is illustrated by Figure 2.

3. QUANTUM MECHANICS IN CALCULATION

Let’s quickly investigate the actual events in quantum mechanics and the theory of computation aims to simulate without heading through the technical issues of quantum computation. The field of quantum mechanics performs an excellent job of clarifying the results of the theory of quantum physics, notwithstanding the reality that they may appear contradictory [18]. Thus, that we may approximate the conventional calculation by modelling mathematically these kinds of events. These findings are referred as quantum impacts in this paper. Similar to the nature of semiconductors in traditional computers, quantum influences perform an identical impact on quantum computers as well.

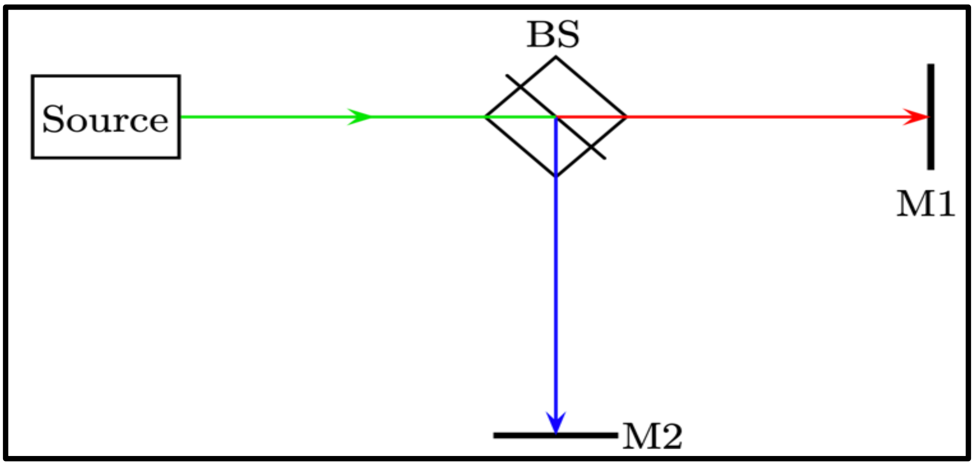

Figure 3. Superposition Creation

In Figure 3, we're going to address the phenomenon of quantum impacts adopting an ordinary photonic setup for experimentation. The photon source (Source), an electromagnetic beam split (BS), plus 2 photon sensors compose a superposition arrangement, as shown in Fig. 3. Just a single of both sensors has an equal likelihood for recognising up or measuring the energy of the photon. In a nutshell, after being evaluated, it stays in a combination of two different paths (two potential outputs). Users are able to turn to Section II.C for the mathematical description of the outcomes, but in general they simply have to think of both of these opportunities as 0 and 1.

In simple terms, a system made up of quantum particles has the capability of being in many different states at the same time, each of that having an opportunity of measuring something. This is referred to as an instance of combination. There are in fact two feasible outcomes in our scenario: 0, and 1, respectively. A highly complex quantum system, nevertheless, can frequently exist in a multi-state combination with two different outcomes, where n represents the total amount of regions. Other settings for experimentation might assist with issue.

3.1. Quantum Algorithms and Protocols

The methods employed by quantum computing devices have been referred to as algorithms for quantum computing. Several quantum computation techniques are used in different computing domains. We present widely used cognitive protocols and algorithms that are based on the previously mentioned cognitive logic gate model in the following section. They are among the most frequently referred to techniques that are constructed via quantum computers. They surpass conventional methods in terms speed information technology through the use of quantum mechanics which includes interference, superposition, interference, and entangle.

3.2. Quantum Deutsch-Jozsa algorithm

The first case that demonstrated the mathematical advantages associated with quantum computer technology involves the Deutsch-Jozsa algorithm [19]. It indicates that with regard to the Deutsch-Jozsa issue. The use of a quantum solution might outperform the best standard method. In this Deutsch-Jozsa task, a secret equation (x): *0,1+n *0,1+ is presented. A Binary operation, it produces 0 or 1 following obtaining a n-bit sequence as inputs.

3.3. Quantum Shor's algorithm

The challenging task of considering a combination of a pair of big numbers that are prime is the building block of the most frequently employed conventional security system (as well as RSA). For resolving the large-number decomposition in an exponential amount of a period of time Shor's technique provides an alternative solution that utilises classical phase's prediction [20]. In reality, it overcomes the matter of factorization problem by addressing the period-finding challenge. In terms of mathematics, if we are capable of estimate the amount of time of the periodic equation (x) = (axe module N), we could effectively factorise N. For a number N = 15, for instance, the phases of Shor's technique could be summarised up as a result:

3.4. Grover's algorithm for Quantum Computing

Unorganised retrieval problems can be addressed in (N), which is time utilising Grover's approach. It may successfully flip an encryption function, for example, to identify the distinctive input(s) to a function with one direction that has a significant likelihood. A black-box functioning, which can be a function with a single direction, allows for simple to determine (x) provided x, yet it's difficult to compute x knowing the outcome of (x). Using the conventional approach, the sole means to solve the problem is by using brute force all possible values of x. During repetitions, it enhances the frequency of the intended result, which subsequently in effect improves the possibility of a desirable incident. During (N) phases, the expected outcome's amplitude dominates; therefore we have the opportunity to be certain that the outcome of the measurement reflects the value we were aiming for. In this section N is the total amount of black-box product outputs that could potentially be found, or every potential value for the domain of the function or x.

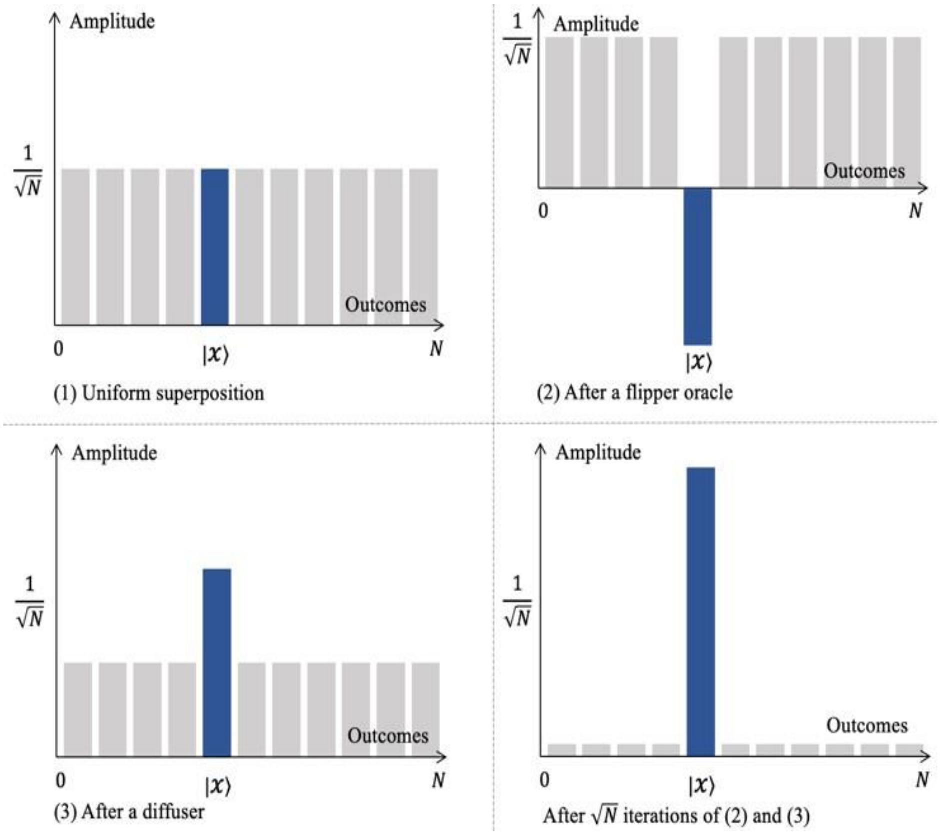

Figure 4. Amplification Changes Over in Grover's algorithm

The design of the circuit that measures the outcome of the algorithm developed by Grover is shown figure 4, and the x-direction shows every possible solution (i.e., both the measurements and outputs of the circuit). The ratio of the magnitude corresponding to each square root answer corresponding to the probability of every measurement result is shown on the y-axis of the graph. We required N = 2n outcomes for measurement to be able to use n quantum bits to cover all possible solutions. In phase 1, each measurements outcome has an equivalent magnitude of 1 N (i.e., 1 = likelihood to be observed), and here is n quantum bits in a homogeneous combination.

4. (QKD) QUANTUM KEY DISTRIBUTION

Cognitive-based key exchange protocols were developed since conventional key exchange procedures, including the Diffie-He key exchange protocol, are going to be in threat from quantum computer algorithms like as Shor's algorithm. The most frequently provided exchange of keys mechanism is QKD. Several nations have built its implementations[4,] [5]. the QKD networks are generated by the interconnection of QKD communication. QKD is a combined quantum-classical methodology. In order to conclude the key exchange procedure, both Alice and Bob must jointly submit the results of their measurement outcomes. In Article disabilities, the concept of quantum cryptography will be covered alongside the widely recognised QKD approaches.

5. MACHINE LEARNING WITH QUANTUM MECHANISM

Identifying universal minima is an unambiguous use of quant annealing. In additional to quantum the annealing there are additionally techniques for exploiting quantum phenomena that help (or improve) conventional models for machine learning. However, it can be difficult to connect quantum concepts to real-life problems considering the advanced state of computing power available today.

The objective underlying superconducting artificial intelligence is to reduce the amount of the amount of information processing time as well as storage costs. A quantum memory with association’s neural networks architecture, for example, has been developed to exponentially boost store capability. In addition, it was recently shown that the support vector machines (SVM) for classification of binary data that was developed with the theory of quantum mechanics performed exponentially superior to its traditional comparable. Both solely quantum techniques (such as quantum annealing) and hybrid cognitive-classical techniques are currently being studied in the discipline of cognitive machine learning. They are being examined with several data types (further details concerning the data formats can be found within Section VII). Conventional methods for machine learning, such classical walk and classical artificial neural networks, have already been tried to be applied to quantum systems as well. For the purpose of more effective learning methods, quantum artificial intelligence employs quantum computations. Here, we outline the primary barriers to cognitive analysis of information and talk about the final significant problem, quantum algorithm learning.

6. DATA TYPES FOR QUANTUM COMPUTERS

Despite research with quantum deep learning on real data sets have been productive, the distracting hardware renders scaling up in reality difficult. It is being established that data from the real world can be analysed by intermediate-scale quantum computing devices. It is not required to match the amount of quantum bits to the information's dimension (without features elimination) while analysing data that is highly dimensional. But additional study is required in order to determine how quantum machine learning can be effective for datasets from the real world.

7. QUANTUM MACHINE LEARNING AND ITS USE

A further significant field to investigate is the use using quantum machine learning for learning. By integrating machine learning with quantum computer technology, it finds solution to difficult problems. Creative applications continue to be created as the business sector develops. In this section we're looking at two methods related to the advancement of quantum machine learning, which include enhancing classical analysis of information with quantum machines and accelerating the evolution of quantum computer technology using conventional machine learning models.

8. CONCLUSION

The most important components of quantum determining quantum machines, networked quantum computers, quantum encryption, and quantum machine learning—have being classified and discussed in this paper. Regardless of being different topics they have similarities in some approaches. In addressing the challenges that arise, we presented users with an in-depth introduction to the subject matter (from a technological science point of view). We analysed the important changes and greatest recent advances in every field and highlighted the most recent scientific trends in the field of quantum computing. Non-trivial efforts and breakthroughs are being undertaken frequently on the path towards the projected advent of quantum technology and the emerging quantum network. Recent methods are employed to highlight the benefits and drawbacks in an effort to thoroughly analyse existing quantum technologies.

REFERENCES

[1] E. Gibney, "Quantum computer race intensifies as alternative technology gains steam," *Nature*, vol. 587, no. 7834, pp. 342–343, Nov. 2020, doi: 10.1038/d41586-020-03237-w.

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, p. 025002, May 2020, doi: 10.1103/RevModPhys.92.025002.

[3] J. Aaron Lopez-Leyva, A. Talamantes-Alvarez, M. A. Ponce-Camacho, E. Garcia-Cardenas, and E. Alvarez-Guzman, "Free-Space-Optical Quantum Key Distribution Systems: Challenges and Trends," in *Quantum Cryptography in Advanced Networks*, IntechOpen, 2019. doi: 10.5772/intechopen.81032.

[4] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sep. 2017, doi: 10.1038/nature23655.

[5] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proc. R. Soc. London. A. Math. Phys. Sci.*, vol. 400, no. 1818, pp. 97–117, Jul. 1985, doi: 10.1098/rspa.1985.0070.

[6] M. Schlosshauer, "Quantum decoherence," *Phys. Rep.*, vol. 831, pp. 1–57, Oct. 2019, doi: 10.1016/j.physrep.2019.10.001.

[7] K. C. Miao *et al.*, "Universal coherence protection in a solid-state spin qubit," *Science (80-.).*, vol. 369, no. 6510, pp. 1493–1497, Sep. 2020, doi: 10.1126/science.abc5186.

[8] R. C. C. Leon *et al.*, "Coherent spin control of s-, p-, d- and f-electrons in a silicon quantum dot," *Nat. Commun.*, vol. 11, no. 1, p. 797, Feb. 2020, doi: 10.1038/s41467-019-14053-w.

[9] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports Prog. Phys.*, vol. 76, no. 7, p. 076001, Jul. 2013, doi: 10.1088/0034-4885/76/7/076001.

[10] T. van Leent *et al.*, "Long-Distance Distribution of Atom-Photon Entanglement at Telecom Wavelength," *Phys. Rev. Lett.*, vol. 124, no. 1, p. 010510, Jan. 2020, doi: 10.1103/PhysRevLett.124.010510.

[11] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon, "Light-matter entanglement over 50 km of optical fibre," *npj Quantum Inf.*, vol. 5, no. 1, p. 72, Aug. 2019, doi: 10.1038/s41534-019-0186-3.

[12] S. Wengerowsky *et al.*, "Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre," *npj Quantum Inf.*, vol. 6, no. 1, p. 5, Jan. 2020, doi: 10.1038/s41534-019-0238-8.

[13] H. Hübel *et al.*, "High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber," *Opt. Express*, vol. 15, no. 12, p. 7853, 2007, doi: 10.1364/OE.15.007853.

[14] M. Pittaluga *et al.*, "600-km repeater-like quantum communications with dual-band stabilization," *Nat. Photonics*, vol. 15, no. 7, pp. 530–535, Jul. 2021, doi: 10.1038/s41566-021-00811-0.

[15] J.-G. Ren *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, Sep. 2017, doi: 10.1038/nature23675.

[16] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science (80-.).*, vol. 356, no. 6343, pp. 1140–1144, Jun. 2017, doi: 10.1126/science.aan3211.

[17] Y.-A. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, Jan. 2021, doi: 10.1038/s41586-020-03093-8.

[18] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?," *Phys. Rev.*, vol. 47, no. 10, pp. 777–780, May 1935, doi: 10.1103/PhysRev.47.777.

[19] D. D. and R. Jozsa, "Rapid solution of problems by quantum computation," *Proc. R. Soc. London. Ser. A Math. Phys. Sci.*, vol. 439, no. 1907, pp. 553–558, Dec. 1992, doi: 10.1098/rspa.1992.0167.

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2012. doi: 10.1017/CBO9780511976667.

BIOGRAPHIES OF AUTHORS

S.SUBASH CHANDRA BOSE, Ph.D., and Researcher. Currently working as an Assistant Professor for Department of Computer Science at Islamiah College (Autonomous), Vaniyambadi, Tamilnadu, India & Worked as Assistant professor , Department of Computer Science, Veltech Institution Avadi ,Chennai ,Tamilnadu , India . Worked as an Assistant Professor , Department of Computer Applications , Karpagam Academy of Higher Education (Deemed to be University) , Coimbatore , Tamilnadu ,India & Worked as an Assistant Professor , Department of Information Technology , Guru Nanak College (Autonomous) , Velachery , Chennai ,India. His research interests include Data Mining, Artificial Intelligence (Machine Learning: Deep Learning) and Quantum Computing. He has extensive knowledge in research and has good publication records. He has published research papers in reputed international journals with SCOPUS and SCI indexed journals (ORCID: 0000-0001-7863-532X), and published papers in National and International conferences. He is an Editorial Board Member of International Journal of Data Informatics and Intelligent computing (IJDIIC). IJDIIC is an international open access, scholarly peer-reviewed journal publishing high quality articles in all areas of data informatics and intelligent computing, especially current research, new concepts, innovative methods, and approaches for early detection and reporting new methods on basic and advanced aspects of data informatics and intelligent computing. His main research work focuses on Prediction and performance enhancement through Machine Learning, Deep Learning and Quantum-Computing based research. He can be contacted at email: bose.milestone@gmail.com

V.SHAFEEQ AHMED M.Sc. M. Phil., has an experience of more than 20 years in teaching field. He started his career as Lecture of computer science in the year 2002 at Mazharul Uloom College Ambur .He Joined Voorhees College, Vellore in the year 2008 as Assistant Professor in PG Department of computer Science. Currently He is working as Assistant Professor at Department of computer science Islamiah College[Autonomous] ,Vaniyambadi .He served as Examiner for Thiruvalluvar University practical & Theory Examination for affiliated colleges and Autonomous colleges more than 15 years. He participated various National /International conferences, workshops. His area of interest in the field of Research is Data Mining and Cryptography & Network Security. He can be contacted at email: shafeeahd29@gmail.com