Quantum Secure Communication: A Comprehensive Literary Analysis with In-Depth Insights

Vavilla Rupesh[1], Cheemalamarri Venkata Naga Rugvidh[2], Thatiparthi Subramanya Prem Rajiv Kumar[3], S. Kiran[4], A. Ashok Kumar[5] and Chinnem Rama Mohan[6]*

[1, 2, 3]UG Scholars, Department of Computer Science and Engineering,
Narayana Engineering College, Nellore, 524004, Andhra Pradesh, India
[4]Department of CSE, YSR Engineering College of YVU, Proddatur, 516360, Andhra Pradesh, India
[5]Department of Physics, YSR Engineering College of YVU, Proddatur, 516360, Andhra Pradesh, India
[6]Associate Professor, Department of Computer Science and Engineering,
Narayana Engineering College, Nellore, 524004, Andhra Pradesh, India

ABSTRACT

This article helps us to understand the world with quantum secure communication. In this quantum landscape, the classical barriers of secure communication are transcended, and a brand-new era of impenetrable information safety emerges. The laws of quantum mechanics will be helpful in quantum secure communication for data transmission. It highlights the inherent security blessings conferred by using quantum properties, including the no-cloning theorem and the uncertainty precept, rendering eavesdropping impossible. In addition, this article gives us an understanding of how encryption can be done using quantum computing techniques compared to the classical ones. This article also outlines the challenges and ongoing research within quantum secure communication, addressing problems like sensible implementation, community scalability, and quantum key management. It underscores the collaborative efforts of researchers, industries, and governments in advancing quantum cryptography.

KEY WORDS: QUANTUM SECURE COMMUNICATION, QUANTUM KEY DISTRIBUTION, QUANTUM CRYPTOGRAPHY, INFORMATION SECURITY, QUANTUM COMPUTING, DATA PROTECTION, POST – QUANTUM CRYPTOGRAPHY.

INTRODUCTION

Imagine this 20 Years from now: all your bank account passwords, your messages, Photos, your browsing history, and finally, all the information that defines your societal status can be accessed by anyone with only a few seconds of computing. Scary right? Well, it is true, it is possible through Quantum Computing. If it is that dangerous, why should we even develop it? Here is an example of quantum computing. John is in a maze searching for an exit; he needs to find the route to the exit. He goes through a route and determines whether that route leads to the exit or not, and then he tries another route like that he goes on until he finds a route to the exit. In this time-consuming process, John thinks, what if someone like him searches another route while he is searching in his route? Well, the quantum computer does the same. Simply, it searches for the number of routes that lead to exit in different dimensions simultaneously and gets the shortest path to it.

This is possible because of the Qubits and their properties, such as superposition, entanglement, quantum sifting, and some dedicated search algorithms. After reading this, we get a question: well, a faster solution, so is it worth the risk of losing all kinds of encryption? Shouldn't we abort it like a failed experiment or potential dangers? We are already reaching speeds that are less than milliseconds. Here, speed is a by-product; its real value is how to solve and handle more complex problems like How complex? Experts expect solutions for, quote, "The birth of the universe and its mysteries," it is expected to solve other real-world problems that are more complex for classical computers. Coming to security, there is genuine concern about data privacy and communications, so why don't we use the same technology to solve this problem? Quantum Secure Communication Came into the thoughts and is actively being implemented globally (Alhayani et al., 2023).

Article Information:*Corresponding Author: ramamohanchinnem@gmail.com
rkirans125@gmail.com & drashok.yvuce@gmail.com
Received 15/08/2023 Accepted after revision 29/09/2023
Published: Sep 2023 Pp- 171-177

Available at: https://bbrc.in/ DOI: http://dx.doi.org/10.21786/bbrc/16.3.7

Quantum Key Distribution (QKD): Quantum Key Distribution (QKD) is a technique for establishing secure communication channels. This can be done by exchanging keys, which are in encrypted format, between the sender and receiver. This method uses the principles of quantum physics, which can help us achieve security measures that can withstand the threats from quantum computing. Mechanics Behind QKD: QKD ensures secure transmissions by sending packets of quantum particles, commonly known as photons, through fiber optic cables (Cao et al., 2022). Each photon carries a random quantum state or qubit, representing a binary digit 0 or 1. These qubits are measured at the recipient's end, forming a line-up of bits or sequences. This series of bits then becomes the key for encrypting and deciphering messages. Any attempts made by external sources to meddle with or monitor the transmission can be detected due to intrinsic attributes governed by quantum mechanics.

Types of QKD Protocols: QKD protocols fall into two primary classifications: prepare-and-measure and entanglement-based. The former involves measuring the states of a particle. At the same time, the latter depends on an exclusive quantum entanglement phenomenon where measurement actions performed on one particle have consequential effects on another particle's behavior. These protocols ensure thwarting unauthorized access attempts, thereby securing communications effectively.

Challenges and How It is Accomplished: Quantum Key Distribution (QKD) confronts issues, including merging into present infrastructure, restricted transmission ranges for quantum photons (typically 100 kilometers), and the necessity for an initially protected communication path. Regardless, QKD is gaining importance as a safeguard against quantum computers, especially in view of the imminent threats they pose. Real-world QKD measures have discovered weaknesses such as phase remapping and photon number splitting attacks. To combat such risks, decoy state QKD protocols were developed to intensify security.

Evolution and Future of QKD: The roots of QKD go back to the 1970s when Stephen Wiesner started the idea of quantum cryptology. Charles H. Bennett later released the BB84 protocol, which became the cornerstone for quantum cryptology relying on non-parallel states. In 1990, Artur Ekert made a noteworthy contribution to QKD by investigating quantum entanglement as a bedrock for secure communication.The outlook for QKD presents a favorable future. Gradients such as the Quantum-Safe Security Working Group (QSSWG) endeavor to endorse the acceptance of QKD alongside other quantum-safe technologies to combat emerging threats ushered in by quantum computing. Researchers are engrossed in augmenting data velocities and extending distances for deploying QKD. Companies have also delved into the QKD space with commercially available systems on offer.

Quantum Repeaters

Illuminating Pathways towards Quantum Communication Network: The prospect of a paradigm-shifting world with exceptional security in communication, advanced AI systems, and state-of-the-art medical imaging lies within sight with the advent of the quantum internet. However, crafting a global reach depends heavily on transmitting quantum bits or qubits across substantial stretches, which brings us face-to-face with an issue requiring resolution – introducing Quantum repeaters into the mix.Distinguishing Quantum Repeaters from Classical Counterparts: In classical cyberspace, information is conveyed as binary codes via optical fibers, with repeaters performing the essential task of dealing with signal loss caused by weak intensity. The traditional repeaters receive incoming signals, amplify them, and transmit them at higher power levels (Wallnöfer et al., 2022).

The Challenge of Loss in Quantum Networks: Quantum networks encounter a similar dilemma regarding signal degradation due to feeble intensity levels. However, conventional repeater techniques cannot be employed in quantum transmissions because of an intrinsic aspect of quantum information: the no-cloning theorem. Unlike standard data bits, quantum details cannot be replicated or measured without modifying their state. This unique characteristic inherent within quantum data enhances its unmatched resistance against hackers' spying activities. However, it simultaneously generates problems compensating for weakened signals within quantum links. Unleashing the Power of Entanglement Swapping: The primary objective of quantum networks revolves around disseminating entangled states across their members. Distributing entanglement unlocks a host of applications, such as qubit teleportation. Entanglement swapping is a nifty technique that cleverly mitigates signal loss without violating the no-cloning principle.

Teleportation & A Vital Player: If repeaters possess qubits entangled with pairs at Alice and Bob's ends, they can conduct measurements and transmit. The essential data to establish the newly entangled connection. By constructing a chain of repeaters, the project of spanning lengthy distances is damaged down into practicable segments for photon transmission.Experiments and Milestones: Quantum teleportation among nodes has been experimentally established via various studies and organizations in various scenarios, consisting of free-area hyperlinks over vast distances and ground-to-satellite uplinks. Although there have been successful quantum teleportation experiments, building realistic quantum repeaters gives distinct demanding situations. Notably, quantum repeaters must be tailor-made to paintings inside the limitations of modern-day quantum gadgets.

The Evolution of Quantum Repeaters: 1st Generation Repeaters: These preliminary repeaters depend on quantum processors, which might be inherently blunders inclined. First-generation repeaters appoint entanglement distillation to catch up on errors, 1st generation repeaters appoint entanglement distillation, where remarkable entanglement is distilled from several low-excellent copies. While these repeaters permit groundbreaking applications, their communique charge is restricted through the distillation procedure.

2nd Generation Repeaters: As mistakes charge decrease, second era repeaters transition from entanglement distillation to quantum error correction, which handles operational mistakes through encoding records into blocks of qubits. This transition helps extensively faster facts switch and unlocks additional programs. 3rd Generation Repeaters: With similar upgrades in quantum gadgets, third-generation repeaters hire quantum blunder correction to manage loss and operational errors. Then, it ensures that the information in the nodes will secure its spot irrespective of verification of the established order of entanglement. Future Vision: Quantum networks are already in improvement, with projects like the Center for Quantum Networks at the University of Arizona pioneering the development of quantum networks equipped with completely error-corrected quantum connectivity, made viable through quantum repeaters. Comparable endeavors are underway globally at universities and country-wide laboratories.

Post-Quantum Cryptography: Post-quantum cryptography is one of the departments of cryptography for developing algorithms on encryption and protocols, which will even be applicable in quantum computing. So, developing these algorithms has become vital to maintaining protection and safety in digital communication (Joseph et al., 2022).

Several households of cryptographic algorithms are considered promising applicants for post-quantum cryptography. These consist of lattice-primarily based cryptography, hash-primarily based cryptography, code-primarily based cryptography, and other tactics.Lattice-Based Cryptography: Lattice-based cryptography is one of the leading contenders for post-quantum cryptography. It depends on lattices, which are grids of points in a multi-dimensional area. Lattice troubles are believed to be complicated even for quantum computers, making lattice-primarily based cryptography a sturdy desire. Some prominent lattice-based cryptographic schemes consist of: NTRU Encrypt and Ring-LWE (Ring Learning with Errors).

Hash-Based Cryptography: Hash-primarily based cryptography is another approach to post-quantum cryptography. It is predicated on the properties of cryptographic hash capabilities, which can be believed to be resistant to quantum assaults. Some hash-primarily based cryptographic schemes include: Merkle-Damgård Construction SPHINCS (SPHINCS-256).Code-Based Cryptography: Code-based totally cryptography is based totally on error-correcting codes and is taken into consideration as a possible option for publish-quantum cryptography. It depends on how complex the decoding of error correction code is. Some code-based cryptographic schemes consist of: McEliece Cryptosystem Niederreiter Cryptosystem.

Other Quantum-Resistant Algorithms: Apart from the households of algorithms, other approaches and cryptographic schemes are being explored for submit-quantum cryptography. These encompass: Multivariate Polynomial Cryptography, LWE-Based Cryptography, Isogeny-Based Cryptography, Code-Based Signature Schemes. The closing intention is to ensure that touchy records stay stable in the era of quantum computing.

Quantum-Secure Communication Networks

Design Principles of Quantum Secure Communication Networks: Quantum Key Distribution (QKD): Since a discussion was already covered on QKD, integrating its security with the fastest communication, like quantum communication, will give us an efficient and secure communication network. End-to-End Encryption: This Quantum Communication is built to ensure a network almost invulnerable to eavesdroppers. Quantum Repeaters and Relays: These devices work between the sender and the receiver, which handle encryption and decryption of the data based on the quantum keys of the sender and the receiver. Authentication and Authorization: The quantum network implements strong authentication and authorization mechanisms to ensure that only authorized people access the data. Quantum Secure Hardware and Protocols: Hardware and Protocols designed to withstand and overcome various quantum attacks are employed .Components including Quantum Nodes, Optical Fiber, and Trusted Repeaters:

Quantum Nodes: There are two significant nodes in Quantum Communication Networks. They are Transmitters and Receivers. Transmitters are responsible for generating and transmitting quantum states like qubits. This also deals with the data encryption using its own Encryption Key. The other node is the Receiver, which handles the receiving and Decryption of data and ensures the safety of the data by measuring the quantum state of the data transmitted by the transmitter. Optical Fibers: These are the communication mediums that are used to transmit quantum states between the quantum nodes. They should be placed and maintained carefully so there will be no signal loss and reduce the effects of the transmission impairment on the data. Trusted Repeaters: Trusted Repeaters can sometimes be called Quantum Nodes. They act as intermediate devices within the quantum communication networks. Purpose Their primary purpose is to enable long-distance quantum-key distribution and quantum state transmission, which was a limitation of the Optical Fibers. Quantum Memory These devices are included with memory devices that can store the quantum states temporarily. This Favors the long-distance QKD.

Quantum Operations These devices can perform operations like entanglement swapping and quantum error correction to maintain the security and integrity of the quantum keys.

Security Since repeaters are intermediate devices, they are built to provide the maximum security possible for quantum states or quantum key distributions. Integration with classical Encryption for added security: Classical Encryption Layer: This layer uses traditional cryptographic algorithms, such as Advanced Encryption Standards (AES) or Rivest, Shamir, and Adleman (RSA). This layer is placed on the top of quantum-secure keys.Quantum Key as One-Tiem Pad: Any quantum key like KAB, KBA, etc., serves as a one-time pad. It means these keys are used only once to encrypt and decrypt a message by the transmitter and the receiver, respectively. This uses a matching one-time pad and key. Data Encryption and Decryption: Consider a transmitter, Alice, and a receiver, Bob. Alice has a crucial KAB to encrypt and transmit the message. When Bob receives the encrypted message, the same KAB key is used to decrypt the message.

Double-Layer Security: Since we have placed Classical Layer on Quantum encryption, this gives us a two-layered data encryption in which even if a layer is compromised, there will still be another layer that should be compromised. This will enhance the safety of the data. Quantum Key Rotation: The quantum key generated through QKD is used only once, giving them a shorter lifetime duration. Then, another key is rotated between the quantum nodes. Even if a key is compromised, it will no longer be in use (Muralidharan et al., 2016; Bernstein & Lange, 2017; Villoresi, 2010; Nakahara & Sasaki, 2012).

Security Considerations And Threats: Overview of Potential Threats: Quantum Eavesdroppers: The Eavesdroppers are the ones who keep observing the data line silently, and they will have the potential to copy the encrypted data on the data line. They also can decrypt and break classical encryption algorithms like RSA, ECC, etc. Side-Channel Attacks: Whenever there is a vulnerability or a weakness in implementing the quantum system, the attackers will use it as an advantage to exploit the system, such as measuring quantum states and extracting information through unintended channels.Man-in-the-Middle Attacks: Sometimes, even the quantum-secure network is vulnerable to this kind of attack where the attacker tries to impersonate themselves as a quantum node to another quantum node and tries to get data directly from it. He could also intercept or modify quantum states and keys (Bennett & Brassard, 2014).

Discussion on counter measures and mitigation strategies against quantum attacks: Quantum Key Distribution (QKD): One of the best countermeasures for eavesdropping attacks that can be implemented in a quantum-secure communication network is QKD. Where the quantum states are encrypted, when an attacker tries to intercept, then the states are disrupted, which can be easily identified. Post-Quantum Cryptography: Implementing Post-Quantum Cryptographic Algorithms along with QKD ensures resistance against quantum attacks. The classical encryption layer remains secure if the quantum computer becomes a threat.

Security Key Management: Some of them are One-Time Pads and Key Rotation, which provide strict access control on the message and prevent tampering and side-channel attacks. Quantum Repeaters: These devices are used for long-range quantum communications that ensure long-distance secure key distribution and security. Comparison with Classical Security Measures: Security Posture: Quantum Security provides Security against quantum Security, whereas classical Security is vulnerable to quantum attacks. Key Distribution: Classical Security relies on third parties or pre-shared keys for secure key distribution. However, quantum Security does key distribution by itself without relying on other party keys.Practical Implementation: Quantum secure Communication is still evolving, and it might face some practical challenges in the future, like limited range and specialized hardware. Classical Communication is already well-established and widely implemented.Key Length: Critical lengths of the classical encryption take longer than the quantum encryption. The keys of quantum encryption are shorter in length and more secure due to their unique properties (Scarani et al., 2009).

Quantum-Secure Hardware

Quantum Resistant Hardware components: Quantum-Safe Cryptographic Accelerators: These are the components that help to accelerate the post-quantum cryptographic algorithms. They can efficiently perform complex computations required by quantum-resistant encryption algorithms. Physical Security Measures: The hardware components are specifically built for tamper prevention and protection against side-channel attacks. Random Number Generators: These are used to generate random cryptographic keys. The Quantum-Resistant Random Numbers that are generated are resilient to quantum attacks. Secure Hardware Modules: Hardware Security Modules (HSM) ensure the security of the keys even after the post-quantum threat landscape. They are also known as Secure Enclaves.

Quantum-Secure Communication Devices: Devices like quantum nodes and quantum repeaters are known as quantum-secure communication devices that ensure safe long-distance data transmission in quantum communication networks.

Secure Key Storage: The components of hardware that store the cryptographic keys should be highly secured against quantum attacks. Importance of Secure Hardware in Quantum Communication Networks: Protection Against Quantum Attacks: Now, classical security has become more vulnerable to quantum attacks. So, quantum communications came into play, with more algorithms implemented to ensure secure communication. Tamper Resistant: The Quantum-Communication Hardware is purposefully built to prevent quantum attacks and physical access to sensitive data like cryptographic keys. Preventing Side-Channel Attacks: Communication Hardware uses Double-Layered Encryption Algorithms that help prevent quantum and side-channel attacks. Long-Term Security: The hardware of quantum-communication networks has a longer life span than any other security hardware. They ensure network security even after the advancement of quantum computing technology (Ramakrishnan et al., 2022).

Uses And Implementations

A topic like secure communication in quantum technology has uses and cost efficacies of nearly millions or even billions, but is the cost worth it? Here are a few case studies and practical implementations: OTPs through QKD: using quantum key distribution, we can send the OTPs and verify persons, and their identities will be much more accurate. In the increasing cases of cloning mobile numbers/emails, etc., very important OTPs can be shared using Quantum technology, specifically the more significant transactions or authorization to Accounts that have a heavier influence. Voting through QKD: if this QKD becomes a household norm, voting from anywhere could be possible since a Quantum secure connection is established once we can verify if there is any tampering or not so the voting process can happen in the home itself, which reduces the burden of going to a voting booth, problems like rigging, lousy influence on voters will be reduced. With a connection made through the QKD path, the voter can generally vote according to their will from the comfort of their home. Since any middleman tries to intervene in the connection, it can be spotted as a disturbance, and the voter can abort the connection and retry again till a safe connection is established.

Energy Sector: A never-ending threat to the energy sector from wrongdoers via MITM attacks or DDOS Attacks, etc these generally happen through a loophole in the communication system like weak passwords of office accounts or human error, accessing unknown links, etc., when the QKD comes into play ultra-sensitive data will be passed in this method hence reducing a significant chance for an attack. Cloud Computing: since there is a proposal of quantum computing through the cloud, if it happens, quantum computers are easily accessible, so most kinds of encryption can be broken.

To prevent this, QKD is beneficial, and by improving human verification methods, authorities can act fast since a trail in the QKD system is unerasable. Supply Chains: with even more security, the ordered goods and payments will be safer and end-to-end encrypted. This QKD in the supply chain can be quoted as "a double-edged sword. "Since the wrongdoers can have secure communication and access to the blockchain, AI, etc., their supply chain will be hard to track, but QKD is only used on a connection basis and not for anonymity purposes authorities with the right level of social engineering tactics can still have the upper hand (due to the wrongdoers are human so they are vulnerable to social engineering).

Satellite Communication: satellites currently use radio waves for long-distance communications, but if a Qubit's entanglement feature is enhanced, it can deliver information more instantaneously and, of course, more security. Defense: The need for a secure route for communication is mainly due to conflicts between nations or high military tensions. We human beings tend to think emotionally, but Defense is a sector where rational thinking is needed, and the highest level of problem-solving is utilized because there is no single solution for everything. Hence, this quantum technology aims to solve real-world problems the human mind cannot solve. Hence, the first step in protecting the nation's peace is to have a secure line of communication in the Defense sector.

IOT (Internet of Things): In the Day and age of IOT devices, quality of life is improved in the same way threats such as accessing the Devices and causing some inconvenience or even accidents. Quantum technology will be beneficial in determining if there is any risk for a device or even some unnoticed logins and attempts to manipulate specific IOT devices. Remote Devices: Remote accessing our Devices from one place to another is an excellent option, but it sometimes comes at the cost of leaking credentials etc. QKD will ensure the remote access is secure, and no tampering occurs during connection time.

There are many implementations such as QKD in Health Care, Data Centres, copyright protection, Networks, Legal Contracts, Auctions, identity verification, and much more; the thing is, with the rapid development of quantum computing, experts are preparing for potential crimes and trying to invent new cryptography methods to encrypt our data there are new types of cryptography to encrypt the end-to-end keys (Sheng et al., 2022; Hasan et al., 2023; Gill et al., 2022).

Beyond Moore's Law And The Potential Developments: According to Moore's Law, computational power doubles every two years, i.e., in specific terms, the number of transistors in an integrated circuit (IC) doubles about every two years. However, as we progress on silicon chips, we are reaching its limit on computational power as per the law of thermodynamics and laws of quantum mechanics; this is going to happen soon as naturally, we tend to look for other alternatives in terms of producing computational power and lo and behold, we have quantum computing, with the power of Qubits there are some drawbacks to it:

Decoherence: is a phenomenon where the qubit loses its superposition due to noise or other factors such as temperature change.AI and Quantum Technology: The deadly combo of Artificial Intelligence and Quantum computing is very dangerous and yields capricious results.

Cryptography: As quantum technology offers speedy results and more computational power, the current encryption could be easily decrypted, governments are trying new cryptographies now, but the major problem that is happening is SNDL (store now, decrypt later) actions, which means the encrypted data that is available today can be stored now, and when the quantum technology is available for the public this stored information with old cryptographies can be decrypted using a quantum computer in future. We predict that quantum technology will be the new normal in businesses and governments. Household quantum computers are a long shot since laypeople do not need that much computational power for their daily tasks. Developments: With this technology, Developments would be secure, i.e., all sorts of possibilities can be calculated faster and made. Since problem-solving happens in complex scenarios, we may find surprising cases of faults and errors and potential new solutions for them—the creation of the universe and predictions such as predicting accurate weather (Gill et al., 2022).

Risks In Quantum Technology: A Big Obstacle for Blockchain Technology: Some of us will have an idea about blockchain technology, which will depend on several algorithms. Blockchain uses algorithms like RSA and EC, which are asymmetric as quantum computing is compelling enough to crack those algorithms, which will result in the difficulties of blockchain. This will become a problem for many companies investing in blockchain technology.

Unknown Security issues: Quantum computing is the upcoming technology that has the power to change the entire digital system. Although it has certain advantages, many issues that cannot be foreseen today will arise. Everything goes differently than planned in this world. So, we need to be prepared for a counterattack. Usage Difficulties: This is one of the most critical risks in quantum computing. We must find where and when we must use it. There will be some areas where there is no necessity for the usage. Analyzing the situation, one can understand which aspect of quantum computing can be fitted. To implement this, companies must use high-end computers in addition to the software. DNN's Complexity: DNN (deep neural network), if a quantum computer is utilized in developing Deep neural networks, it is possible that the Neural Network might exceed Human Comprehension, and supervising it will become tough.

A Queen less Nation's Sorrow: Wars are a never-ending cycle; when a quantum computer is involved in Armies, a nation without a quantum computer is equal to playing chess without a queen. Digital Divide: Like in the real world, the divide between The Rich and The Poor here in the digital era Quantum computer holds the power to flip the tables completely; as usual, the wealthiest will uphold this power, and the poor will be left in the dust (Faruk et al., 2022).

Transparency Issues And Scalability Factor: Transparency issues in Quantum Secure Communication refer to how weak the accessibility and security of the network are. These issues might impact the reliability and trust of the network by the users and stakeholders. Some of the issues are: Complexity of Quantum Technology: Quantum Communication works on complex principles and technologies that are difficult for beginners and non-experts to understand. The users may need help understanding how it works, which might compromise transparency.

Limited Public Awareness: Since quantum communication is a developing concept, it might have limited implementations, leading to a need for more public awareness. Since only a few will be able to know about that, it might lead to skepticism among the public and the users. Opaque Quantum Key Distribution Protocols: Some aspects of QKD protocols are very complex to explain the technical concepts. This might hinder explaining the concept transparently, leading the user to lose trust in the network's security.The scalability factor in quantum communication speaks about the ability of the network to expand its capability to facilitate the increasing number of users, devices, and requests (like data traffic). Not only that, but it should also maintain its level of performance and security even after changing its capacity. Some of the scalability factors are:

Network Size and Range: One day, enormous users might be worldwide. This means the network should be able to cover a larger geographic area that requires scalable Quantum Key Distribution (QKD) technology. Quantum Repeaters: These are the quantum nodes that are used as the intermediate devices for long-distance communication. For this, there have to be multiple quantum repeaters that are capable of providing secure communication over large networks and distances to be deployed. Quantum Resources: Number of users are proportional to the number of resources required. Resources should be maintained in such a way that it serves the users even if there is any unexpected rise in the number of users. The Entangled Photons can be one of the critical resources. Integration with Existing Infrastructure: Quantum Communication is now a widely used network nowadays. So, implementing and integrating them with existing classical infrastructure is very important. Moreover, it has to be done without disturbing the network's security and the capability to serve the larger areas (Ben-Sasson et al., 2018; Lo et al., 2012; Gisin et al., 2002; Qi et al., 2019; Kumar & Garhwal, 2021; Diamanti et al., 2016; Long, 2017; Zhou et al., 2018).

CONCLUSION

It is the year 2023, a long way from the year 1998 when Quantum computing began. Quantum computing is being developed rapidly, and the development of computational power and newer algorithms will continue. We are looking for more and more resources and more experimentation processes to find new possibilities. There might be another way to get more computing power. Who knows, but in this race against computing power, we risk losing current security measures and our data privacy. This is a well-known fact; we experience what happens if we do not act fast and develop countermeasures. Experts are already inventing newer cryptography methods and communications using quantum technology.

It is like the quantum computer was never invented but, at the same time, getting benefits from the computational power of a full-fledged quantum computer. The Key takeaway from this paper is to provide most of the information available on this topic (Quantum Secure Communication) and understand the wonder of science that brought the technology we are using today. However, the cycle of wars, crimes, inventions, beliefs, the good and the bad, Rights, suffering, hunger, food, and Money will relentlessly continue even with all these technologies.

So, why should we develop our technology if there is no change? Quantum technology can solve more and more complex problems like food shortages, wars, crimes, and any tensions that include religion, Money, power, etc. if we humans cannot solve the problems like these. It is up to nature to provide us with the resources and knowledge to solve this. Quantum communication is a step closer to protecting the journey of unraveling the mysteries of humanity and, of course, the Universe.

Funding: This research did not receive any specific grant from any funding agencies.

Conflict Of Interests: The authors declare no conflict of interest.

data availability statement: Data can be available on request.

REFERENCES

Alhayani, B.A., AlKawak, O.A., Mahajan, H.B., Ilhan, H. and Qasem, R.A.M. (2023). Design of quantum communication protocols in quantum cryptography. Wireless Personal Communications, pp.1-18. https://doi.org/10.1007/s11277-023-10587-x

Bennett, C.H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science, 560, pp.7-11. https://doi.org/10.1016/j.tcs.2014.05.025

Ben-Sasson, E., Bentov, I., Horesh, Y. and Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive. https://eprint.iacr.org/2018/046

Bernstein, D.J. and Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), pp.188-194. https://doi.org/10.1038/nature23461

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S.X. and Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys & Tutorials, 24(2), pp.839-894. DOI: 10.1109/COMST.2022.3144219

Diamanti, E., Lo, H.K., Qi, B. and Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, 2(1), pp.1-12. https://doi.org/10.1038/npjqi.2016.25

Faruk, M.J.H., Tahora, S., Tasnim, M., Shahriar, H. and Sakib, N. (2022). A review of quantum cybersecurity: threats, risks and opportunities. In 2022 1st International Conference on AI in Cybersecurity (ICAIC) (pp. 1-8). DOI: 10.1109/ICAIC53980.2022.9896970

Gill, S.S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M. and Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience, 52(1), pp.66-114. https://doi.org/10.1002/spe.3039

Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. (2002). Quantum cryptography. Reviews of modern physics, 74(1), p.145. https://doi.org/10.1103/RevModPhys.74.145

Hasan, S.R., Chowdhury, M.Z., Saiam, M. and Jang, Y.M. (2023). Quantum Communication Systems: Vision, Protocols, Applications, and Challenges. IEEE Access. DOI: 10.1109/ACCESS.2023.3244395

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P. and Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), pp.237-243. https://doi.org/10.1038/s41586-022-04623-2

Kumar, A. and Garhwal, S. (2021). State-of-the-art survey of quantum cryptography. Archives of Computational Methods in Engineering, 28, pp.3831-3868. https://doi.org/10.1007/s11831-021-09561-2

Lo, H.K., Curty, M. and Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical review letters, 108(13), p.130503. https://doi.org/10.1103/PhysRevLett.108.130503

Long, G.L. (2017). Quantum secure direct communication: principles, current status, perspectives. In 2017 IEEE 85th Vehicular Technology Conference (VTC Spring) (pp. 1-5). IEEE. DOI: 10.1109/VTCSpring.2017.8108697

Muralidharan, S., Li, L., Kim, J., Lütkenhaus, N., Lukin, M.D. and Jiang, L. (2016). Optimal architectures for long distance quantum communication. Scientific reports, 6(1), p.20463. https://doi.org/10.1038/srep20463

Nakahara, M. and Sasaki, Y. eds. (2012). Quantum Information and Quantum Computing-Proceedings of Symposium (Vol. 6). World Scientific. https://doi.org/10.1142/8568

Qi, R., Sun, Z., Lin, Z., Niu, P., Hao, W., Song, L., Huang, Q., Gao, J., Yin, L. and Long, G.L. (2019). Implementation and security analysis of practical quantum secure direct communication. Light: Science & Applications, 8(1), p.22. https://doi.org/10.1038/s41377-019-0132-3

Ramakrishnan, R.K., Ravichandran, A.B., Kaushik, I., Hegde, G., Talabattula, S. and Rohde, P.P. (2022). The quantum internet: A hardware review. Journal of the Indian Institute of Science, pp.1-21. https://doi.org/10.1007/s41745-022-00336-7

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N. and Peev, M. (2009). The security of practical quantum key distribution. Reviews of modern physics, 81(3), p.1301. https://doi.org/10.1103/RevModPhys.81.1301

Sheng, Y.B., Zhou, L. and Long, G.L. (2022). One-step quantum secure direct communication. Science Bulletin, 67(4), pp.367-374. https://doi.org/10.1016/j.scib.2021.11.002

Villoresi, P. ed. (2010). Quantum Communication and Quantum Networking: First International Conference, QuantumComm 2009, Naples, Italy, October 26-30, 2009; Revised Selected Papers. Springer. https://doi.org/10.1007/978-3-642-11731-2

Wallnöfer, J., Hahn, F., Gündoğan, M., Sidhu, J.S., Wiesner, F., Walk, N., Eisert, J. and Wolters, J. (2022). Simulating quantum repeater strategies for multiple satellites. Communications Physics, 5(1), p.169. https://doi.org/10.1038/s42005-022-00945-9 ---3

Zhou, T., Shen, J., Li, X., Wang, C. and Shen, J. (2018). Quantum cryptography for the future internet and the security analysis. Security and Communication Networks, 2018, pp.1-7. https://doi.org/10.1155/2018/8214619 23.