International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Quantum Cryptography for Health Data Security - A Review

Kantharaju[1], Srinidhi G A[2]

[1]Research Scholar, Department of Biomedical Engineering, SSIT, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
Corresponding Author Email: *kantharajus[at]ssit.edu.in*

[2]Research Supervisor, Department of Biomedical Engineering, SSIT, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India

Abstract: ***The protection of private data is of utmost importance in the contemporary digital era, with particular emphasis on the healthcare sector. Traditional cryptographic techniques, despite their limitations, have been widely accepted as the prevailing method for ensuring data security. The rapid development of quantum computers necessitates the urgent implementation of enhanced encryption techniques to ensure heightened security. Quantum cryptography is a cutting - edge approach that leverages the principles of quantum mechanics to safeguard confidential data. By harnessing the unique properties of quantum particles, this novel technique offers a revolutionary means of ensuring the security of sensitive information. Quantum cryptography is a cutting - edge technology that offers unbreakable encryption by leveraging the fundamental principles of quantum physics, such as entanglement and superposition. Quantum cryptography, in contrast to classical cryptographic systems, is based on the principles of physics rather than the computational complexity that forms the foundation of classical cryptography. The utilisation of this particular encryption method ensures its resistance against potential attacks from quantum computers, which possess the ability to easily compromise traditional encryption methods. This article presents a comprehensive discussion on the latest advancements in the utilisation of quantum cryptography for safeguarding sensitive medical records.***

Keywords: Quantum cryptography, Data security, Covert communication

1. Introduction

System authentication via digital signatures is a crucial function within healthcare systems that heavily relies on information technology (IT). Information technology (IT) plays a crucial role in various aspects of modern communication. One such application is the use of IT in cellular and Voice over Internet Protocol (VoIP) phone calls, which allows for efficient and cost - effective voice communication over the internet. Additionally, IT enables web surfing, email, and instant messaging, providing users with convenient and instant means of communication and information exchange. Furthermore, IT is instrumental in ensuring data protection. The user has provided the interval [1]– [3] for analysis.

In order to safeguard sensitive patient data and identification from potential threats posed by malicious third parties, commonly known as adversaries, cryptographic technologies are extensively employed. Within the domain of information security, certain encryption algorithms have garnered significant recognition. Several cryptographic algorithms are commonly used in various applications. Notable examples include SHA - 1 and SHA - 2, which are widely used for secure hashing. TripleDES, AES, and MD - 5 are symmetric encryption algorithms that provide different levels of security and performance. Additionally, Rivest - Shamir - Adleman (RSA) is a widely used asymmetric encryption algorithm known for its strong security properties. These algorithms play a crucial role in ensuring the confidentiality, integrity, and authenticity of data in modern cryptographic systems. The SHA - 1 and SHA - 2 algorithms are widely recognised and respected in the field of secure hash value creation. On the contrary, TripleDES is widely recognised for its ability to enhance data confidentiality by utilising a triple - layered encryption technique. The Advanced Encryption Standard (AES) is a widely - used cryptographic algorithm that offers a high level of security and efficiency for encrypting data. MD - 5 is a widely used cryptographic hash function that produces a 128 - bit hash value. The "RSA algorithm" is a well - known public - key encryption technique that derives its name from the initials of its developers, Ron Rivest, Adi Shamir, and Leonard Adleman. It is widely recognised for its robustness and versatility. In the healthcare industry, conventional cryptographic techniques continue to be utilised for the purpose of safeguarding patient information. Regrettably, the constraints of these firmly established methodologies are becoming increasingly evident as the volume of confidential data continues to expand. The user has provided a numerical value of [7]. The issues outlined in this sequence hold particular relevance in the context of neonatal intensive care units (NICUs) and mother - infant care. The primary reason for the utmost importance of safeguarding the "personal health information (PHI) " obtained from the entire household is primarily attributable to this factor. Significant progress has been achieved in the realm of healthcare data preservation, specifically pertaining to the well - being of patients and their families, in recent times. As an integral component of this procedural framework, it is imperative that the data is stored in a manner that optimises efficiency, ensuring seamless retrieval when required, while concurrently safeguarding against potential threats or adversaries through the implementation of robust security protocols. There has been a noticeable increase in the rate of growth of the data, raising concerns about the potential inadequacy of our existing computational infrastructure in the near future. It is evident that there exists a clear requirement for novel and innovative concepts within the specific context under consideration. The

field of quantum computing, which has the potential to yield intricate solutions by harnessing the intricate dynamics of subatomic interactions, represents an area worthy of further investigation. Quantum phenomena can be harnessed and applied more efficiently by directing our attention towards this specific domain of research.

The utilisation of QC models has led to the emergence of numerous captivating prospects for outcome prediction in various settings with extensive datasets. The scenarios encompass a wide range of events, including hurricanes, pandemics, forest fires, and climate change, among others. The utilisation of non - canonical prediction models has demonstrated novel approaches to enhance the efficiency of healthcare systems and forecast outcomes [4]. Through the implementation of quality control (QC) methods, it becomes possible to analyse extensive and delicate patient datasets while minimising the potential for decryption - related vulnerabilities. According to previous research, the number 7 has been identified as a significant value in various contexts. Through the development of techniques aimed at managing entropy within the framework of numerous simultaneous occurrences and reducing error rates to levels deemed acceptable within our existing electronic semiconductor systems, there exists the potential to address a multitude of seemingly improbable events. The references cited in this study range from 13 to 18.

The impact of recent technological advancements on neonatal care has been noteworthy and advantageous. Several notable advancements have emerged in the field, such as the extensive utilisation of "Electronic Medical Records (EMRs) " and comparable systems, the introduction of telehealth services, the creation of continuously monitored vital signs, and the accessibility of affordable at - home testing instruments. The various technical advancements that have been developed and implemented in recent years have significantly contributed to the improvement of newborn care. Within the context of this particular scenario, it is crucial to acknowledge the significance of the numerical values falling between [11] and [13]. Significantly, by obtaining families' consent, the sharing of data derived from these devices has the potential to enhance the efficacy of patient treatment and reduce the occurrence of errors. Real - time data is utilised by various healthcare practitioners in numerous applications. Examining this data with the intention of improving patient care is a notable application. In addition, it is worth noting that healthcare professionals have the ability to utilise real - time data for the purpose of conducting clinical research projects. This is especially relevant in the context of documenting research findings and carrying out drug trials. An enhanced and more targeted methodology for education can be facilitated through the systematic documentation of the quantification of familial well - being. Improved data recording techniques and enhanced collaboration among different medical subspecialties have the potential to enhance the diagnostic evaluation process. Machine learning (ML) and other state - of - the - art methodologies have the potential to significantly enhance the accuracy and effectiveness of results analysis. Full integration of data - driven initiatives has the potential to completely transform the entire health sector. Concern arises due to the presence of personally identifiable health information (PHI) of patients in the aforementioned databases.

Various technologies, such as medical devices, computers, email systems, cloud storage platforms, servers, databases, and electronic health records (EHRs/EMRs), are responsible for storing and managing protected health information (PHI). It has been observed that the healthcare industry is more susceptible to cyberattacks due to the abundance of highly accurate and valuable data that is readily available. This makes it an attractive target for malicious actors seeking to exploit vulnerabilities and gain unauthorised access to sensitive information. It is imperative for hospital networks and healthcare providers to place a high level of importance on ensuring patient safety and ensuring secure access to data in order to maintain the trust of families with newborns. The Health Insurance Portability and Accountability Act (HIPAA) is a significant legislative measure that delineates the protection of Protected Health Information (PHI) and the safeguarding of individual identities against fraudulent activities and theft. The relevance of numbers within the range of [17] and [9] is significant in this context. A recent edition of The HIPAA Journal has reported a concerning and conspicuous increase in the annual occurrence of healthcare record breaches. Based on the available data breach statistics, it can be observed that the year 2015 was characterised by significant challenges, as a substantial number of records were impacted.

The data provided in the disclosure reveals a staggering total of 113.27 million records that were compromised during the specified period, underscoring the gravity of the situation at hand. It is widely acknowledged that the infamous "WannaCry" virus attacks that occurred in May 2017 have left a negative impact on the perception of many individuals. The aforementioned attacks resulted in data breaches at the British National Health Service, as well as other reputable American medical companies. Upon conducting thorough investigations, it has been determined that a significant breach has occurred, resulting in the loss or theft of highly sensitive data. This data includes individuals' dates of birth, social security numbers, email addresses, phone numbers, credit card information, and home addresses. Consequently, the purloined fragments of data were exchanged on subterranean online marketplaces commonly referred to as the dark web. The acquisition of certain patients' medical records was highly coveted, with instances reported of records being exchanged for a substantial sum of $1, 000 USD. According to data obtained from the US Department of Health and Human Services, it has been observed that a significant proportion, approximately 75%, of healthcare breaches are attributed to malicious hacking activities. The user's text consists of a single reference marker [13]. It is imperative to maintain strict security and confidentiality measures for safeguarding protected health information (PHI) within mother - infant units and neonatal intensive care units (NICUs) due to their significant importance within hospital settings. Infants and their respective families exhibit a wide range of characteristics, including varying levels of proficiency in safeguarding confidential data such as social security numbers, financial records, and medical records. Mothers and other family members may experience transient mental health challenges that could potentially impact their

employment prospects, even following a complete recovery. Infants, comprising a total of 46 individuals in this particular case, are recognised as a particularly vulnerable group due to the restrictions imposed on their legal rights and their limited ability to make independent decisions. Upon careful analysis of the given statement, it becomes evident that the implementation of additional measures beyond parental proxy permission is imperative in order to ensure the protection of this particular demographic. The objective of implementing these safeguards should be to mitigate the potential risks that individuals may face, while simultaneously ensuring their safety and well - being. The storage of biological data within the context of family dynamics necessitates careful consideration of the short - term and long - term consequences associated with protected health information (PHI). The user's text consists of two references, namely [7] and [8]. Due to the urgent nature of the situation, prompt assessments are necessary to determine the individuals authorised to access and oversee the protected health information (PHI) of the newborns. The potential outcomes for these young individuals may undergo significant changes as a result of these decisions.

2. Quantum Computing

The processing speeds of classical computers have significantly improved due to the incorporation of a growing quantity of transistors within a single integrated circuit. It is important to highlight, however, that the progress made in these areas is constrained by the fundamental principles dictated by quantum mechanics. The source in question has been referenced as [18]. The utilisation of binary digits, commonly referred to as "bits, " which are typically represented as zeros and ones, has garnered significant recognition and acclaim for classical computers. Within the framework of Dirac notations, the binary units in question are represented by mathematical objects known as "kets. " Specifically, the ket $|0\rangle$ corresponds to the binary value 0, while the ket $|1\rangle$ represents the binary value 1. Both references [18] and [19] have been cited in previous research studies. One of the most prominent characteristics of a quantum computer is its primary constituent, commonly referred to as a "qubit. " According to our research, the numerical value of ten is a positive integer that follows the number nine and precedes the number eleven in the natural number sequence. It is commonly represented by the numeral "10 The fundamental components of bits and qubits are depicted diagrammatically in Figure 1. One possible conceptualization of a qubit, which serves as the fundamental constituent of quantum information, is as a two - dimensional superposition comprising two distinct unit vectors. Due to this particular characteristic, it is possible to utilise column vectors as a mathematical representation for qubits. The term "eleventh" refers to the numerical position of an object or element in a sequence, specifically denoting that it is the one following the tenth and preceding the selection of the vectors $|0\rangle$ and $|1\rangle$ as basis vectors in the 2 - dimensional vector space is justified due to their orthogonality and unit magnitude. It is crucial to bear in mind the aforementioned context. According to previous research findings [11]. In the context of vector spaces, a 2n - dimensional vector space is characterised by the existence of 2n basis vectors. Given the condition of appropriate normalisation of the resultant vector, it is possible to define a qubit state as a quantum superposition of two distinct basis vectors. The user's text is a reference to a source, indicated by the [12] notation. However, without any additional context.

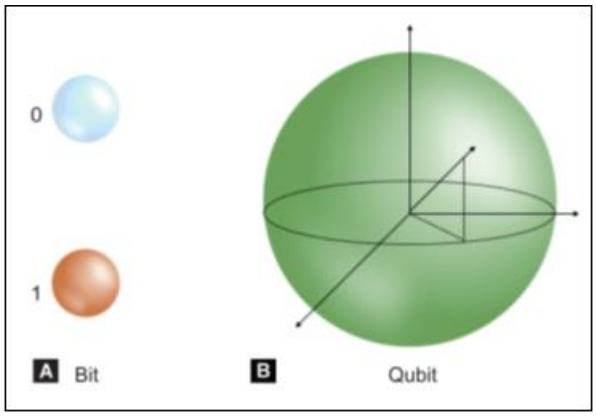

Figure 1: Representation of bits and q – bits

Quantum Entanglement:

The phenomenon of entanglement at the quantum level is a highly fascinating and distinctive characteristic of quantum mechanics, which distinguishes it from classical mechanics. Quantum entanglement (QE) is observed when two particles, despite being physically distant from each other, exhibit a remarkably strong correlation in their location, momentum, spin, and polarization. The reference [15] is presented in isolation, lacking any accompanying contextual details or specific information. Based on the existing circumstances, it is anticipated that the overall spin of the two particles mentioned previously will exhibit a certain level of predictability [16]. It has been observed and documented that upon the measurement of a particle's attributes, there is an irreversible collapse of its wave function. The collapse of the quantum state of a particle has a profound impact on the entangled system as a whole, as documented in reference [16].

3. Quantum Algorithms

Similar to classical algorithms designed for execution on classical computers, quantum algorithms consist of sets of instructions that are specifically optimized for execution on quantum computers. The user has provided a numerical value of 80. When examining the realm of quantum algorithms, it becomes evident that Grover's algorithm and Shor's algorithm have emerged as the focal points of extensive scrutiny and investigation. It is worth noting that in the given scenario, the larger of the two consecutive integers is 82, while the smaller number is 81. Shor's algorithm, a renowned method in the field of quantum computing, is highly efficient in determining the prime factors of an integer. Crucial to the functioning of this methodology is the utilization of a specific unitary operator. Recent findings have revealed that the particular algorithm under investigation has the potential to compromise the security of RSA and ECC cryptographic systems. This vulnerability primarily stems from inherent flaws within the program's design and implementation. By applying modular arithmetic, valuable insights can be gained into the inner workings and behaviors of these algorithms. The Grover algorithm, also known as the quantum search algorithm, is a quantum technique that has the potential to significantly reduce the time required for an unstructured search. The

supplied data consists of two numerical values, specifically [13] and [14]. Hence, it is unfeasible to formulate informed conjectures in order to expedite the process of locating the desired element. Adopting a sequential approach by starting at the initial element and proceeding in a forward direction appears to be the most apparent and straightforward method for addressing this particular matter. One potential avenue for enhancing search processes involves the utilization of Grover's method, a technique that draws upon the fundamental principles of superposition, entanglement, and interference. According to previous research studies [12],. . . The desired ket's phase can be flipped using the oracle, which is a well - known quantum gate. In addition, it should be noted that there exists an extra gate which, in relation to the average of their respective amplitudes, effectively reverses the amplitudes of all component kets [15]. Nevertheless, it is imperative to acknowledge that despite the significant progress made in the field of quantum computing, there remain numerous challenges to be addressed and potential limitations that may arise upon the widespread availability of fully functional quantum computers. Researchers are currently studying a wide range of algorithms. The aforementioned algorithms encompass a range of notable examples in the field of quantum computing. These algorithms include the Deutsch - Jozsa algorithm, the Bernstein - Vazirani algorithm, the Simon algorithm, the quantum Fourier transform algorithm, the quantum phase estimation algorithm, the quantum counting algorithm, the quantum walk search algorithm, and the dense coding algorithm.

The BB84 Protocol, also known as the Bennett - Brassard 1984 Protocol, is a cryptographic protocol that was proposed by Charles H. Bennett and Gilles Brassard in 1984. It is The BB84 protocol, which is named after its creators Giles Brassard and Charles Bennett, is a cryptographic technique that relies on quantum principles to generate a private key. The user has provided a numerical value. The number 93 is a numerical value that represents a quantity or position in a sequence. It does not provide any specific context or After acquiring a sequence of qubits, the initial observer in the current protocol has the ability to perform a conceivable orthogonal measurement on each qubit. Typically, the experimental procedures involved in these tests necessitate the determination of the spin orientation either along the x - axis or the z - axis. The initial individual performs the transfer of the aforementioned objects to the subsequent individual, who subsequently replicates the action. The current implementation of the initial operator lacks the capability to communicate the precise measurements to the subsequent operator. Thus, it is highly probable that the second operator will employ identical techniques as the first operator in order to quantify half of the qubits. Once the experiments have concluded, it is ethically justifiable for researchers to make their findings available to the public domain. During the process, it is imperative to maintain scientific rigor by eliminating any measurements that exhibit inconsistencies or conflicts. It is conceivable that individuals with malicious intent may expend considerable resources in their attempts to decrypt the message qubit. However, it is important to note that in accordance with the measurement postulate, the actions performed on the qubit will inevitably result in a change, occurring approximately 50% of the time. The no - cloning theorem is based on the premise that individuals will encounter difficulties when attempting to replicate certain objects or information. It is essential for the initial two operators to engage in knowledge sharing in order to facilitate the exchange of their respective discoveries. One possible method for individuals to assess the potential compromise of their encryption key is through the application of correlation analysis.

As stated in "The E91 Protocol", the BB84 protocol is widely recognized as a quantum key distribution system of significant popularity. The protocol being examined in this context is a variant that has been slightly altered from the original BB84 protocol. The defining characteristic of this particular variant lies in its utilization of entanglement, a phenomenon rooted in quantum mechanics. Entanglement refers to a state in which the properties of two or more particles become so intricately linked that they cannot be described independently of one another. The participant has provided a numerical value of 94. The experimental protocol commences with the primary operator initiating the generation of a set of entangled qubits, specifically denoted as qubits95 in this particular scenario. Subsequently, the initial operator will transmit the aforementioned qubits to the subsequent operator. Upon examination, it is observed that the initial operator retains one entangled qubit for internal utilization while transferring the other qubit to the second operator. Subsequently, the remaining components of the protocol exhibit a striking resemblance to the BB84 protocol. Based on the high level of confidence in the observed correlation between the entangled pairs, it is unnecessary to utilize the initial operator for data tabulation.

4. Conclusions and Future Work Plans

According to Shor's algorithm, it is anticipated that public key encryption schemes such as ECC and RSA, which rely on factoring and discrete logarithmic problems, will continue to be considerably susceptible when confronted with the capabilities of quantum computing (QC). The numerical value of 96 provided by the user lacks any accompanying context or information. As a result, it is difficult to ascertain the significance or relevance of this value within a specific domain or research area. However, it is crucial to bear in mind that several quantum - safe encryption methods have been developed, demonstrating potential for long - term viability, possibly extending into the next century. This is particularly significant considering the anticipated emergence of quantum computing (QC) within the next few decades. The National Institute of Standards and Technology (NIST) has recently published the four encryption techniques that have been approved for use in the post - quantum era. The CRYSTALS cryptography package comprises a collection of various techniques that have been devised specifically for algebraic lattices. Several algorithms have been developed in the field of cryptography. These include the lattice - based Dilithium signature scheme, the cryptographic signature algorithm FALCON, the stateless hash - based signature scheme SPHINCS+ (which is an enhanced version of SPHINCS), and the cryptographic signature method CRYSTALS - Kyber [see page 97–99]. The provided spectrum represents the subjects of active research in the realm of cryptography include lattice cryptography, code - based cryptography, multivariate

cryptography, the super singular isogeny key exchange protocol, and symmetric key systems such as AES and SNOW - 3G. The interval [10–14] represents a range of numerical values. The time span in question is At the core of Campagna's latest postulation are three fundamental inquiries regarding the timeframe required to fulfill our health sector requirements.

The inquiries encompass a broad spectrum of subjects, encompassing (a) the assurance of the robustness of our encryption techniques, (b) the assurance of the quantum - resilience of our IT infrastructure, and (c) the determination of the timeline for the construction of a large - scale quantum computer. Regarding the numerical data provided by the user, a value of 105 has been supplied. Transmons and superconducting traps are two prominent examples of the physical hardware components that are essential in the fabrication of qubits. The successful utilization of these hardware components necessitates a comprehensive understanding of cavity quantum electrodynamics. The user has provided a numerical representation of a value, specifically [13, 16, 17].

There is currently a significant amount of effort being dedicated by numerous individuals towards enhancing the field of topological quantum computing. The construction of the largest operational Quantum Key Distribution (QKD) network to date was undertaken by a group of esteemed academics. The remarkable achievement showcased the potential of quantum technology in the realm of secure communication through the integration of photons and relay optics. This achievement holds significant importance in the field of quantum networking, representing a major advancement.

References

[1] Liu X, Sutton PR, McKenna R, et al. Evaluation of Secure Messaging Applications for a Health Care System: A Case Study. Appl Clin Inform 2019; 10 (1): 140–150. DOI: 10.1055/s - 0039 - 1678607.
[2] De Moor G, Claerhout B, De Meyer F. Implementation framework for digital signatures for electronic data interchange in healthcare. Stud Health Technol Inform 2004; 110: 90–111. PMID: 15853257.
[3] Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. The AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic–Patient Electronic Mail. J Am Med Inform Assoc 1998; 5 (1): 104–111. DOI: 10.1136/jamia.1998.0050104.
[4] Donaldson A. Policy for cryptography in healthcare: A view from the NHS. Int J Med Inform 2000; 60 (2): 105–110. DOI: 10.1016/s1386 - 5056 (00) 00109 - x.
[5] He Y, Aliyu A, Evans M, et al. Health care cybersecurity challenges and solutions under the climate of COVID - 19: Scoping review. J Med Internet Res 2021; 23 (4): e21747. DOI: 10.2196/21747.
[6] Yu YW, Weber GM. Balancing accuracy and privacy in federated queries of clinical data repositories: Algorithm development and validation. J Med Internet Res 2020; 22 (11): e18735. DOI: 10.2196/18735.
[7] Bos JW, Lauter K, Naehrig M. Private predictive analysis on encrypted medical data. J Biomed Inform 2014; 50: 234–243. DOI: 10.1016/ j. jbi.2014.04.003.
[8] Mohammed EA, Slack JC, Naugler CT. Generating unique IDs from patient identification data using security models. J Pathol Inform 2016; 7: 55. DOI: 10.4103/2153 - 3539.197203.
[9] Malmurugan N, Nelson SC, Altuwairiqi M, et al. Hybrid encryption method for health monitoring systems based on machine learning. Comput Intell Neurosci 2022; 2022: 7348488. DOI: 10.1155/ 2022/7348488.
[10] Filkins BL, Kim JY, Roberts B, et al. Privacy and security in the era of digital health: What should translational researchers know and do about it? Am J Transl Res 2016; 8 (3): 1560–1580. PMID: 27186282.
[11] Asai A, Konno M, Taniguchi M, et al. Computational healthcare: Present and future perspectives (Review). Exp Ther Med 2021; 22 (6): 1351. DOI: 10.3892/etm.2021.10786.
[12] Tariq RA, Hackert PB. Patient Confidentiality. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing, 2022.
[13] Yang L, Brome CR, Butterworth JS, et al. Invited article: Development of high - field superconducting Ioffe magnetic traps. Rev Sci Instrum 2008; 79 (3): 031301. DOI: 10.1063/1.2897133.
[14] Solenov D, Brieler J, Scherrer JF. The Potential of quantum computing and machine learning to advance clinical research and change the practice of medicine. Mo Med 2018; 115 (5): 463–467. PMID: 30385997.
[15] Tim Hollebeek. How long before quantum computers break encryption? Available at: https: //www.helpnetsecurity. com/2019/ 09/30/quantum - computers - break - encryption/ 2019. Accessed date: 31 October 2022.
[16] Vinod Vaikuntanathan. Quantum computing: The new moonshot in the cyber space race Available at: https: //www.helpnetsecurity. com/2019/08/23/cyber - space - race/ 2019. Accessed date: 31 October 2022.
[17] Brendyn Lotz. What does quantum computing mean for cybersecurity, healthcare and the internet? Available at: https: //www.htxt. co. za/2019/04/02/what - does - quantum - computing - mean - for - cybersecurity - healthcare - and - the - internet/ 2019. Accessed date: 31 October 2022.
[18] Gulbahar B. Theory of quantum path computing with Fourier optics and future applications for quantum supremacy, neural networks and nonlinear Schrodinger equations. Sci Rep 2020; 10 (1): 10968. DOI: 10.1038/s41598 - 020 - 67364 - 0.
[19] Kuhn MG. Some introductory notes on quantum computing. Available at: https: //www.cl. cam. ac. uk/~mgk25/quantum. pdf 2000. Accessed date: 31 October 2022.
[20] Sengupta K, Srivastava PR. Quantum algorithm for quicker clinical prognostic analysis: An application and experimental study using CT scan images of COVID - 19 patients. BMC Med Inform Decis Mak 2021; 21 (1): 227. DOI: 10.1186/s12911 - 021 - 01588 - 6.