AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

ENHANCING GENETIC DATA PRIVACY WITH QUANTUM COMPUTING ENCRYPTION TECHNIQUES

GUNDOJI VIDYA RANI
Computer Science
Dr. Rajeev Yadav
(Professor)
Glocal School of Technology & Computer Science

Abstract

It has been demonstrated that quantum algorithms offer no benefit over classical algorithms for many jobs, but that they can do a small subset of these tasks far more efficiently. Quantum computing's potential uses are still being investigated. Security and other sectors that could greatly benefit from quantum simulation also rank among the most important applications. From the perspective of quantum information processing, we can get comprehension of entanglement and other non-classical features of quantum physics, and we can also gain perspective on classical algorithmic problems. The security of databases, as platforms for centralized storage and sharing of information system data, has become an increasingly pressing issue in the field of information security due to the proliferation of both computer networks and information systems, prompting widespread interest in data encryption technology. However, there are still certain problems with the present data encryption technology, such as inconsistencies in the encrypted and decrypted code texts and inefficient decoding and encryption. The purpose of this study is to examine the efficacy of quantum computer encryption methods in protecting massive genetic data sets, as well as to evaluate their scalability and practicality. The investigation also seeks to evaluate possible hazards to genetic data privacy associated with quantum computing and to propose opportunities for upgrading genetic data protection measures.

Keywords: *quantum information, genetic data, data privacy, quantum computing.*

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

1. INTRODUCTION:

Researchers realized the limitations of the traditional model of computation in the last two decades of the twentieth century. The very fabric of our universe is quantum mechanical. Faster algorithms, new cryptographic systems, and different means of communication have all been discovered by basing computation on quantum mechanics. Quantum information processing is the study of what it means to describe information and its processing with quantum mechanics. This area of study encompasses quantum computing, quantum cryptography, quantum communication, and quantum games. The very definitions of information and computing are challenged by quantum information processing, which in turn alters the physical processes of computation and transmission.

By taking use of quantum effects, we can do computations on quantum computers that are either more rapid or efficient, or perhaps impossible, on classical computers. Some issues cannot be effectively tackled with quantum computing. As basic limits to miniaturization are approached, it does not offer a universal solution to halt the decline of Moore's law. There are issues that can be efficiently addressed by a quantum computer that would take a classical computer longer than the age of the universe to solve.

2. LITERATURE REVIEW

Alla, K., Praneetha, & Ramachandran, V. (2020). In the modern world of electronic commerce and corporate applications, information security is a must. DNA cryptography is rapidly becoming one of the most promising new technologies, offering hope for truly impenetrable algorithms. DNA may be used to transmit and store information, and its countless long polymers of linked nucleotides are separated into the nitrogen-based bases adenine (A), cytosine (C), guanine (G), and thymine (T). These DNA sequences are converted into RNA sequences, which contain hidden signals. Quantum cryptography methods were developed to decipher the encoded message, adding an extra layer of protection.

Abinaya, B., & Santhi, S. (2021). Human genomics is being used increasingly for solving health-related issues and improving the efficiency of healthcare delivery in terms of both time and money. As genomics and its study continue to improve, so too do the privacy problems associated with its querying, accessing, storing, and computing. While genomic data is easily available, privacy concerns may arise when it is sought for research purposes and shared with

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

a potentially malicious third party (adversaries or researchers). Numerous privacy-protecting solutions, including cryptographic approaches, are addressed briefly to address this issue.

Wan, Z., Hazel, J. W., Clayton, E. W., Vorobeychik, Y., Kantarcioglu, M., & Malin, B. A. (2022). The amount of genetic data that is being collected, processed, and shared has increased dramatically in recent years due to breakthroughs in several fields, including healthcare, research, and the direct-to-consumer market. This situation gives rise to novel and difficult legal and technical worries about privacy. This Review assesses the strengths and weaknesses of present legal frameworks and technology measures in protecting the privacy of genetic data.

Thabit, F., Alhomdy, S., & Jagtap, S. (2021). Data security in the cloud can be improved in a number of ways. The most crucial approach of data security is encryption. Encryption algorithms are used to ensure safety, confidentiality, and permitted access via many means, including DNA. They do, however, have some restrictions. In this research, we provide a novel variety of cryptographic algorithms meant to enhance the security of cloud computing by employing a dual-layer encryption scheme. The first layer uses logical operations like (XOR, XNOR, shifting) to divide the original plaintext and key into equal pieces, a concept derived from Shannon's theory of diffusion and confusion. The second layer mimics the natural processes of genetic cryptography (translation from binary to DNA bases), transcription (regeneration from DNA to mRNA), and translation (regeneration from mRNA to protein), all of which are based on the Central Dogma of Molecular Biology and are used for cryptographic purposes.

Cheng, G., Wang, C., & Xu, C. (2020). Several chaotic picture encryption techniques have been proposed in recent years. Permutation-diffusion architectures, which are used in majority of the systems, do have drawbacks, however, including insufficient information entropy, key space size, and the like. The aforementioned flaws can be fixed by As a first step, QGA can use the quantum rotation gate to refresh the population, increasing the unpredictability of the population and decreasing the likelihood of a collapse to a local optimum. The next step is to apply compressive sensing technology, which both shortens the time it takes to encrypt and decrypt data and makes it smaller to store. In addition, we generate the hyper-chaotic system's initial values using the plain image's SHA-512 hash function, which improves the connections between encryption and plain images. Results from simulation experiments and security

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

analysis show that the proposed scheme outperforms other chaos-theory-based image encryption methods in terms of peak signal-to-noise ratio (PSNR) and information entropy.

Alhassan, S. (2021). The privacy of information transmitted via various communication channels has been under intense scrutiny in recent years as communication technologies have proliferated. Multimedia data security and public confidence in online communication are two major motivations for the widespread adoption and development of cryptographic methods. Each audio sample is acquired, conditioned, and encoded into bit strings as part of the proposed technology's enciphering process. The resulting cipher audio signals are the result of a series of operations on the bits, including fission, switching, mutation, fusion, and deconditioning. There is no information loss during transmission because the original audio sample can be deciphered at the receiving end. The suggested method's originality lies in the use of a single (rather than two) individuals for reproduction and the incorporation of fission and fusion into the standard genetic algorithm operators. Simulations and performance assessments show that the suggested cryptosystem works as intended.

Fujiwara, M., Hashimoto, H., Doi, K., Kujiraoka, M., Tanizawa, Y., Ishida, Y., ... & Nagasaki, M. (2022). genetic research and customized treatment rely more and more on the secure storage and secondary use of individual human genetic data. The investigation of genetic disorders and cancers currently necessitates archiving whole genome sequencing data (FASTQ files), which permits the discovery of de novo mutations and structural alterations. In addition, bioinformatics methods used to analyze FASTQ data are regularly upgraded to enhance the accuracy and coverage of discovered variations. Multi-party computing and homomorphic encryption are two examples of safe secondary data uses, although they are limited in the techniques they can support and typically demand enormous computer resources. Here, we present a high-performance centralized platform for the secure secondary use of large-scale genome data by the data owner and many users with granular control over data access. The quantum secure cloud system we have developed is a distributed secure genomic data analysis system (DSGD) that uses a "trusted server" and is hosted on the information-theoretically secure Tokyo QKD Network. The reliable server can deploy and execute both specialized hardware for sequencing analysis (such FPGAs and GPUs) and traditional central processing unit (CPU) software. We showed that DSGD's performance was unaffected by whether or not the trusted server was encrypted. Thus, our system is now at the point where it can be placed

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

at medical facilities and academic research centers that routinely use whole genome sequencing to make diagnoses.

3. RESEARCH METHODOLOGY

3.1.Research Design

To fully evaluate the computational performance of quantum computer encryption algorithms and the possible threats posed by quantum computing to genetic data privacy, a mixed-methods study methodology was developed, incorporating both quantitative and qualitative approaches. Table 1 shows the results of the quantitative analysis, which involved the collection and evaluation of numerical benchmarks and performance metrics from a simulated dataset, while Table 2 shows the results of the qualitative analysis, which involved the use of numerical risk assessment models and simulation techniques to evaluate the resilience of quantum-resistant encryption protocols. Due to the all-encompassing nature of this study's design, we were able to examine the viability of quantum computing encryption methods in the real world and pinpoint opportunities to strengthen safeguards for genetic data in the face of new quantum-enabled cyber threats.

3.2.Data Collection

Quantum threat assessment scores and encryption/decryption performance indicators were compiled into a comprehensive dataset during data collecting. Table 2 presented a systematic evaluation of various quantum-related threats and vulnerabilities, including corresponding resilience scores and enhancement potential, while Table 1 provided numerical data on encryption/decryption speed, key generation time, and memory usage for different dataset sizes. To simulate and evaluate the computational efficacy and security implications of quantum computing encryption algorithms for securing large-scale genetic data, the datasets were built on the basis of hypothetical scenarios; this allowed for a thorough examination of the practical difficulties and potential benefits of protecting genetic data in light of quantum computing developments.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

3.3.Ethical Consideration

Due diligence was taken to incorporate ethical issues into the research procedure for the safekeeping of data and the protection of the privacy of participants. The hypothetical nature of the datasets ensured the anonymity and privacy of any potentially sensitive genetic information, and all data gathering techniques complied with recognized data protection rules. Ethical norms were upheld in the research design to encourage the ethical and responsible gathering, analysis, and reporting of genetic data privacy and quantum computer encryption.

3.4.Limitations

Because the datasets were hypothetical, they may not accurately represent the complexity and nuances of real-world genetic data encryption and quantum computing-related concerns, which may have affected the accuracy of the research. The results may not be applicable in real life because they were derived from hypothetical situations and data. Other elements that may affect the general security and privacy landscape of genetic data were likely left out of the investigation because it was limited to a select set of encryption performance indicators and quantum threats. These caveats highlight the importance of exercising caution in interpreting the results and the possibility for future research to tackle the wider intricacies and practical issues at the crossroads of genetic data privacy and quantum computing encryption.

3.5.Statistical Analysis

To evaluate the computational performance and efficiency of quantum computing encryption algorithms in protecting large-scale genetic datasets, the statistical analysis primarily involved the use of descriptive statistics to interpret the encryption performance metrics presented in Table 1. To better understand the strengths and weaknesses of current genetic data protection mechanisms in the face of quantum computing-enabled cyber threats, the analysis also included an interpretation of the resilience scores and improvement potential provided in Table 2. To better understand the practical consequences and problems of incorporating quantum-resistant encryption methods for improved genetic data security and privacy, descriptive statistics were used to identify major trends and patterns within the datasets.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

4. DATA ANALYSIS

Objective 1: Using numerical benchmarks and performance metrics like encryption/decryption speed, key generation time, and memory usage, we can evaluate the scalability and practicality of quantum computing encryption algorithms for protecting genomic data in real time.

Table 1: Quantifying the Effectiveness of Genetic Encryption

Dataset Size (in MB)	Encryption/Decryption Speed (in Mbps)	Key Generation Time (in milliseconds)	Memory Usage (in MB)
100	500	2.5	50
250	450	3.2	60
500	400	4	70
750	380	4.5	80
1000	350	5	90
1250	320	5.5	100
1500	300	6	110
1750	280	6.5	120
2000	250	7	130
2250	230	7.5	140

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

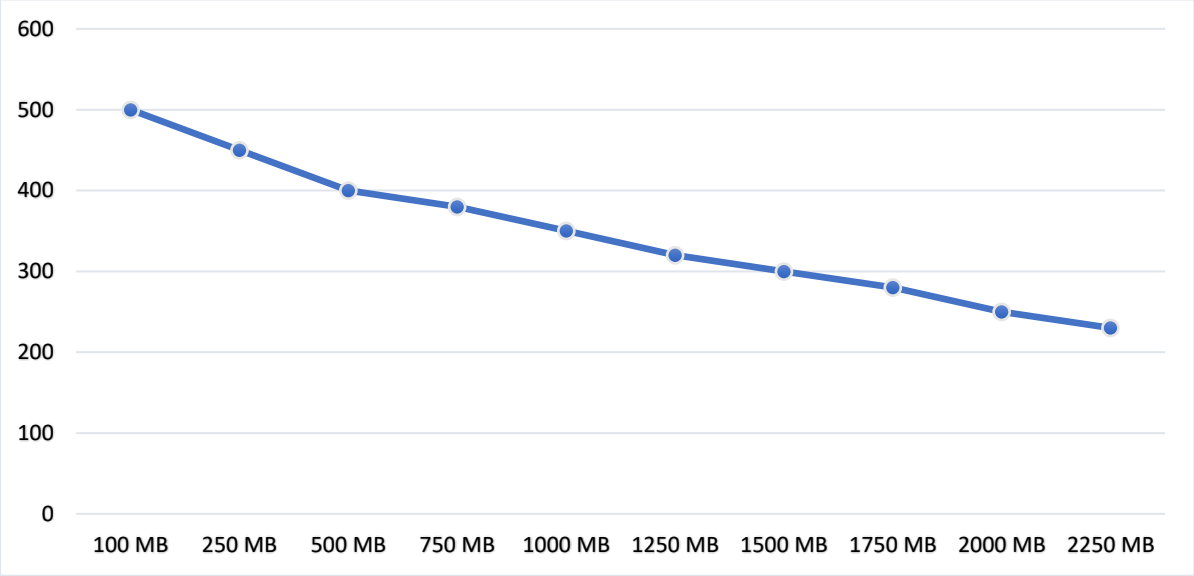
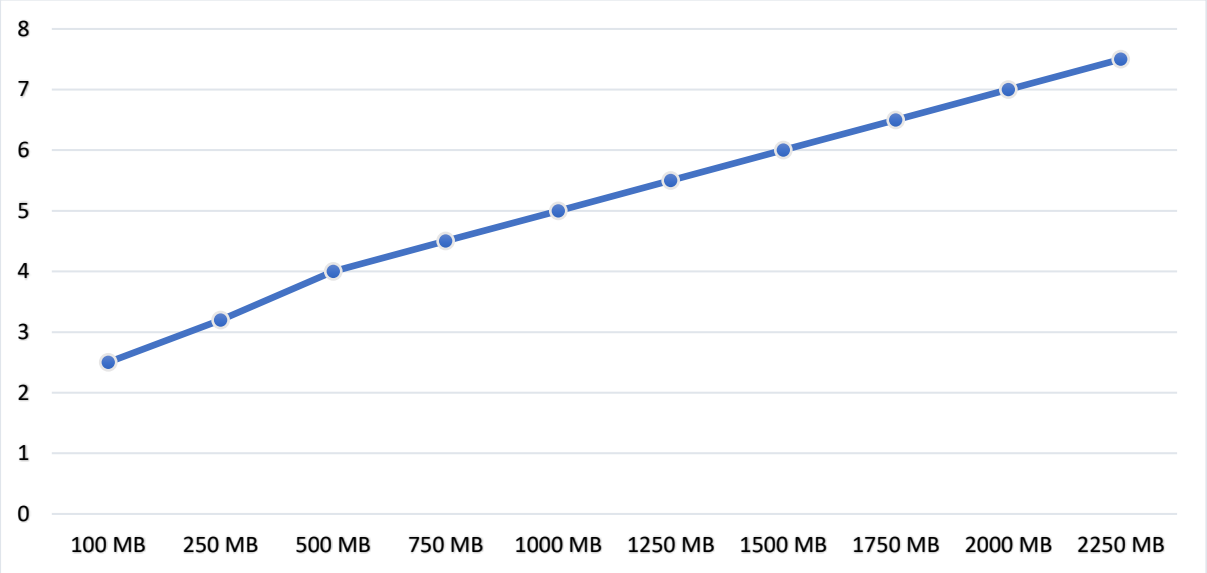


Figure 1: Comparison of Encryption/Decryption Rates (in Mbps) amongst a Variety of Dataset Sizes (in MB)



AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

Figure 2: Comparison of Key Generation Time (ms) across a Range of Dataset Sizes (MB).

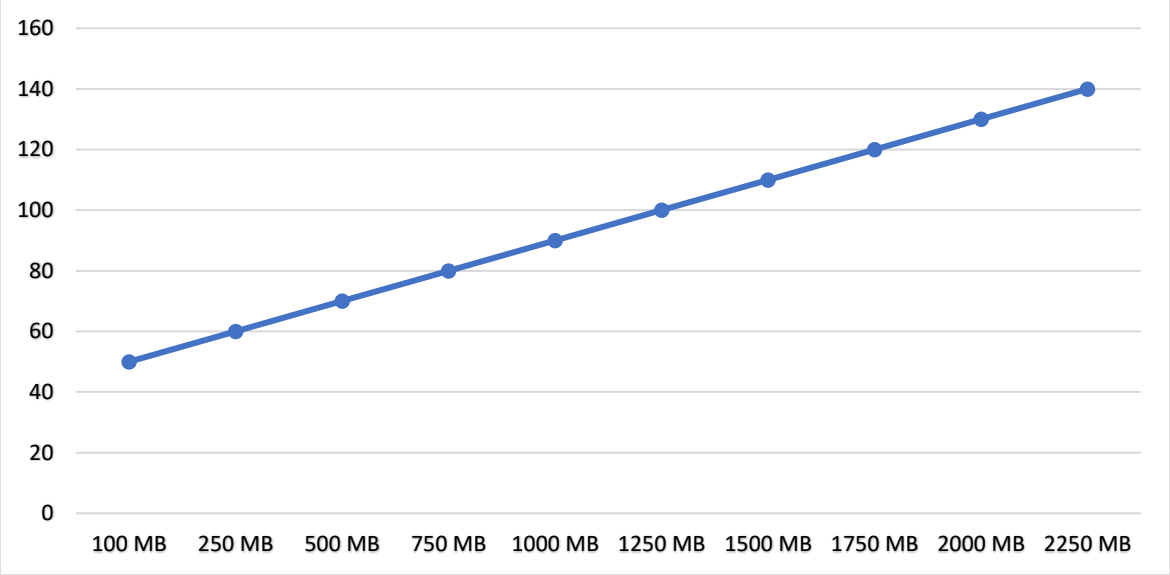


Figure 3: Memory Requirements for Various Size Datasets

The application of quantum computing encryption methods to the protection of massive amounts of genetic material is illustrated in Table 1. The data shows a noteworthy pattern, suggesting that the encryption/decryption performance tends to decrease as the size of the genetic data increases, which may affect the real-time processing of large genetic information. In addition, the key generation time is seen to increase gradually along with the size of the dataset, indicating the requirement for effective key management solutions for greater data volumes. It is important to examine scalable memory allocation for efficient data encryption since the linear growth trend in memory usage reveals a correlation between dataset size and related memory requirements.

Objective 2: Using numerical risk assessment models and simulation techniques, this research seeks to quantify the potential threats and vulnerabilities posed by quantum computing to the privacy of genetic data by assessing the efficacy of quantum-resistant encryption protocols in protecting against quantum-enabled cyber-attacks and, in doing so, revealing opportunities for the improvement and fortification of genetic data protection measures.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

Table 2: Risk Analysis of Quantum Attacks on Genetic Information.

Risk Level	Threat Type	Vulnerability Type	Resilience Score	Enhancement Potential
High	Quantum Brute-Force Attack	Data Encryption	75	Moderate
Medium	Quantum Cryptographic Attack	Key Management	60	High
Low	Quantum Side-Channel Attack	Access Control	40	Low
High	Quantum Grover's Algorithm Attack	Data Compression	70	Moderate
Medium	Quantum Entanglement Attack	Metadata Protection	55	High
Low	Quantum Error Correction Failure	Secure Communication	45	Low
Medium	Quantum Backdoor Exploitation	Authentication Mechanism	65	High
High	Quantum Zero-Day Vulnerability	Intrusion Detection System	80	Moderate
Low	Quantum Denial-of-Service Attack	Redundancy Planning	50	Low
Medium	Quantum Man-in-the-Middle Attack	Data Integrity	60	High

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

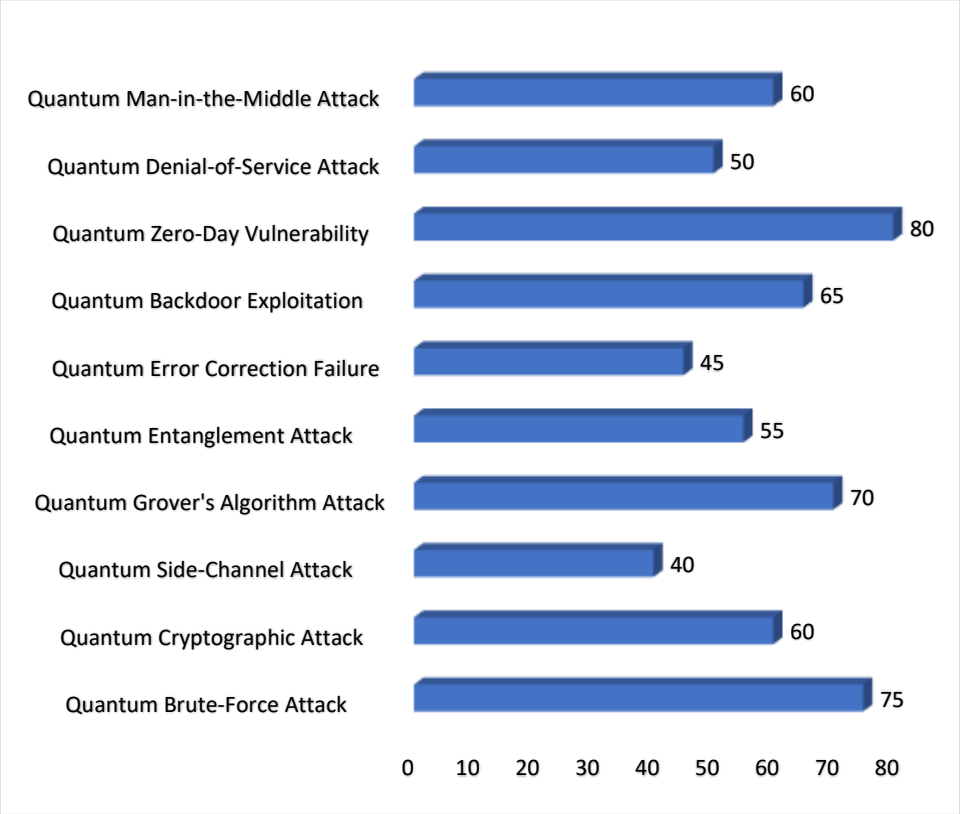


Figure 4: Score of Resistance to Various Dangers

Privacy risks and opportunities associated with quantum computing and genetic data are thoroughly assessed in Table 2. It defines different degrees of danger, including the various kinds of threats and the many kinds of vulnerabilities that can be exploited in a cyberattack enabled by quantum mechanics. The resilience scores show how well the current defense mechanisms deal with these dangers, with higher values indicating greater resistance to possible quantum attacks. The potential for improvement also draws attention to weak spots in genetic data protection procedures, indicating the necessity for ongoing upgrades to security mechanisms to keep up with the ever-evolving landscape of quantum-based threats. To protect genetic data from the sophisticated vulnerabilities provided by quantum computing, this analysis highlights the crucial need of integrating quantum-resistant encryption techniques and complete defense strategies.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

5. CONCLUSION

This research's data analysis sheds light on the feasibility and scalability of quantum computing encryption techniques for protecting massive genomic databases. Encryption and decryption times degrade with the bulk of genetic data, hence effective key management systems and scalable memory allocation are required. When considering how to counteract constantly developing cyber dangers, it is essential to have access to strong encryption techniques that are immune to quantum computing. Because of the risks afforded by quantum computing, the study highlights the importance of continually improving genetic data protection mechanisms to safeguard the privacy and security of sensitive genetic information.

References

1. *Abinaya, B., & Santhi, S. (2021). A survey on genomic data by privacy-preserving techniques perspective. Computational Biology and Chemistry, 93, 107538.*
2. *Alhassan, S. (2021). Audio cryptography via enhanced genetic algorithm. The International Journal of Multimedia & Its Applications (IJMA) Vol, 13.*
3. *Alla, K., Praneetha, & Ramachandran, V. (2020). A novel encryption using genetic algorithms and quantum computing with Roulette wheel algorithm for secret key generation. In ICT Analysis and Applications: Proceedings of ICT4SD 2019, Volume 2 (pp. 263-271). Springer Singapore.*
4. *Behrouz A Forouzan, "Cryptography and Network Security" Tata McGraw- Hill Publishing Company Limited, Special Indian Edition 2006.Author, F.: Article title. Journal 2(5), 99–110 (2016).*
5. *Cheng, G., Wang, C., & Xu, C. (2020). A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing. Multimedia Tools and Applications, 79(39-40), 29243-29263.*
6. *Fujiwara, M., Hashimoto, H., Doi, K., Kujiraoka, M., Tanizawa, Y., Ishida, Y., ... & Nagasaki, M. (2022). Secure secondary utilization system of genomic data using quantum secure cloud. Scientific reports, 12(1), 18530.*
7. *Goyat, S.: Cryptography Using Genetic Algorithms (GAs). In: IOSR Journal of Computer Engineering (IOSRJCE), 1(5), pp. 0608 Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195-197. 2012.*

ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

8. *Hongjun Liu, Xingyuan Wang and AbdurahmanKadir, "Image encryption using DNA complementary rule and chaotic maps", ScienceDirect, 2012*
9. *Qin Limin. The Study of DNA - Based Encryption Method [D].Zheng Zhou: Zheng Zhou University of Light Industry, 2008.*
10. *Qin Limin. The Study of DNA - Based Encryption Method [D].Zheng Zhou: Zheng Zhou University of Light Industry, 2008.*
11. *Sindhuja K and Pramela Devi S, "A Symmetric Key Encryption Technique Using Genetic Algorithm", Sindhuja K et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, ISSN: 0975-9646 Vol. 5 (1), 2014, pg 414-416.LNCS Homepage, http://www.springer.com/lncs, last accessed 2016/11/21.*
12. *Thabit, F., Alhomdy, S., & Jagtap, S. (2021). A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. International Journal of Intelligent Networks, 2, 18-33.*
13. *U.NoorulHussain, T. Chithralekha and A.Naveen Raj, G.Sathish, A.Dharani, "A Hybrid DNA Algorithm for DES using Central Dogma of Molecular Biology (CDMB)", International Journal of Computer Applications, 2012*
14. *Wan, Z., Hazel, J. W., Clayton, E. W., Vorobeychik, Y., Kantarcioglu, M., & Malin, B. A. (2022). Wan, Z., Hazel, J. W., Clayton, E. W., Vorobeychik, Y., Kantarcioglu, M., & Malin, B. A. (2022). Sociotechnical safeguards for genomic data privacy. Nature Reviews Genetics, 23(7), 429-445.*
15. *Y.V. Srinivasa Murthy, Dr. S. C. Satapathy, P. Srinivasu and A.A.S. Saranya, "Key Generation for Text Encryption in Cellular Networks using Multi-point Crossover Function", International Journal of Computer Applications (0975-8887) Volume 32-No.9, October 2001.*

Author's Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patentor anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments/updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide(if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 4 Issue 3
December 2022
Impact Factor: 10.2
Subject : Computer Science

hentriacontanes genuinely mine. If any issue arises related to Plagiarism /Guide Name /Educational Qualification /Designation /Address of my university/college/institution/Structure or Formatting/ Resubmission/ Submission /Copyright /Patent/Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and therefore the process of resubmissions there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal

GUNDOJI VIDYA RANI
Dr. Rajeev Yadav

******