
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN:2321-2152 www.ijmece .com

Vol 10, Issue.4 Dec 2022

# IMPLEMENTATION OF DNA CRYPTOGRAPHY IN CLOUD COMPUTING

**[1] Bhavya Manchukanti, [2] Surkanti Sravan Kumar Reddy,[3] Bellamkonda Upender, [4] Budigijangam Shireesha**

[1,2,3] Assistant Professors,Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

[4]student,Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

## ABSTRACT

Traditional cryptographic methods are becoming less efficient and less resilient in the face of the increasing need for data security in cloud computing settings. An innovative method for protecting private data stored in the cloud is presented in this project. It is called DNA cryptography, and it is based on biological principles. To encode and decode data, it uses the specific characteristics of DNA sequences. Integrating DNA cryptography into cloud-based systems to increase data privacy and security is the major purpose of this study.The method involves encoding data using DNA-based operations after it has been translated into DNA sequences using a mapping technique. For a strong, multi-layered encryption system, the approach uses DNA sequence modification (including transposition, hybridisation, and replacement) in conjunction with conventional cryptographic methods. The information is decrypted after the reverse operation, guaranteeing the safe retrieval of the original data. The suggested DNA cryptography system works well in a cloud computing environment, according to the experimental findings. The system is designed to provide robust data secrecy, attack resistance, and efficient performance even in large-scale settings. Genome cryptography stands out from other cryptographic approaches due to its exceptional computational complexity and secure integration of the two, making it a prime contender for highly secure cloud applications. By investigating the possibilities of

DNA cryptography, this work takes a giant leap forward in the development of quantum-resistant encryption and safe cloud computing. The findings provide the groundwork for future studies that combine bio-inspired cryptography with cloud computing in an effort to find an eternal answer to the ever-increasing problems associated with cloud data security.

## I.INTRODUCTION

Data security has emerged as a major concern in the cloud computing industry due to the growing use of this technology for its scalability, flexibility, and cost-effectiveness. Because of the large amounts of private and sensitive information stored in the cloud, it is vulnerable to cyberattacks, data breaches, and illegal access. Data in cloud settings has traditionally been protected using traditional cryptographic techniques like RSA and AES. But these old cryptographic methods are starting to crumble under the weight of modern cyberthreats, especially those using quantum computing and other sophisticated threat models.

Novel cryptographic techniques that provide improved security features and resistance against new attacks have been investigated by researchers in an effort to alleviate these security problems. An unorthodox approach that draws on the inherent characteristics of DNA molecules is DNA cryptography, one of these novel approaches. DNA

Cryptography makes use of DNA's unique biological features and its enormous information store capacity to encrypt and decrypt data. An alternative to conventional encryption that is both computationally difficult and theoretically safe is DNA cryptography, which draws on biotechnology and computational biology.

In order to better protect data stored in the cloud, this study investigates the possibility of incorporating DNA cryptography into such systems. This architecture adds an extra degree of security by converting data into DNA sequences using encoding methods and then securing the data via a series of DNA operations. The objective is to show that DNA cryptography may overcome the computational complexity and scalability issues with standard encryption methods while substantially enhancing the security, privacy, and reliability of data stored in the cloud.

This study intends to provide the groundwork for more secure cloud

services that can handle future security concerns like quantum computing by integrating DNA-based encryption approaches with cloud computing infrastructures. Biologically inspired security measures and quantum-resistant encryption are just two examples of how the suggested system may revolutionise the way sensitive data stored in the cloud is protected.

## II.SYSTEM ARCHITECTURE

Data security may be improved with the help of DNA cryptography in the cloud by combining existing cryptographic techniques with the special characteristics of DNA sequences. The first step is data encoding, which involves applying a mapping method to convert plaintext data into DNA sequences. The program takes binary data (as 0s and 1s) and transforms it into DNA bases (a, t, C, and g). This format is derived from biology and makes the data unintelligible and secure. At this point, encryption may begin on the data.

After encoding is complete, the system employs a DNA encryption module to further protect the data by applying a variety of DNA-specific operations, including hybridisation, transposition, and replacement. The data becomes unintelligible without the correct decryption key due to the processes that change the DNA sequences. Traditional cryptographic methods, such AES or RSA, are also used with DNA-based processes to provide an additional degree of protection. The data is securely encrypted using this multi-layered technique, protecting it from a variety of cyber-attacks.

For safekeeping and retrieval, encrypted data is then transferred to cloud storage. Data sent between users and the cloud is secured and safeguarded by the cloud's architecture, which permits scalable and flexible data storage via the use of secure communication protocols such as SSL/TLS. To make sure that no unauthorised people may decrypt or change the data, authentication procedures like role-based access controls (RBAC) and multi-factor authentication (MFA) are used.

The system starts the decryption process when an authorised user wants to access the encrypted data. A decryption module takes the encrypted DNA data from the cloud and does the opposite operations (substitution, transposition, hybridisation) on the DNA, therefore decrypting the data. The data is then decrypted using conventional decryption techniques, returning it to its initial plaintext state. After decryption, the user may access the data and utilise it as they see fit.

The system takes further precautions by using quantum-resistant encryption algorithms to ward against any potential dangers that quantum computing may bring in the future. To further secure sensitive information while it is being sent or stored, further data masking and obfuscation methods are used. The audit trail is created by logging and monitoring every data access and modification operations, which helps identify and react to unauthorised access attempts.

The system's intuitive interface makes it simple to manage credentials and permissions, upload, encrypt, and decrypt data. The system's capacity to manage massive amounts of data and a large number of users is ensured by the cloud-based architecture. This takes use of the scalability of cloud computing to effectively conduct resource-intensive encryption and decryption processes. This all-inclusive design offers a scalable and very secure approach for protecting data in the cloud by integrating the biological concepts of DNA cryptography with sophisticated conventional encryption technologies.

## III.EXPERIMENT RESULTS

Here we show you the results of the tests that were run to see how well DNA Cryptography worked in a cloud computing environment. Performance in encryption and decryption, security, scalability, and general system efficiency were among the many characteristics that the studies sought to investigate. The findings shed light on the system's advantages and disadvantages and provide practical advice for using it in cloud settings.

Processing Speed for Encryption and Decryption

This project's success hinged on how well the encryption and decryption functions worked. We timed the system's encryption and decryption processes on data sets of varying sizes. Compared to more conventional cryptography techniques like AES and RSA, the processing time required to decrypt DNA-based data was somewhat longer. Nonetheless, the time difference was manageable for real-world applications. The system was able to maintain efficiency for datasets of modest size, even though encryption and decryption durations rose in direct proportion to the dataset size. The DNA cryptography technology ensured that the system could operate effectively even with higher amounts of data, since it added just a minor processing penalty.

Assessment of Data Security and Integrity

The trials were focused on security.

Multiple attack simulations were run to examine the robustness of DNA cryptography against popular cryptographic techniques. Among these assaults were man-in-the-middle (MITM), brute-force, and known-plaintext ones. Given the enormous key space and great complexity of DNA sequences, the findings demonstrated that the DNA encryption approach was very resistant to brute-force assaults. The complexity of DNA modifications, such as transposition and replacement, rendered known-plaintext assaults useless. The system was also resistant to man-in-the-middle assaults since data was encrypted at rest and in transit using SSL/TLS and other secure communication protocols.

Efficient Scalability in the Cloud

Another important consideration was scalability. By using a cloud-based architecture, we were able to evaluate the system's capacity to manage many users and massive amounts of data. The findings showed that the system could handle many user queries effectively without suffering a major drop in performance. Distributing encryption and decryption operations to the cloud enabled fast processing even when faced with huge loads. Even though the storage size increased somewhat because of the DNA encoding, the storage efficiency was sufficient. The increase was small, however, and contemporary cloud storage options should have no trouble handling it.

Practicality and User-Friendliness

System usability and the user interface (UI) were also evaluated. The user interface was made with ease of use in mind, so users can quickly and simply upload, encrypt, and decrypt data. The interface also allowed users to modify their rights and credentials. According to user reviews, the interface was simple and easy to understand, allowing users of all skill levels to use the system with ease. To make sure the complicated DNA cryptography procedures didn't get in the way of the user experience, this simplicity was crucial.

Evaluation in Light of Conventional Cryptography Techniques

We compared DNA cryptography's performance to that of more conventional encryption algorithms, such as AES and RSA, in order to assess its benefits. Although the encryption and decryption times for DNA cryptography were somewhat longer, the security level was much greater since the data transformation was biological in nature. Without the right key, the DNA encoding process—which involves complicated procedures like hybridisation and transposition—is very difficult to

decipher. The comparison showed that standard approaches are popular and effective, but DNA cryptography adds another level of protection that can be useful for cloud-based sensitive data.

Important Results and Restrictions

The tests revealed many important things. The DNA cryptography system first showed that it could encrypt and decode data efficiently while adding very little computing cost. Second, it was secure; brute-force, known-plaintext, and man-in-the-middle attacks were all successfully warded off by the system. Thirdly, the system worked well in cloud settings, scaling to accommodate big datasets and many users without sacrificing speed. The increased storage needs caused by the DNA encoding was one of the limitations that were noted. This growth, however, was controllable and did not cause cloud storage any major problems. The difficulty of developing and deploying DNA cryptography—which required unique algorithms and hardware for DNA encoding and decoding—was another obstacle.

Data Synopsis from the Experiment

The findings of the experiment show that DNA cryptography in cloud computing is a good way to safeguard sensitive data. Time to encrypt and decrypt, security, and scalability were all strong points of the system's performance. A number of cryptographic assaults were successfully countered by the hybrid encryption method, which incorporates DNA cryptography with more conventional techniques. But there's room for development, especially in terms of improving the efficiency of DNA encoding and decoding. Given the new dangers posed by quantum computing, future research may include quantum-resistant encryption methods to fortify the system's defences even more.

## IV.CONCLUSION

We effectively investigated the use of DNA Cryptography within the framework of Cloud Computing to fortify the protection of private information in this project. The results showed that DNA cryptography is a viable alternative to conventional encryption due to its novel biological encoding methods. In addition to guaranteeing robust encryption, our method fortifies the encryption process against popular assaults like brute force and known-plaintext by using the enormous keyspace of DNA sequences. When compared to more conventional encryption algorithms like AES and RSA,

the system's speed proved more than enough for real-world applications, with just a little overhead. Because DNA encoding is inherently space-intensive, the DNA-based system displayed a rise in storage needs; nonetheless, this posed little to no problem because cloud storage can readily handle such increases. The system's scalability was also confirmed to be strong, with no noticeable drop in performance even when dealing with many users and massive datasets.

Results from security testing showed that the system could withstand typical cryptographic assaults, making it an excellent choice for securing data stored in the cloud. Particularly important in today's cloud-based applications, where data breaches are becoming an increasingly pressing issue, the combination of DNA cryptography with conventional encryption techniques provides an additional degree of protection.

While these findings are encouraging, the experiment did reveal several limits, such as how difficult it is to implement DNA cryptography and how specific algorithms and tools are required for data encoding and decoding. Improving the efficiency of these processes and investigating advanced strategies like quantum-resistant algorithms to ward off future quantum computing dangers should be the focus of future research.

## VI.REFERENCES


1. Adel, A., & El-Latif, A. (2017). "A DNA-based encryption system for cloud computing applications." *International Journal of Cloud Computing and Services Science (IJCCSS)*, 6(3), 147-159.

2. Ahmed, M., & Zulkernine, M. (2013). "Secure DNA-based cryptographic systems for cloud data protection." *Proceedings of the International Conference on Cloud Computing and Big Data Analysis* (pp. 167-171).

3. Benny, P., & Singh, G. (2019). "DNA cryptography: A secure framework for cloud storage applications." *IEEE Transactions on Cloud Computing*, 7(3), 1-9. DOI: 10.1109/TCC.2019.2906891.

4. Brierley, S., & Santelices, M. (2018). "Implementing DNA encryption in the cloud: A comparative study." *Journal of Computational Security*, 5(2), 111-118.

5. Chin, K., & Chin, W. (2015). "DNA cryptography: A survey of recent developments in data security." *Future Generation Computer Systems*, 49, 135-147. DOI: 10.1016/j.future.2014.07.012.

6. Das, S., & Ghosh, D. (2020). "A DNA-based approach for cloud data encryption and security." *Journal of Information Security and Applications*, 53, 102507. DOI: 10.1016/j.jisa.2020.102507.

7. Gonzalez, F., & Torres, L. (2017). "DNA-based cryptography in cloud computing: A practical approach." *International Journal of Network Security*, 19(5), 765-777.

8. Gupta, P., & Soni, V. (2018). "Cloud computing security: DNA-based cryptographic model for cloud data protection." *Proceedings of the International Conference on Cloud Computing Technologies* (pp. 345-355).

9. Hu, X., & Tang, J. (2019). "Efficient DNA cryptography for cloud data storage." *International Journal of Computer Applications*, 168(1), 50-59.

10. Jin, W., & Gao, Y. (2017). "Implementing DNA encryption algorithms for cloud data security." *Cloud Computing and Security: Proceedings of the 5th International Conference on Cloud Computing (CloudCom)*, 98-109.

11. Khan, S., & Zaman, N. (2016). "DNA cryptography techniques for secure cloud computing." *International Journal of Computer Science and Information Security (IJCSIS)*, 14(6), 51-60.

12. Liu, S., & Li, J. (2020). "An enhanced DNA cryptography algorithm for cloud data security." *Journal of Cryptology*, 33(3), 837-856. DOI: 10.1007/s00145-019-09321-7.

13. Moses, J., & Ramaswamy, S. (2021). "Cloud data encryption using DNA-based cryptographic algorithms." *Proceedings of the International Conference on Cloud and Big Data Computing* (pp. 92-101).

14. Singh, S., & Yadav, M. (2018). "DNA-based cryptography: Protecting data in the cloud." *Cloud Computing Journal*, 6(4), 65-72.

15. Zhou, L., & Xu, L. (2019). "Secure DNA cryptography for cloud storage applications: A review." *IEEE Access*, 7, 132456-132471. DOI: 10.1109/ACCESS.2019.2938931.