IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cloud-Based DNA Cryptography: Advancing Data Protection Paradigms

[1]Shirley Castelino, [2]Simran Gupta, [3]Archana Kalathiya, [4]Kumud Wasnik

[1,2,3]Student at Usha Mittal Institute of Technology, [4]Associate Professor at Usha Mittal Institute of Technology
Department of Computer Science and Technology,
Usha Mittal Institute of Technology, SNDT Women's University, Mumbai, India 400049

Abstract: Cloud computing has gained widespread popularity and has emerged as a prominent trend in the field of In- formation Technology. This review explores the significance of cloud computing and its security challenges, focusing on the Bi- directional DNA Encryption Algorithm (BDEA). Despite BDEA's promise, its reliance on ASCII characters poses limitations for non-English users. Efforts to enhance its efficacy with Unicode characters are discussed. The study covers the evolution of data protection methodologies, including DNA cryptography's integration with cloud computing. A proposed DNA-based encryption algorithm employs DNA Digital Coding, Key Combination, DNA Steganography, Graphical Password, and Digital Signature techniques, reinforced by binary coding rules. This amalgamation of biomolecular principles and cryptographic methods offers unparalleled security. The research marks a pivotal stride in augmenting the security landscape of cloud computing, paving the way for impregnable data protection. Through rigorous exploration and innovation, this project aims to secure the digital realm effectively.

Index Terms **- cryptography, digital signature, steganography, cloud computing**

I. INTRODUCTION

The digital era has brought about a heightened focus on data security, particularly with the widespread adoption of cloud computing, where sensitive information is frequently stored and accessed remotely. However, traditional cryptographic solutions face significant challenges as cyber threats evolve, necessitating a paradigm shift in data protection methods.

To address these challenges, our research proposes a novel security framework: Cloud-Based DNA Cryptography. This innovative approach combines the advanced capabilities of cloud computing with the intricate mechanisms of DNA-based encryption. DNA cryptography, inspired by biological systems, leverages the parallelism and storage capacity inherent to DNA molecules to encode information in a highly complex and secure manner.

By integrating DNA cryptography with cloud technology, we aim to create a sophisticated platform for data management that raises the bar for security standards in the cloud. This dual-powered approach offers scalability and adaptability to meet the growing demands of data security.

The problem addressed by this research project lies in developing and implementing an effective Cloud-Based DNA Cryptography system that enhances data security within cloud environments. Key aspects of this problem include:

- Enhanced Data Security: Developing a robust DNA- based encryption algorithm to ensure confidentiality and integrity of data stored in the cloud, protecting it from unauthorized access and attacks.
- Efficiency and Scalability: Designing an encryption and decryption process that is efficient and scalable to accommodate large volumes of data and user demands in cloud environments.
- Compatibility with Cloud Infrastructure: Ensuring compatibility with existing cloud platforms and services for seamless integration into various applications and systems.
- Error Correction and Data Integrity: Addressing challenges related to errors in DNA sequencing to ensure accurate decryption and maintain data integrity throughout the process.
- Privacy and Ethical Considerations: Develop protocols and safeguards to protect genetic information, adhere to ethical guidelines, and prevent misuse or discrimination based on genetic data.

This research aims to bridge the gap between DNA cryptography and cloud computing, revolutionizing data security while addressing challenges associated with efficiency, scalability, and ethical considerations.

II. LITERATURE SURVEY

A detailed study of research papers has been done that helped in the proper implementation of this project and its observations have been listed below.

Table 2.1: Literature Survey

Sr.-no.	Author	Title	Methodology and Technologies	Observation
1	Prasanna Balaji Narasingapuram and M.Ponnavaikko	DNA Cryptography Based User Level Security For Cloud Computing and Applications, 2020 [1]	In this paper, user information is converted into human deoxyribonucleic acid form for generating a strong key and data encryption. The implementation of the proposed approach is carried out in DOTNET framework.	The proposed method uses a DNA-based key generation algorithm to create a unique key for each user. This key is then used to encrypt the user's data before it is stored in the cloud. When the user wants to access their data, they must first decrypt it using their own key. This method offers several advantages: DNA cryptography is highly secure and efficient, with a very large key space. It provides a strong key for user and data encryption, eliminates malicious user activity in the cloud, and is easy to implement. However, the system's security depends on the key strength and is not scalable for large data sets.
2	Sushma N K, Dr. Ravikumar G K, Ms. Sindhu	Distributed Computing Of DNA Cryptography and Randomly Generated Mealy Machine, 2022 [2]	The proposed system consists of three entities: a key pair generator, a sender, and a receiver. The key pair generator generates a 256-bit DNA-based secret key based on the attributes of the receiver. The sender uses this key to encrypt the data. The encrypted data is then fed into a randomly generated Mealy machine, which generates the ciphertext. The ciphertext is then transmitted to the receiver. The receiver uses the secret key to decrypt the ciphertext.	The method provides high security against various attacks, including brute force, known plaintext, differential cryptanalysis, ciphertext-only, man-in-the-middle, and phishing attacks. It is more secure and scalable for large data sets compared to traditional DNA cryptography systems. However, its security depends on the strength of the secret key. The cost of implementing this system in real-world applications is not considered, and it is not as efficient as some other DNA cryptography systems.
3	Abhay Kumar Manmohan Singh	Implementation Of Two-Fold DNA Cryptography Based on Amino Acid Table In Cloud Computing and Using Socket Programming, 2022 [3]	The paper consists of three entities: a cloud server, a sender, and a receiver. The cloud server stores the amino acid table and the DNA sequences of the sender and receiver. The sender uses the amino acid table to encrypt the data. The encrypted data is then transmitted to the cloud server. The cloud server decrypts the data using the DNA sequences of the sender and receiver. The decrypted data is then transmitted to the receiver.	The proposed method is more secure than existing methods due to the complex key space of the amino acid table and is more efficient because of faster encryption algorithms and efficient data storage. It can be easily implemented in cloud computing using socket programming. However, the system's security depends on the amino acid table and DNA sequences, and it is computationally expensive.
4	Poojashree Kamble, Firoz Nagarchi, Akshata Akkole, Vanishree Khanapur, and Bahubali Akiwate	A Dynamic DNA Cryptography Using R S A Algorithm and OTP, 2020 [4]	In this paper, the plaintext is converted into a DNA sequence using a binary coding technique. The DNA sequence is encrypted using the RSA algorithm. The encrypted DNA sequence is then authenticated using OTP.	The method can encrypt and decrypt text, images, and audio files, and it resists brute-force, frequency analysis, and differential attacks. It generates new keys dynamically for each encryption, providing a dynamic key for encryption. The RSA algorithm adds security, and OTP adds an additional layer of security. However, the system is not scalable for large data sets and is not as secure as some other DNA cryptography systems.

5	Vinay S, H. Akshay Kedlaya, Adarsh Pujar, and Vasudev Shahapur	DNA Cryptographybased on Dynamic DNA SequenceTable using Cloud Computing, 2019 [5]	A dynamic DNA sequence table is created, which maps ASCII characters to DNA sequences. The plaintext is converted to binary using ASCII encoding. A one-time pad is applied to the modified binary data. The OTP ciphertext is converted to genomic form using the dynamic DNA sequence table. The genomic ciphertext is compressed using an amino acid table.	The method is more difficult to crack as the attacker needs to know the dynamic DNA sequence table and the number of iterations used. It is efficient since cloud computing can be used for encryption and decryption operations. However, the system's security depends on the dynamic DNA sequence table's strength, and it is less efficient, requiring random generation of the dynamic DNA sequence table each time data is encrypted.
6	Hamza Ham-mami, Hanen Brahmi, and Sadok Ben Yahia	Secured Outsourcing Towards A CloudComputing Environment Based on DNA Cryptography, 2018 [6]	In this paper, the plaintext is converted into a DNA sequence using a binary coding technique. The DNA sequence is encrypted using DNA cryptography algorithm. The encrypted DNA sequence is then outsourced to the cloud.	The method provides high security using a DNA-based encryption algorithm, suitable for data outsourcing in cloud environments. It is efficient, with relatively fast encryption and decryption processes, making it suitable for real-world applications. However, it is not as efficient as some other DNA cryptography systems and not as secure as some other cloud-based security systems.

III. METHODOLOGY

The architecture diagram presents a cutting-edge approach to data storage and security utilizing cloud-based DNA cryptography to safeguard sensitive information. In today's digital landscape, where data breaches and cyber threats pose significant challenges, organizations are constantly seeking innovative solutions to protect their assets and ensure the integrity of their data. This architecture offers a comprehensive framework that addresses these concerns by leveraging the unique properties of DNA for encryption and authentication purposes.

The architecture depicted in the block diagram outlines a sophisticated and secure data storage system utilizing cloud-based DNA cryptography. The detailed explanation of each component is given below:

1. **DNA Digital Coding:** User input data transforms DNA digital coding using an algorithm specifically designed for this purpose. This step involves encoding the user data into a format that resembles DNA sequences, leveraging the inherent complexity of DNA for enhanced security.
2. **DNA Sequence (Encoded Data):** The DNA digital coding process results in the generation of DNA sequences representing the encoded user data. These sequences serve as the encrypted form of the original data and are ready for storage in the cloud.
3. **Cloud Service:** The cloud service is responsible for storing and managing the encrypted DNA sequences. It provides the infrastructure and resources necessary for secure data storage and retrieval.
4. **DNA Indexing Algorithm (User Mapping):** This component encompasses an indexing algorithm designed to map users to their respective DNA sequences. It facilitates efficient data retrieval by associating each user with their encoded DNA data.

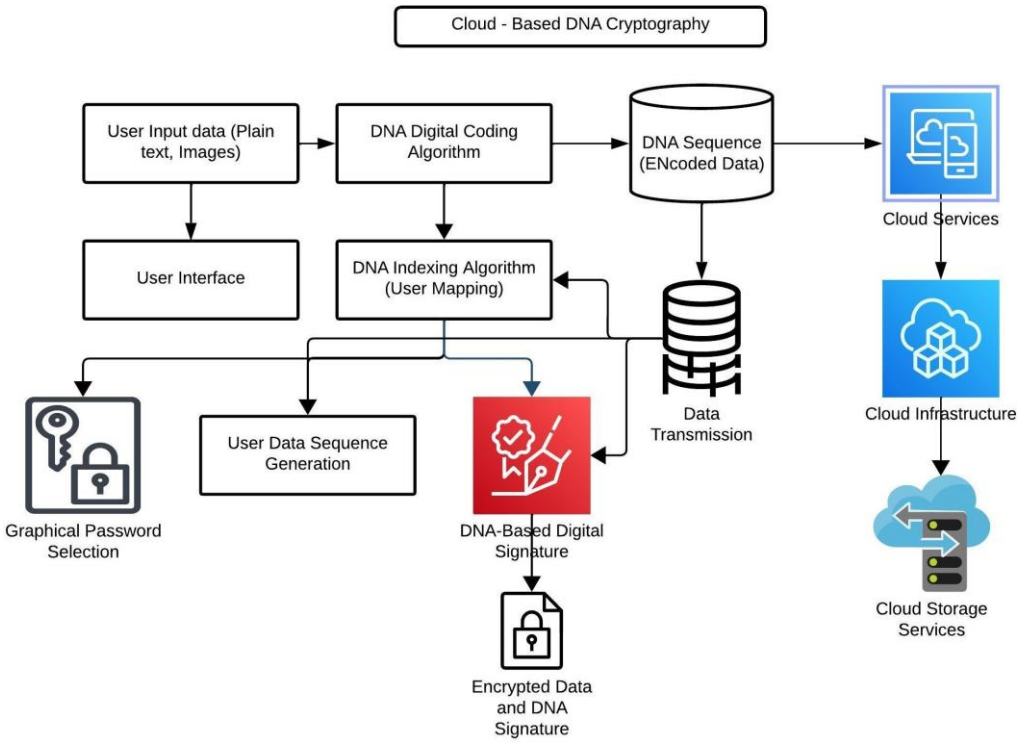

Fig. 1. System Architecture

5. **Data Transmission:** Data transmission handles the transfer of user data and DNA sequences between the client-side application and the cloud service. It ensures seamless communication and synchronization between the user interface and the cloud infrastructure.
6. **User Interface:** The user interface enables users to interact with the system, input data, and manage their accounts. It may include features such as graphical password selection for user authentication and DNA sequence generation.
7. **Graphical Password Selection:** This feature allows users to choose graphical patterns or symbols as passwords for authentication. It adds an additional layer of security by diversifying authentication methods beyond traditional alphanumeric passwords.
8. **DNA-Based Digital Signature:** The DNA-based digital signature is a cryptographic technique used for verifying the integrity and authenticity of DNA sequences. It provides a method for ensuring that the stored data remains unchanged and originated from a legitimate source.
9. **Cloud Infrastructure:** The cloud infrastructure encompasses the hardware and software resources deployed to support the cloud-based storage and processing of DNA-encoded data. It includes components such as servers, databases, and storage services configured to meet the security and scalability requirements of the system.
10. **Encrypted Data & DNA Signature:** This represents the encrypted user data along with the associated DNA signatures. The combination of encrypted data and DNA signatures ensures data confidentiality, integrity, and authenticity throughout the storage and retrieval process.

Workflow

The workflow delineates a robust data management system designed to prioritize security through encryption as its core mechanism. Here's an overview of the key components involved:

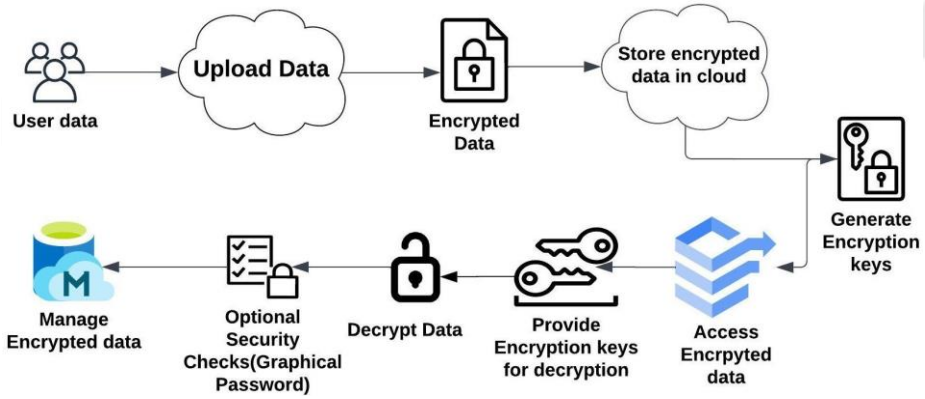

Fig. 2. The Diagrammatic View of Workflow

1. **Data Encryption:** Utilizes advanced encryption techniques to convert user data into a secure format. This process ensures that data is protected from unauthorized access and breaches.

2. **Data Storage:** Encrypted data is stored in a secure environment, such as cloud storage or a dedicated data repository. This ensures the data remains accessible only to authorized users while maintaining its integrity.
3. **User Authentication:** Employs authentication mechanisms to verify the identity of users attempting to access the encrypted data. This step ensures that only legitimate users can access and decrypt the data.
4. **Decryption:** Authorized users can decrypt the encrypted data using a decryption key. This process converts the data back into its original format, making it usable and readable for authorized users.
5. **Data Utilization:** Once decrypted, the data can be utilized for various purposes, such as analysis, reporting, or any other intended application. This step ensures that the data is effectively used while maintaining its security.
6. **Data Transfer:** Encrypted data is securely transmitted between different components of the system. This step ensures that data remains protected during transit, minimizing the risk of interception and unauthorized access.

IV. PROPOSED SYSTEM

The proposed system, known as Cloud-Based DNA Cryp- tography, aims to combine the unique strengths of DNA cryptography and cloud computing to enhance data security, storage efficiency, and communication. This system will in- tegrate various technologies, algorithms, and architectures to ensure secure data encryption, efficient storage, and seamless data retrieval within cloud environments. By leveraging DNA sequences as cryptographic keys and utilizing cloud infrastruc-ture, the proposed system will provide a practical and secure solution for addressing the growing challenges of data securityand privacy.

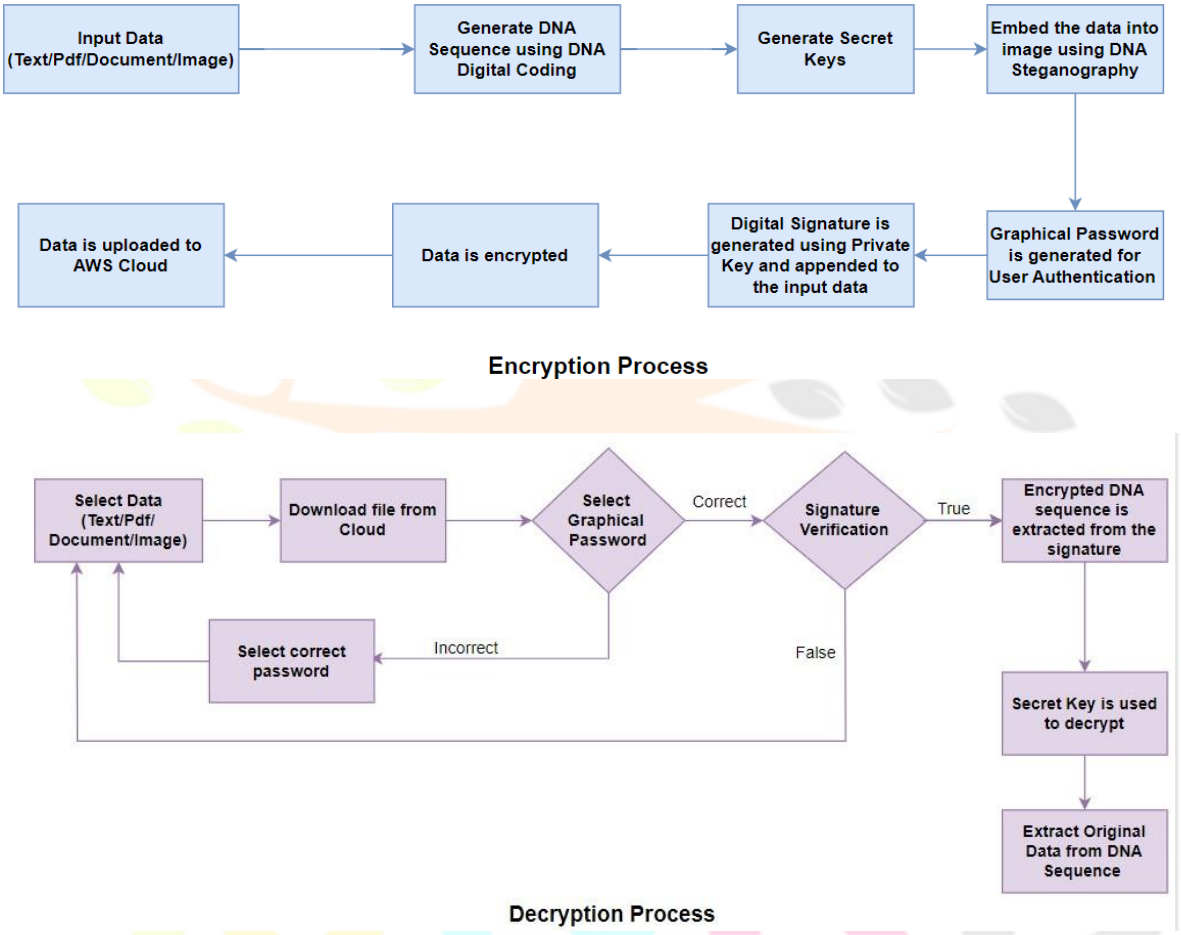

Fig. 3. The Proposed System Diagram

Key Components of the Proposed System:

- **DNA Digital Coding Algorithm:** This component con- verts digital data, such as plaintext messages or files, into DNA sequences. The algorithm maps binary data to DNA bases (A, C, G, T) to represent the encoded information.
- **DNA-Based Digital Signature Algorithms:** DNA sequences will be employed for generating and verifying digital signatures, ensuring data integrity and authenticity. These algorithms will play a crucial role in securing data transactions and communication.
- **Encryption Algorithms:** The Rivest-Shamir-Adleman (RSA) encryption algorithm will be utilized for secure data encryption and decryption. This widely accepted algorithm will provide strong security for the Cloud-Based DNA Cryptography system.
- **Dataset and Data Preprocessing:** The system will work with a dataset consisting of plain-text messages, base images, and image data for graphical password authentication. Data preprocessing will be performed to ensure compatibility with DNA encoding and encryption techniques.
- **Cloud Infrastructure (AWS):** Cloud resources will be set up to facilitate secure storage and processing. Virtual machines and storage services will be configured to accommodate the system's requirements.

V. RESULT ANALYSIS

The project implements a multifaceted approach to secure data encryption and decryption. It begins by transforming the data into a DNA sequence through binary-to-DNA encoding, ensuring a unique representation. RSA key pairs are generatedfor asymmetric encryption, and a graphical password is estab- lished through image selection, enhancing both security and user experience. The DNA-coded data is concealed within an image using steganography, Digital signatures and Amazon S3integration contributing to data integrity and secure storage. During decryption, the graphical password is verified, andthe DNA sequence is decrypted using derived keys. The system recognizes the data type based on file signatures and provides clear success or failure messages. Overall, the projectillustrates a robust security framework encompassing DNA coding, RSA encryption, steganography, and graphical passwords, ensuring a comprehensive and user-friendly approach to data protection. The project supports all formats: Text, Image, PDF and Document. The result of image format is provided below as an example.

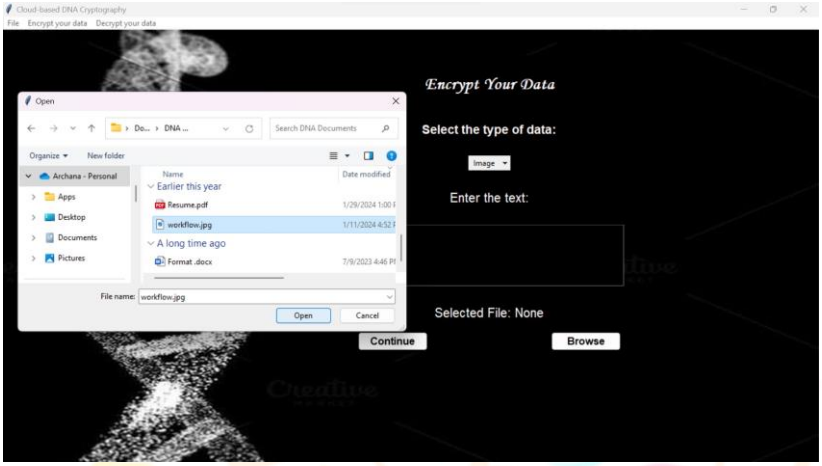

Fig. 4. Upload input image

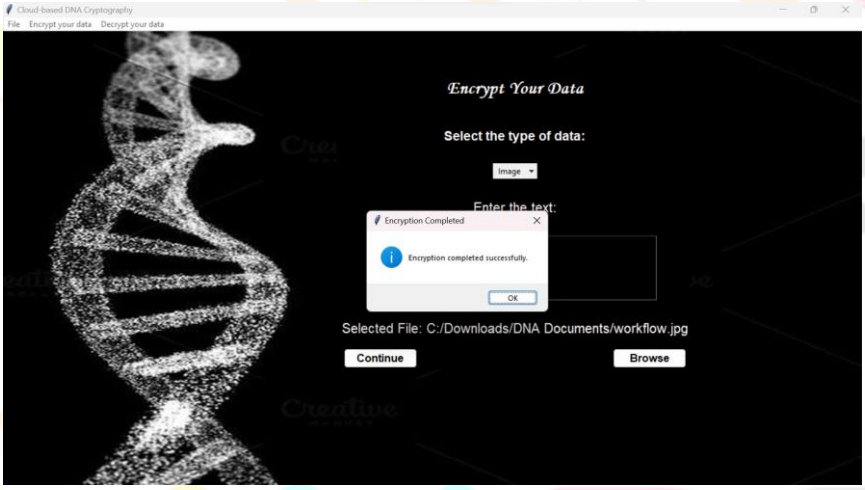

Fig. 5. Image Encryption

```
Signature: b'\x85\nq\xf5\x82\xe1W\xdcNZ=\x1e\xb7"\xa0\x1c[\x84\x9e\x8aG\x8a\xa4W[\nN_\xfc\x1f4\xd2jw\xf1;}\xd0\x0cp\\\xa3
\x7f\x15vzR\xe3qG\xd4\x90T%\xf6\x97\x1edw3A\xc3t}A3c\xda\xbd;\x1f\xadS\x82\x8b0\xa9\x07t\xff\xfb\xde\'[\xce^z\x11\xdc\x17
S\x13{\xf2`\x18&\xe6\x9d\xb7\x9fJ\xadQ\xe2\xb1\xfbp\x93I\xae\x0f\xac\xb2K\xc7\xad"]Z\xd6Y)^s\x82\xaa\xfa\xd4\xf0p\xb8\xd0
\xb1\xf9\x96G\x10\xa1\x1a\x84\x0cL\xcc\xbcF(\x9e\xee&\xf5\xbbm\x88}b\x89$`\xe4\x13\x08e\xef\xd4ew;O*I\xc8E&\xbda\x8e\xb2&
\x8cO\x88La>\xf6\xca\xea\n\r4\xc5x\xba\xe6W\x11\xae\x85\xebh\xd8\xa7\xcc\xc7\xaa\x89!Y\x9f\x94dt\xee\xae{U\x80`\xa6\xdb\x
e9\x89%\x04\x17\x18\x1e\xfa6\x9f\x9e#]\xee;\x8b\xd4\xb3\x04\xb0\x05\xa3P#\xa2\xc3\x07M\x17\x13\xb2\x9e\xdd\t\x8b'
Encryption completed successfully.
File workflow.jpg uploaded to S3 bucket
File signature.pem uploaded to S3 bucket
File public_key.pem uploaded to S3 bucket
File graphical_password.txt uploaded to S3 bucket
```

Fig. 6. Digital Signature and Cloud Upload

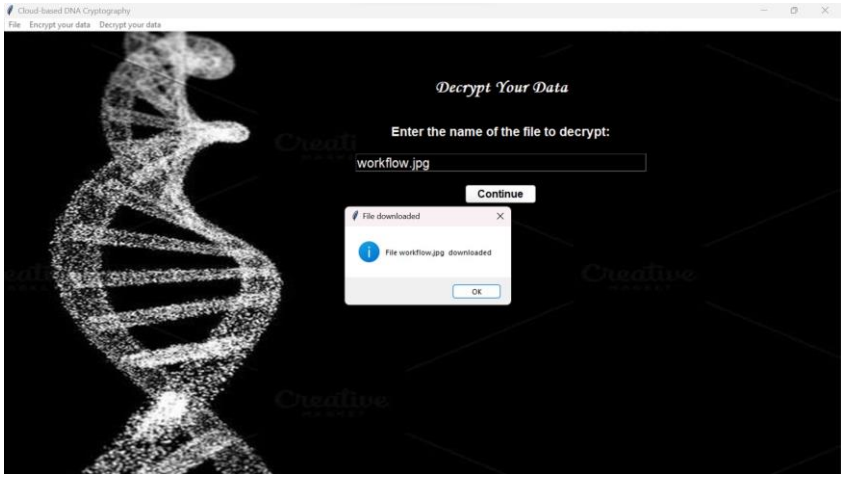

Fig. 7. Download image to be decrypted

Fig. 8. Graphical Password Authentication

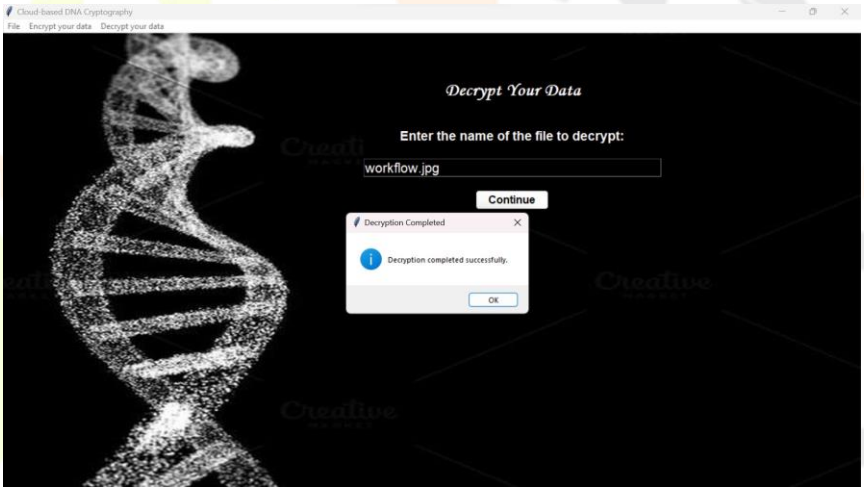

Fig. 9. Image Decryption

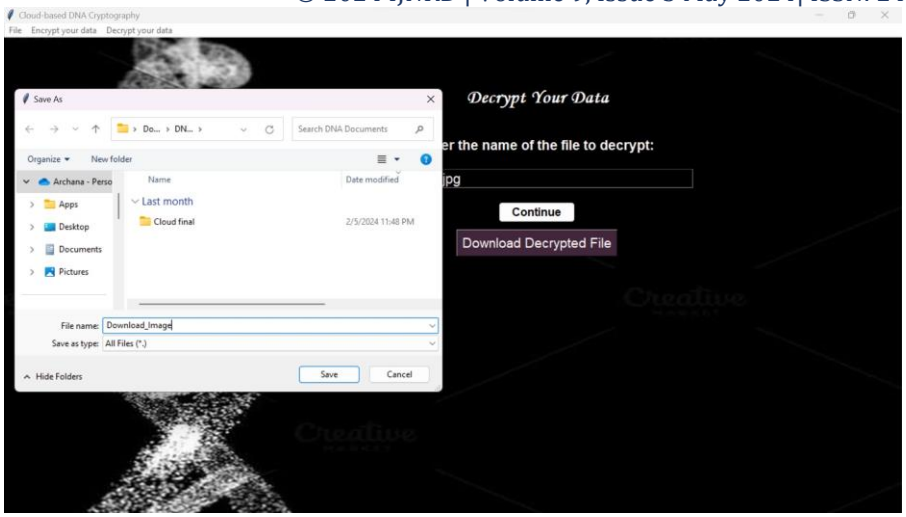

Fig. 10. Download and Save the Decrypted file

VI. CONCLUSION

This study introduces a novel cloud-based DNA cryptography system designed to enhance data security in cloud environments. The cryptographic model, inspired by the complex structure of DNA, exhibits high security and performance.Acknowledged limitations involve the simulation's inabilityto fully replicate real-world cloud complexities, reliance on pseudo-random number generators for DNA sequence generation, and the absence of exploration into ethical and privacy concerns. Future work is outlined, including enhancing error correction mechanisms, integrating with blockchain, applying machine learning optimizations, and addressing ethical and legal frameworks. The study emphasizes the need for energy efficiency studies, advanced steganography techniques, andreal-world deployment testing. In conclusion, the research contributes significantly to cloud security, laying the groundwork for future interdisciplinary studies to further develop the promising fusion of DNA cryptography and cloud computing.

REFERENCES

[1] Prasanna Balaji Narasingapuram, M. Ponnavaikko, "DNA Cryptography Based User Level Security for Cloud Computing and Applications," 2020.
[2] Sushma N K, Dr. Ravikumar G, Ms. Sindhu, "Distributed Computing of DNA Cryptography and Randomly Generated Mealy Machine," 2022.
[3] Abhay Kumar, Manmohan Singh, "Implementation Of Two-Fold DNA Cryptography Based On Amino Acid Table In Cloud Computing And Using Socket Programming," 2022.
[4] Poojashree Kamble, Firoz Nagarchi, Akshata Akkole, Vanishree Khanapur, Bahubali Akiwate, "A Dynamic DNA Cryptography Using RSA Algorithm and OTP," 2020.
[5] Vinay SH, Akshay Kedlaya, Adarsh Pujar, Vasudev Shahapur, "DNA Cryptography based on Dynamic DNA Sequence Table using Cloud Computing," 2019.
[6] Hamza Hammami, Hanen Brahmi, Sadok Ben Yahia, "Secured Outsourcing Towards a Cloud Computing Environment Based on DNA Cryptography," 2018.