INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Ensuring Authentic Access in Cloud Computing: Introducing DNA-Based Encrypted Data Authentication (DEDA)

J Vinnarasi[1]*, D I George Amalarethinam[2]

1 Research Scholar, PG and Research Department of Computer Science, Jamal Mohamed College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, 620020, Tamil Nadu, India
2 Principal and Head, Associate Professor, PG and Research Department of Computer Science, Jamal Mohamed College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, 620020, Tamil Nadu, India

OPEN ACCESS

Received: 25/08/2025
Accepted: 14/10/2025
Published: 29/10/2025

Citation: Vinnarasi J, George Amalarethinam DI (2025) Ensuring Authentic Access in Cloud Computing: Introducing DNA-Based Encrypted Data Authentication (DEDA). Indian Journal of Science and Technology 18(39): 3159-3169. https://doi.org/10.17485/IJST/v18i39.1483

* **Corresponding author**.

j.vinnarasicharles@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: To develop a secure authentication framework for accessing encrypted cloud data. This study introduces an effective and secure authentication structure for accessing data in cloud using DNA based methodology**.** **Methods:** This study employs DNA computing to generate an encrypted password and a secret key derived from the DNA bases: Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). We have utilized an encrypt based data upload by users in Amazon S3. The execution time (key generation, encryption, decryption, authentication and data access time) was used for performance comparison. The proposed approach reduces execution time by more than 25% compared to DNACDS and DNASK methods. **Findings:** The approach significantly enhances barriers to unauthorized data access while safeguarding user privacy. The experimental findings demonstrate the superiority of the proposed strategy over other established methods in the cloud computing environment. The suggested method reduces encryption time by 32.12% and 45.64%, authentication time by 27.63% and 52.38% for DNACDS and DNASK approach. **Novelty:** This study proposes DNA-based encrypted data authentication (DEDA) to ensure authentic access to cloud data. The novelty of this work lies in generating encrypted user passwords and keys via DNA computing, utilizing ASCII values, DNA sequences, binary operations, and XOR operations, thereby enhancing the system's defense against various security threats.

Keywords: Cloud Computing; Data Storage; Security; DNA Computing; Authentication; Encrypted Data; Access Control

1 Introduction

The primary attributes of the cloud encompass scalability, reliability, and availability; nevertheless, information security, privacy, and compliance represent significant concerns that hinder organizational migration to the cloud, particularly for those managing sensitive data[(1)]. Security is a vital concern in the cloud, and numerous

countermeasures, including cryptographic solutions, have been presented to date. Nonetheless, there remains a need for innovative and economical methods to counteract the assaults. Risks to data confidentiality have been highlighted due to the multi-tenant nature of cloud platforms [2]. Data leaks during transmission have been considered a significant threat, especially when information is exchanged over insecure channels. Additionally, weak authentication methods have been pointed out as a factor contributing to unauthorized access. Furthermore, threats to data integrity have been addressed, as stored information may be altered or tampered with by malicious actors. To overcome these concerns, efforts have been directed towards developing novel cryptographic solutions. Specifically, the security flaws in handling multi-user environments and protecting data during transmission and storage have been actively addressed through improved algorithmic designs [3].

Traditional cryptographic algorithms are insufficient for dealing with modern attacks, highlighting the need for novel and secure technology. DNA computing methods can be utilized for safeguarding data in cloud environments due to their bio-computational intricacy and potential integration with traditional encryption methods. DNA cryptography is a method that encodes information utilizing DNA sequences. This technique transforms each letter of the data into a unique configuration of the bases Cytosine (C), Adenine (A), Thymine (T), and Guanine (G) depicted as groupings of 0's and 1's. The encryption is rendered unbreakable and robust due to these four principles [4]. DNA computing provides superior performance and storage compared to conventional cryptography algorithms.

Recently, there has been an increasing interest in employing DNA computing for safeguarding data in cloud computing environments. Many researchers have proposed diverse methodologies employing DNA computing to tackle security-related challenges, such as the authentication process, the use of encryption, and decryption. Reddy et al. [5] introduced a bio-inspired cryptosystem that employs DNA computing for generating keys, data encryption and decryption. Encryption and decryption are executed using the Central Dogma of Molecular Biology. This system does not facilitate rapid data retrieval.

Thabit et al. [6] devised a cryptographic method incorporating dual layers to augment cloud computing security. The foundational layer was shaped by Shannon's theory of diffusion and confusion. The design of genetic coding for cryptographic functions impacted the subsequent layer. A substantial amount of time is necessary for the computation. Pavithran et al. [7] introduce an innovative cryptosystem founded in the cryptography of DNA and the finite theory of automata. The sender generates a 256-bit DNA-derived secret key based on the receiver's attributes, which is employed for encrypting data. A randomly generated Mealy machine is utilized to encode the DNA sequence, thereby augmenting the security of the ciphertext.

Sohal et al. [8] presented an innovative cryptographic method utilizing binary DNA, which employs on the client side information encryption to secure data prior to its upload to the cloud. It is a multifaceted symmetric-key encryption technique based on DNA cryptography. It obtained better throughput, but it takes a high execution time. Namasudra [9] designed a unique cryptosystem utilizing DNA cryptography and steganography for a cloud-based IoT framework. A complex and confidential key is employed to encrypt essential information. Encrypted information was embedded within an image. It obfuscates and encrypts data prior to transferring it to the cloud. The method has high time complexity and security issues.

Kumar et al. [10] presented a novel methodology utilizing DNA computing to improve data security in cloud-based computing environments. The 512-bit DNA-derived key is generated by the data individuals and utilized for the encryption of information before being outsourced to the cloud server. It is confined to guaranteeing data security and does not encompass other facets of effective access control. It employs many encoding protocols and procedures that elevate computational complexity. Gadde et al. [11] formulated an integrated cryptography-based authentication and authorization mechanism for secure and efficient cloud information storage. It provides distinct data access and storage for healthcare data on an online platform. A DNA-based technique is employed to produce keys, from which the optimal key is picked using an optimization algorithm.

Selvakumar et al. [12] presented a cryptographic algorithm that employs Huffman coding and DNA cryptography to ensure the secure transmission of confidential medical data. This method seeks to generate a cipher output that complicates an attacker's ability to deduce the key and input data. The maintenance and analysis of the code are more complex due to the inadequate structure of the Huffman tree. Singh et al. [13] presented a cryptographic method based on DNA and an access control paradigm. A data encryption technique is proposed to ensure the safeguarding of information against various attacks and hazards. An effective access control method ensures that only those with permission are granted access to the encrypted data. This method involves more intricate processes and has elevated temporal complexity for the security algorithm. Pavithran et al. [14] offer an innovative cryptosystem utilizing DNA cryptography and finite state machines. A DNA character conversion table is proposed to enhance the randomness of the ciphertext. It is more secure and can endure more rigorous assaults. The primary shortcoming of this study is the omission of user authentication and fine-grained access control. Table 1 shows the summary of existing literature.

Most of the prior research exhibits significant time consumption, computational complexity, and security concerns. Security concerns in cloud computing impede the storage of sensitive data. The conventional access control models are insufficient for the complexities of cloud environments. The previous research has also data integrity and unauthorized access issues. To

Table 1. Summary of Existing Literature

Ref	Methodology	Contributions	Limitations/ Research Gap
[5]	Central Dogma of Molecular Biology, Bidirectional Associative Memory Neural Network, and Whale Optimization Algorithm.	A bio-inspired cryptographic DNA system comprising encryption, key generation, and decryption stages that augments data security. WOA is utilized to enhance the cryptography procedure.	The system's scalability in managing exceptionally big datasets is not addressed, which is essential for its usefulness in high-demand scenarios.
[6]	Dual layers of encryption: logical processes and genetic frameworks.	An innovative data security algorithm for cloud computing utilizing dual levels of encryption. The initial layer employs logical processes derived from Shannon's theory, but the subsequent layer integrates genetic methodologies grounded in the Central Dogma of Molecular Biology.	The computational burden brought about by the new cryptographic algorithms, which may affect performance in real-time applications, is not sufficiently discussed.
[7]	A unique cryptographic system utilizing DNA cryptography and finite automata theory.	DNA algorithm, a secret key derived from 256 bits of DNA and characteristics, key pair generator, dynamic random Mealy machine, and transition tables.	The scheme's security cannot be mathematically demonstrated.
[8]	BDNA algorithm, client-side data encryption, symmetric key cryptography	It employs client-side data encryption to secure the data prior to its upload to the cloud. It is a multifaceted symmetric-key cryptography method grounded in DNA cryptography.	It achieved superior throughput; however, it requires a prolonged execution time.
[9]	DNA cryptography and steganography	It integrates the encrypted data into a cover image as an extended DNA sequence before uploading it to the cloud server.	The approach exhibits significant time complexity and security vulnerabilities.
[10]	DNA based cryptography	A DNA-based data encryption method that use complimentary principles and encoding tables to create a secret key for data encryption and decryption. It employs ECC-based operations.	It is confined to guaranteeing data security within a cloud environment and does not encompass other facets of effective access control.
[11]	Improved Robust S-box-based AES, Modified ECC	A hybrid cryptographic security framework that markedly improves the safeguarding and segregation of medical data in the cloud, providing enhanced performance and addressing essential privacy issues associated with cloud-based healthcare data storage.	The intricacy of secure key generation, distribution, storage, rotation, and revocation is a considerable problem, particularly in a distributed cloud system with numerous users and varying access levels.
[12]	DNA cryptography, Huffman coding	Cryptographic algorithm employing DNA cryptography and Huffman coding to guarantee secure transmission of healthcare digital data on the cloud.	Assessment of cryptographic specifications and keyspace analysis.
[13]	DNA cryptography and access control model	A data encryption method is proposed to protect information from diverse attacks and threats. An efficient access control mechanism guarantees that only authorized individuals are permitted access to the encrypted data.	This strategy entails more complex processes and has increased temporal complexity for the security algorithm.
[14]	DNA cryptography and finite state machine	DNA character translation table to enhance the randomness of the ciphertext.	Authentication and access control are not considered.

overcome these issues, this work presents an efficient and safe authentication strategy for accessing encrypted data in the cloud with a DNA-based approach. This research utilizes DNA computing to produce encrypted passwords and secret keys using the DNA sets: Cytosine (C), Adenine (A), Guanine (G), and Thymine (T). This work generates encrypted user passwords and keys through DNA computing, ASCII values, DNA sequences, binary operations, and XOR operations to bolster the system's resistance against diverse security threats.

This study's main contributions can be summarized as follows:

- A DNA-based authentication scheme is proposed for accessing the encrypted data in the Cloud.
- This study introduces a technique for generating user passwords and secret keys based on DNA computing.
- This work employs a three-layered strategy to enhance data security and provide safe storage of data in the cloud environment.
- This study provides a security analysis and empirical results to illustrate its superiority compared to existing methodologies. The DNA-based authentication and key generation technology may withstand numerous security assaults.
- The experimental results of the proposed algorithm validate its efficacy with other authentication and encryption techniques.

The subsequent sections of the research article are structured as follows: Section 2 elucidates the suggested DNA-based authentication method for accessing encrypted data. Section 3 evaluates the efficacy of the proposed method. Section 4 concludes the research paper, and finally, Section 5 outlines the limitations and prospective directions for further work.

2 Methodology

This section explains an efficient, secure authentication scheme for accessing encrypted data in the cloud using a DNA-based approach. This research introduces DNA-based encrypted data authentication (DEDA) to guarantee legitimate access to cloud data. This study innovatively generates encrypted user passwords and keys by DNA computing, employing ASCII values, DNA sequences, binary operations, and XOR operations, thereby fortifying the system's protection against diverse security threats.

The proposed approach contains three entities: Cloud Server, Data Owner, and Data User. The Cloud Server serves as the primary administrator, facilitating infrastructure and other cloud services through a multitude of powerful machines with ample memory capacity. It comprises a cloud storage system where user data is saved in an encrypted fashion. The data proprietor publishes encrypted data to the cloud through the cloud interface. The secured file is retrieved from the cloud and provided to the requesting user. The data owner is a distinct type of user within a cloud environment. The data proprietor uploads the encrypted file to the cloud server. The authorized data user is able to access the encrypted file. Figure 1 illustrates the recommended system model.

The suggested approach contains three phases: Authentication, Data Encryption, and Data Access with Decryption.

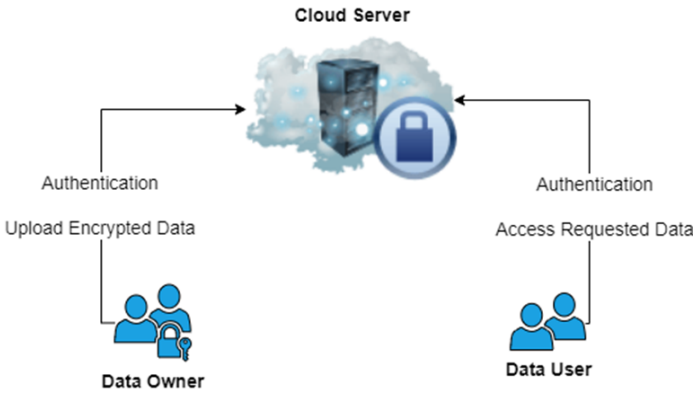

Fig 1. General System Model

2.1 Authentication

Authentication acts as the safeguard of a system, validating user identities and permitting access to legitimate persons or entities. It protects against illicit use and other security threats while ensuring that those who have permission are granted access to the services. In this paper, DNA-based cryptography is applied for secure authentication. In a DNA-based cryptography system, information is encoded utilizing DNA terminology: A (Adenine), G (Guanine), C (Cytosine), and T (Thymine). Table 2 shows the binary code for DNA.

Table 2. Binary Code for DNA base

DNA Symbol	Binary Value
A	00
C	01
G	10
T	11

DNA computing involves the utilization of diverse biological and algebraic operations on DNA sequences, such as addition, XOR, and subtraction operations on DNA-encoded sequences. This paper uses XoR operation to encode the DNA sequence. Table 3 shows the XoR operation of the DNA base.

Table 3. DNA XoR Operation

XoR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

Algorithm 1 explains the user registration process. The user password is encrypted using a DNA sequence and stored in the cloud for further processing.

Algorithm-1: User Registration
Input: User Name, Password
Output: Encrypted DNA Password
Step 1: Get User Name and Password
Step 2: Divide the Password into characters
Step 3: Each character is converted into the corresponding ASCII value
Step 4: The ASCII value is transformed into a binary representation
Step 5: Consolidate every binary number into one format
Step 6: 2-bit binary values are created by dividing the entire binary number
Step 7: Generate DNA sequences based on the 2-bit binary value
Step 8: Apply XoR operation to get the encrypted DNA Password

Figure 2 illustrates the workflow for generating encrypted passwords.

Initially, the user password is divided into a number of characters and converted into an ASCII value. For example, password = 'vincy'. The ASCII value of the password is v = 118, i = 105, n = 110, c = 99, y = 121. The ASCII values are transformed into an 8-bit binary representation. v = 01110110, i = 01101001, n = 01101110, c = 01100011 and y = 01111001. Combine all the binary numbers into one format: v + i + n + c + y = 0111011001101001011011100110001101111001. Create a 2-bit binary value 01 11 01 10 01 10 10 01 01 10 11 10 01 10 00 11 01 11 10 01. The pair of binary numbers is correlated with the DNA sequence according to the DNA-based presentation in Table 2. The transformed DNA sequence is- CTCGCGGCCGTGCGATCTGC. Finally, apply the XoR operation on the DNA sequence to get the encrypted password ACGTGGAATC. Figure 3 illustrates the process of generating a DNA-encrypted password using the XOR operation. The XOR operation is applied based on the position of the bits in a binary number. The encrypted password is stored in the cloud.

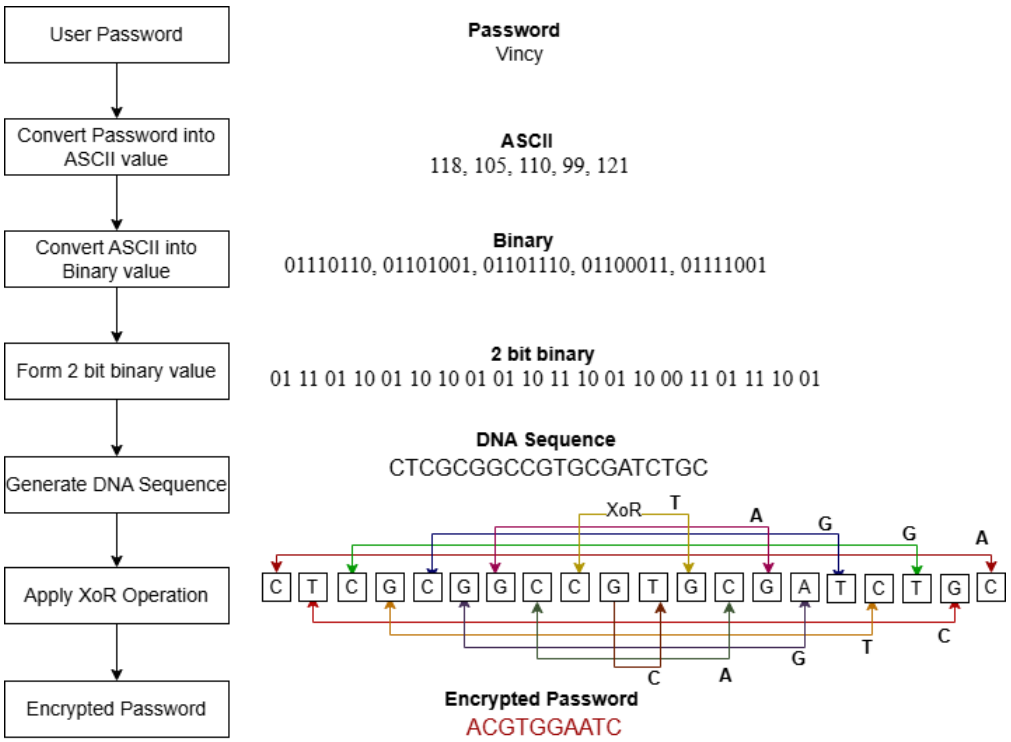

Fig 2. Flow diagram of Encrypted Password Generation

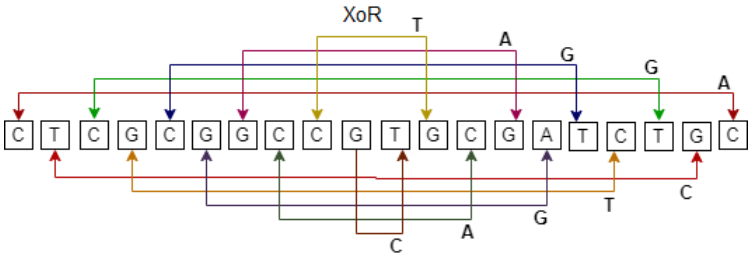

Fig 3. DNA encrypted password

2.2 Data Encryption

This approach entails customer-side encryption, whereby the data owners protect the data before delivering it to the cloud. The supplier of cloud services does not have access to the original data. Even if the malicious person has access to the cloud data, they would be unable to retrieve the original, unencrypted information. The procedure of encryption has multiple stages, including message division, square matrix generation, scrambling, and binary logical operation. The encryption technique first partitions the input file into shares, transforms each share into ASCII format, and subsequently generates a square matrix for each share. Scramble the square matrix and convert the scrambled matrix into binary form; each binary bit is transformed into its one's complement. Generate the binary key, apply the logical XOR operation to convert binary data into character format, and thereafter amalgamate each share of character data into a unified ciphertext format. The detailed description of the algorithm is explained in [15]. The DNA key is generated as follows: consider the binary key = '0111111' and find the 1's complement 1000000. Combine each binary value (01111111000000) and create the DNA key (CTTTAAA) using Table 2. The DNA key and the encrypted message are stored in the cloud. The hash value for the encrypted message was generated using a Secure Hash Algorithm (SHA), and it is stored on the local machine. The SHA can be used for checking the integrity of data [16].

2.3 Data Access and Decryption

The software assumes that the client has been authenticated using the cloud platform during this procedure. The user seeks access to the cloud server. The server authenticates the user's authorization and additional rights. Following the successful verification of the user request, the data must be provided. The whole approach must adhere to the subsequent procedures to get data from the cloud.

Step 1: The users register on the cloud server through registration requests.

Step 2: The cloud server consolidates the users' information and details. Subsequently, the server transmits a registration confirmation to the user, accompanied by the encrypted DNA key, contingent upon the successful completion of the registration process.

Step 3: The user submits the data access request to the cloud.

Step 4: The server verifies the user's request upon successful validation and authentication.

Step 5: The encrypted DNA key and the encrypted message are transmitted to the user.

Step 6: The user decodes the key and encrypted message.

Data received from the cloud is in an encrypted form, which requires decryption. To decrypt, the user acquires the DNA key and submits the share number. The decryption procedure is the exact opposite of encryption. **Algorithm 2** delineates the decryption procedure.

Algorithm 2: Decryption Process
Input: Encrypted DNA Key (EncKey), Encrypted Message (EncMsg)
Output: Decrypted Message
Step 1: Convert DNA Key sequences into binary numbers based on Table 2
Step 2: Divide the binary number into two parts
Step 3: Use the first part as a decryption key (binkey)
Step 4: Generate a square matrix
Step 5: Convert EncMsg into a binary value
Step 6: Apply the XOR operation for each element in the square matrix with the binary key
Step 7: Find the 1's complement
Step 8: Convert the binary value into a decimal value
Step 9: Descramble the square matrix elements
Step 10: Find the corresponding character of the ASCII value
Step 11: Read row by row the component of the square matrix to get the decrypted message

For example, consider the encrypted message shared in[15] EncMsg = '%'%3#249. Initially, the encrypted DNA key (CTTTAAA) is decrypted into a binary key (0111111). Generate the square matrix for the encrypted message.

$$\begin{bmatrix} ' & \% & ' \\ \% & 3 & \# \\ 2 & 4 & 9 \end{bmatrix}$$

The encrypted message is transformed into an ASCII value, which is subsequently reverted to a binary value.

$$\begin{bmatrix} 96 & 37 & 96 \\ 37 & 51 & 35 \\ 50 & 52 & 57 \end{bmatrix} = \begin{bmatrix} 1100000 & 0100101 & 1100000 \\ 0100101 & 0110011 & 0100011 \\ 0110010 & 0110100 & 0111001 \end{bmatrix}$$

Apply the XOR operation for each element in a square matrix with binary values and find the 1's complement.

$$\begin{bmatrix} 1011111 & 0011010 & 1011111 \\ 0011010 & 0001100 & 0011100 \\ 0001101 & 0001011 & 0000110 \end{bmatrix} = \begin{bmatrix} 0100000 & 1100101 & 0100000 \\ 1100101 & 1110011 & 1100011 \\ 1110010 & 1110100 & 1111001 \end{bmatrix}$$

Convert the binary value into a decimal value and descramble the square matrix elements

$$\begin{bmatrix} 32 & 101 & 32 \\ 101 & 115 & 99 \\ 114 & 116 & 121 \end{bmatrix} = \begin{bmatrix} 121 & 32 & 115 \\ 101 & 99 & 114 \\ 101 & 116 & 32 \end{bmatrix}$$

Find the corresponding character of the ASCII value and read the row-by-row elements in the square matrix to get the decrypted message.

$$\begin{bmatrix} y & & s \\ e & c & r \\ e & t & \end{bmatrix} = \text{y secret}$$

Figure 4 shows the workflow process of the encryption and decryption of the proposed DEDA.

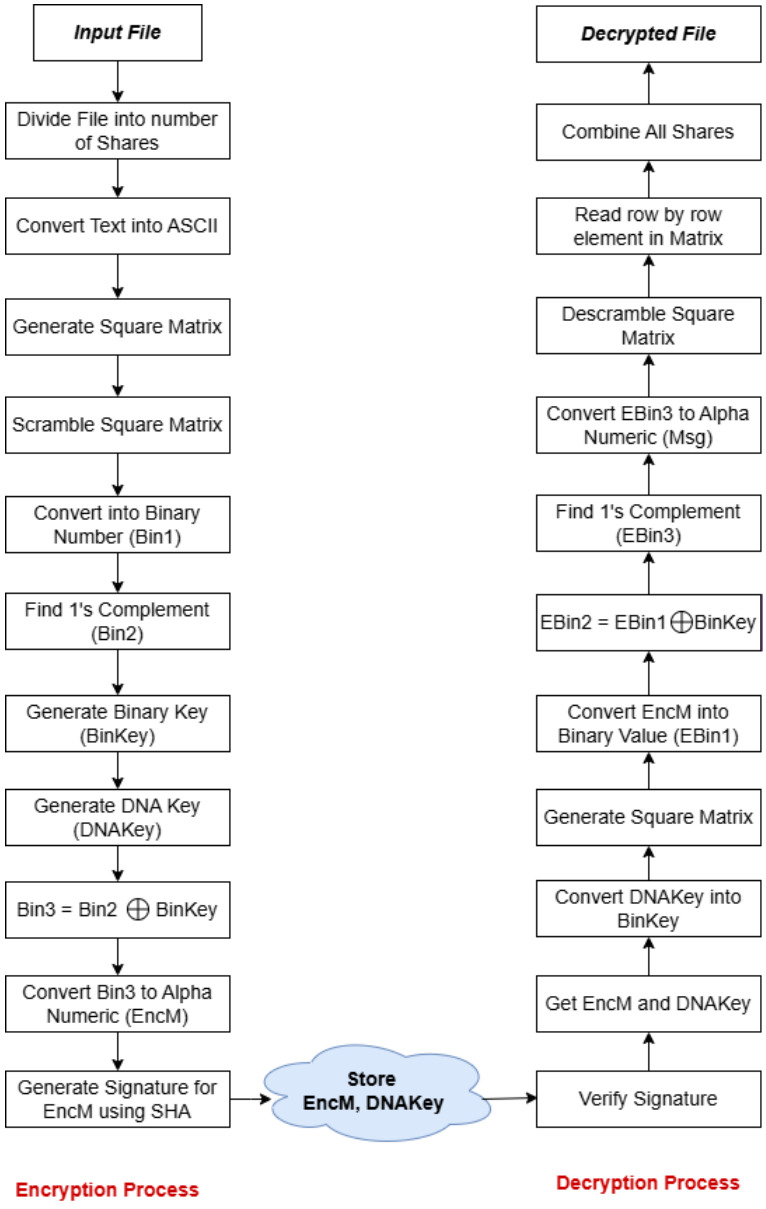

Fig 4. Encryption and Decryption Process of Proposed DEDA

3 Results and Discussion

This section examines the effectiveness of the proposed approach, considering implementation details, assessment metrics, comparative analysis, and security analysis. The proposed methods are implemented using Java (version JDK 8) and Amazon

S3 (Simple Storage Service) for storing encrypted data. A multitude of security investigations and studies were conducted to validate the proposed method. The resilience of the proposed coding scheme is assessed through key generation time, encryption time, decryption time, authentication time, and data access time.

The results gained are compared with other existing schemes and provide superior outcomes. The analogous existing schemes are: DNACDS[13] and DNASK[14]. The current DEDA approaches enhance the system's security through the use of the DNA methodology. Table 4 shows the comparison of all metrics.

Table 4. Metrics Comparison

Metrics	Methods		
	DNACDS[13]	DNASK[14]	DEDA
Key Generation Time (ms)	8.65	10.45	5.23
Encryption Time (ms)	3.58	4.47	2.43
Decryption Time (ms)	2.91	5.88	2.05
Authentication Time (ms)	1.52	2.31	1.10
Data Access Time (ms)	1.34	2.90	1.01

Figure 5 shows the performance comparison of DNACDS[13], DNASK[14], and the proposed DEDA approach. The proposed method requires 5.23 milliseconds for key generation, whereas the alternative methods necessitate 8.65 milliseconds for DNACDS[13] and 10.45 milliseconds for DNASK[14]. The results demonstrated that the proposed strategy requires less time than alternative approaches. The proposed method requires minimal computations to produce the key. The algorithm does not necessitate transmitting the key to external parties. The proposed approach reduces key generation time by 39.53% and 49.95% for DNACDS[13] and DNASK[14] approaches.

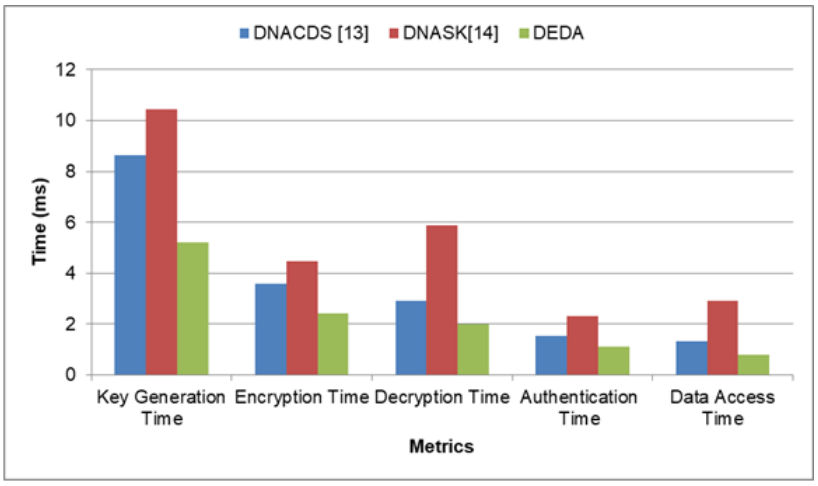

Fig 5. Performance Comparison

The proposed approach takes 2.43 ms for encryption. The proposed DEDA mainly used simple scrambling, binary and XoR operations. Thus, it required less time for encryption compared to other approaches. The proposed approach reduces encryption time by 32.12% and 45.64% for DNACDS[13] and DNASK[14] approaches. The proposed method takes 2.05ms for decryption. The proposed method necessitated simply XOR and basic operations, which used minimal time. The suggested method decreases decryption time by 29.55% for DNACDS[13] and 65.14% for DNASK[14].

The data access time delineates the intervals during which a user sends a query to the system and receives the results. This encompasses the total duration for processing the client request, generating the encrypted data, and transmitting it back to the user. The proposed approach takes 1.01ms for data access. The proposed approach reduces the data access time by 24.62% for DNACDS[13] and 65.17% for DNASK[14]. The efficacy of the suggested method is superior, since data encryption time, key generation time, and decryption time operate with reduced time requirements. The alternative system exhibits elevated key generation, data encryption, and decryption durations.

The proposed approach takes 1.10 ms for authentication. The proposed approach decreases the authentication time by 27.63% for DNACDS [13] and 52.38% for DNASK [14]. The evaluated schemes necessitated considerable time to verify authenticity due to the extensive computations involved in their execution. Consequently, the overall performance of the suggested work is superior and requires minimal time to handle user requests. Table 5 shows the time reduction (%) comparison.

Table 5. Comparison of Time Reduction (%)

Metrics	DNACDS [13]	DNASK [14]
Key Generation Time	39.53%	49.95%
Encryption Time	32.12%	45.64%
Decryption Time	29.55%	65.14%
Authentication Time	27.63%	52.38%
Data Access Time	24.62%	65.17%

The proposed approach can resist some security attacks including password guessing attack, ciphertext-only attack, and masquerade attack

In a password guessing attack, the adversary endeavors to ascertain the login credentials by systematically examining all conceivable password combinations. This study employs a DNA-based method to encrypt the user password and secret key. It is exceedingly challenging for attackers to ascertain all the confidential particulars of a user.

In a ciphertext-only attack, the assailant possesses the ciphertext and seeks to deduce the plaintext and the associated key. Consequently, deriving the plaintext and secret keys from the ciphertext pair is a challenging task. The suggested methodology takes into account a randomly produced DNA nucleotide. The encryption system employs scrambling and logical XOR operations. This induces confusion and dispersion within the system.

In a masquerade attack, unauthorized individuals employ false information or identities to gain illicit access. In the suggested methodology, all end users must register with the cloud server and log in to access any cloud service after completing the registration process. Consequently, unauthorized or malicious users are prohibited from accessing the server with a falsified identity and are unable to obtain any cloud services unless they successfully complete the login process.

4 Conclusion

This work presents an efficient and safe authentication strategy for accessing encrypted data in the cloud with a DNA-based approach. DNA cryptography offers numerous benefits compared to conventional cryptographic techniques, including resilience against potential computational attacks and enhanced encryption complexity. It can be utilized to protect governmental and corporate data within cloud infrastructures against illegal access and hacking efforts. However, it encounters constraints such as elevated computational complexity, dependence on biological processes ill-suited for digital contexts, and vulnerability to noise and attacks particular to DNA manipulation. The suggested work is confined to guaranteeing data security inside a cloud context and does not consider other facets of effective access management. This study utilizes DNA computing to generate encrypted passwords and secret keys derived from the four DNA bases. The suggested approach is safeguarded against specific security threats. The experimental results indicate that our proposed method surpasses alternative approaches for key generation, encryption, decryption, authentication, and data access time. The proposed approach reduces execution time more than 25% compared to DNASK and DNACDS methods.

The time-consuming nature of an encryption algorithm may be lowered in the future, particularly by minimizing intricate procedures. Alternative secret key generation methodologies predicated on user attributes can enhance the data security framework. A novel DNA security framework can be established for cloud computing to address a broader spectrum of security threats and assaults, hence enhancing cloud data security.

In authentication, the proposed approach uses only two attributes: username and password. In the future, multi-factor authentication with multiple user identity mechanisms will be used for secure authentication. Intricate mathematical functions can be employed to enhance the encryption and decryption procedures. Innovative machine-learning and deep-learning methodologies can be used alongside cryptography techniques to improve security and performance. Data integrity can be maintained by the utilization of powerful blockchain and hashing technology.

4.1 Contributory statement:

Formulation of the research problem, Algorithm & cryptographic method: J. Vinnarasi; Research Guidance: Dr. D. I. George Amalarethinam.

References

1) Qiqieh I, Alzubi J, Alzubi O. DNA cryptography based security framework for health-cloud data. *Computing*. 2025;107(35). https://doi.org/10.1007/s00607-024-01393-9.
2) Satheesh KK, Sree TK. Enhancing Cloud Security with Authentication for Securing Sensitive Information. *Pattern Recognition*. 2025;171. https://doi.org/10.1016/j.patcog.2025.112345.
3) Kairi A, Bhadra T, Pandey SK, Sinha A, Nag A. Adaptive DNA Cryptography With Intelligent Machine Learning for Cloud Data Defense. *Engineering Reports*. 2025;7(6). https://doi.org/10.1002/eng2.70223.
4) Kaur H, Jameel R, Alam MA, Alankar B, Chang V. Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography. *Journal of Enterprise Information Management*. 2023;36(4):861–878. https://doi.org/10.1108/JEIM-02-2021-0084.
5) Reddy MI, Kumar AS, Reddy KS. A secured cryptographic system based on DNA and a hybrid key generation approach. *Biosystems*. 2020;197. https://doi.org/10.1016/j.biosystems.2020.104207.
6) Thabit F, Alhomdy S, Jagtap S. A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. *International Journal of Intelligent Networks*. 2021;2:18–33. https://doi.org/10.1016/j.ijin.2021.03.001.
7) Pavithran P, Mathew S, Namasudra S, Lorenz P. A novel cryptosystem based on DNA cryptography and randomly generated mealy machine. *Computers & Security*. 2021;104. https://doi.org/10.1016/j.cose.2020.102160.
8) Sohal M, Sharma S. BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. *Journal of King Saud University-Computer and Information Sciences*. 2022;34(1):1417–1425. https://doi.org/10.1016/j.jksuci.2018.09.024.
9) Namasudra S. A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure. *Computers and Electrical Engineering*. 2022;104. https://doi.org/10.1016/j.compeleceng.2022.108426.
10) Kumar T, Namasudra S, Kumar P. Providing data security using DNA computing in the cloud computing environment. *International Journal of Web and Grid Services*. 2023;19(4):463–486. https://doi.org/10.1504/IJWGS.2023.135587.
11) Gadde S, Amutharaj J, Usha S. A security model to protect the isolation of medical data in the cloud using hybrid cryptography. *Journal of Information Security and Applications*. 2023;73. https://doi.org/10.1016/j.jisa.2022.103412.
12) Selvakumar K, Lokesh S. A cryptographic method to have a secure communication of health care digital data into the cloud. *Automatika*. 2024;65(1):373–386. https://doi.org/10.1080/00051144.2023.2301240.
13) Singh A, Kumar A, Namasudra S. DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography. *Frontiers of Computer Science*. 2024;18(1). https://doi.org/10.1007/s11704-022-2193-3.
14) Pavithran P, Mathew S, Namasudra S, Singh A. Enhancing randomness of the ciphertext generated by DNA-based cryptosystem and finite state machine. *Cluster computing*. 2023;26(2):1035–1051. https://doi.org/10.1007/s10586-022-03653-9.
15) Amalarethinam DG, Vinnarasi J. Enhancing the data security of cloud computing critical systems using layered encryption technique. *International Journal of Critical Computer-Based Systems*. 2024;11(3):194–215. https://doi.org/10.1504/IJCCBS.2024.143209.
16) Vinnarasi J, Amalarethinam DIG. Advancing Data Security in Cloud Computing: Introducing Secured Layered Technique for Data Security Approach (SLT-DSA), A Multi-Layered Security Framework. *Indian Journal of Science and Technology*. 2025;18(11):848–860. https://doi.org/10.17485/IJST/v18i11.273.