IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 6, June 2024

Impact Factor: 5.731

DNA as a Storage Medium for Efficient and Reliable Cloud Data Archieving

Sriram.S[1] and Dr. D. R. Krithika[2]

II MCA Student, Department of Computer Applications[1]

Assistant Professor, Department of Computer Applications[2]

22304240@vistas.ac.in and krithika.scs@velsuniv.ac.in

Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

Abstract: *On Earth right now, there are about 10 trillion gigabytes of digital data, and every day, humans produce emails, photos, tweets, and other digital files that add up to another 2.5 million gigabytes of data.Much of this data is stored in enormous facilities known as exabyte data centers (an exabyte is 1 billion gigabytes), which can be the size of several football fields and cost around $1 billion to build and maintain.Demand for data storage is growing exponentially, but the capacity of existing storage media is not keeping up.This project enables molecular-level data storage into DNA molecules by leveraging biotechnology advances in synthesizing, manipulating and sequencing DNA to develop archival storage. Additionally an effective algorithm is introduced using deoxyribonucleic acid (DNA)-based cryptography to enhance data security while sharing the data over the cloud*

Keywords: DNA (Deoxyribonucleic Acid)

I. INTRODUCTION

The global data burden is increasing every day and data storage companies have to invest millions of dollar for new storage facilities each year.DNA will be the next big thing for digital data storage in the future. DNA is a future of data storage technology.DNA storage technology is a new data storage technology through DNA storage medium, which can achieve digital data storage (text, image, audio, video, etc.) by encoding and decoding for the synthesized DNAs with specific sequences based on certain encoding/decoding methods.DNA storage technology is a new data storage technology through DNA storage medium, which can achieve digital data storage (text, image, audio, video, etc.) by encoding and decoding for the synthesized DNAs with specific sequences based on certain encoding/decoding methods.Cloud computing is the on-demand, pay-as-you-go service may rent computing power, storage, and databases from a cloud provider like Amazon Web Services on an as-needed basis (AWS). The term "cloud" simply refers to the internet distribution model over the Internet. Instead of purchasing, operating, and maintaining physical data centres and servers, you. Computing is the architecture and techniques that allow a computer to execute, create, distribute, and interact with data. This means that, rather than hosting infrastructure, systems, or programs on your hard drive or on an on-site server, you host them on virtual/online servers that connect to your computer via secure networks.Cloud computing allows users to access online services as long as there is an available internet connection. The user does not need to be physically present in a specific location or own a costly infrastructure to keep files. Rather than holding a proprietary hard drive or local storage, cloud-based storage saves the company a remote database.

II. LITERATURE SURVEY

The paper addresses the challenges and opportunities of DNA-based data storage. Traditional storage mediums may not keep pace with the increasing demand for long-term, high-density, and durable data storage solutions [1]. The paper addresses the problem of scalability and security in cloud data storage systems. As the volume of data stored in the cloud continues to grow exponentially, there is a need for efficient and secure storage solutions that can handle the increasing demands [2]. The paper addresses the problem of achieving fine-grained access control in cloud data

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

storage systems. Traditional access control mechanisms often lack the flexibility to provide granular control over data access, which can lead to security and privacy concerns [3]. The paper addresses the problem of efficient and verifiable cloud data storage. Traditional encryption schemes often hinder data processing operations, such as search or computation, requiring data to be decrypted before performing operations. Additionally, ensuring the integrity of data stored in the cloud can be challenging [4]. The paper addresses the problem of preserving privacy in cloud data storage systems. Traditional approaches may not adequately protect sensitive data from unauthorized access or inference, leading to privacy breaches [5]. The paper addresses the problem of secure data storage and access control in cloud environments. Traditional access control mechanisms may not provide sufficient security assurances, and data breaches can occur due to centralized storage systems [6]. The paper addresses the problem of efficient and scalable data storage with dynamic access control in cloud environments. Traditional access control mechanisms may not easily accommodate changes in access permissions, leading to inefficiencies and limitations in managing data access [7]. The paper addresses the problem of efficient and scalable data storage with dynamic access control in cloud environments. Traditional access control mechanisms may not easily accommodate changes in access permissions, leading to inefficiencies and limitations in managing data access [8]. The paper addresses the problem of secure data sharing in cloud storage environments. Traditional approaches to data sharing may not adequately protect the privacy and confidentiality of shared data, leading to concerns about unauthorized access or data leakage [9]. The paper addresses the problem of data deduplication in cloud storage systems. Data deduplication is a technique used to eliminate redundant copies of data and reduce storage requirements. However, ensuring the integrity and authenticity of deduplicated data can be challenging [10].

III. IMPLEMENTATION WORK

SCREEN LAYOUTS:

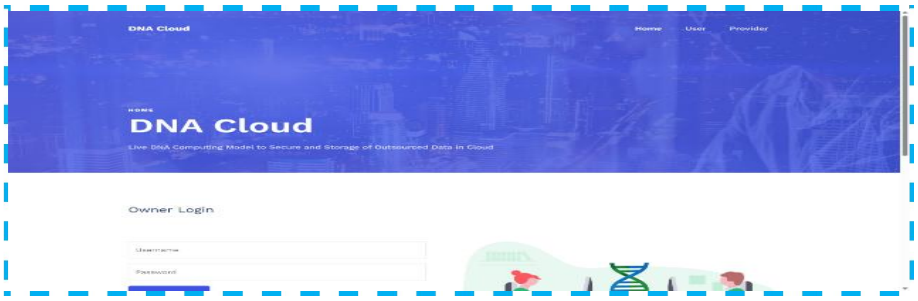

Fig.1:OWNER LOGIN:

description: In this fig1 we need to enter the owner username and password and then need to login.

Fig.2: OWNER REGISTRATION:

description:In this fig.2,the next step if not a owner exist or need to create a new owner then we need toregister for the owner

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

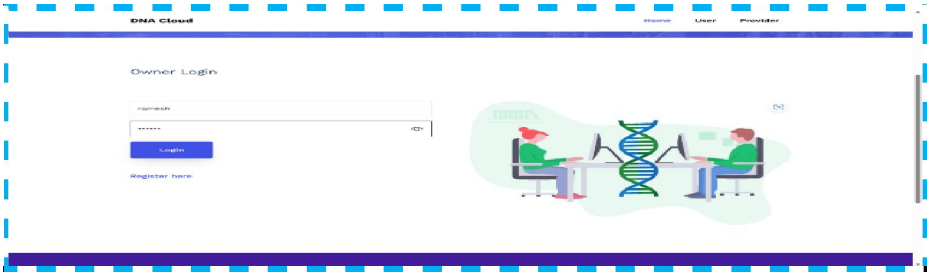

Fig.3 OWNER LOGIN (2):

description: In this fig.3, After registering the owner details then need to login.

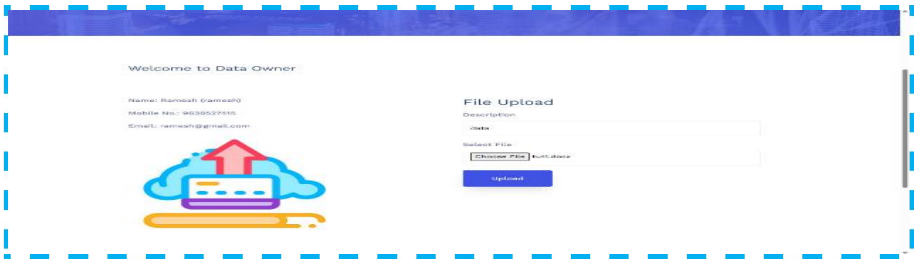

Fig.4FILE UPLOAD:

description: In this fig.4, The next step we need to upload the file which we are going to compress and share.

Fig.5ASCII CONVERTION:

description: In this fig.5, After uploading the file, it will convert the file in first step into ASCII value

Fig.6 BINARY CONVERTION:

description: In this fig.6, Then it will convert to binary code as the next step.

Fig.7DNA CODE:

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

description: In this fig.7, Then it will substitute the DNA code

Fig.8 ENCRYPTION ID:

description: In this fig.8, We need to enter the public key by accessing the database.

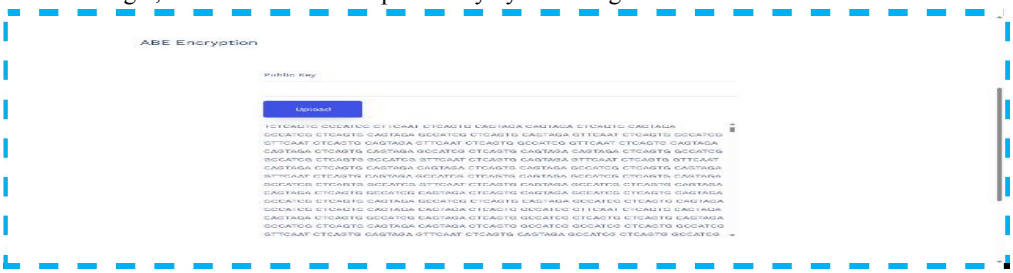

Fig.9 ABE ENCRYPTION:

description: In this fig.9, After, it will encrypt it.

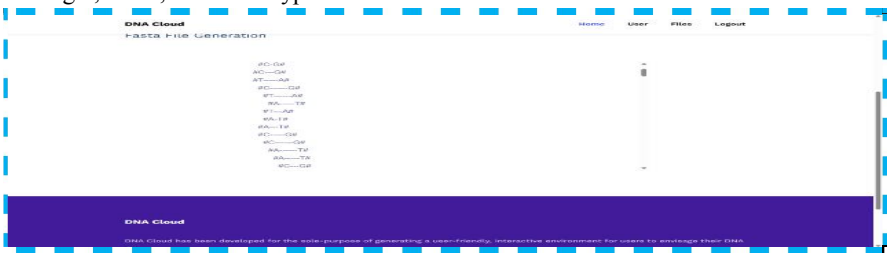

Fig.10 FASTA-FILE GENERATOR:

description: In this fig.10, Then, the next step it will converts it into Fasta file generator.

Fig.11 ACCESSING FILE:

description: In this fig.11, It will compress the file then we can to access and share

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

Fig.12 ADD USER:

description: In this fig.12, Then, the next step we need to enter the receiver's details in the add user.

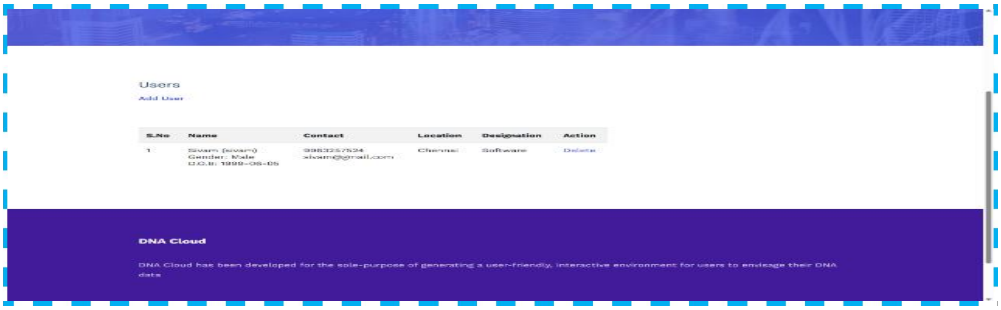

Fig.13 USER ADDED:

description: In this fig.13, Then it will adds the user's address in the add user.

Fig.14 SHARING FILE:

description: In this fig.14, We can share the details to the user's address.

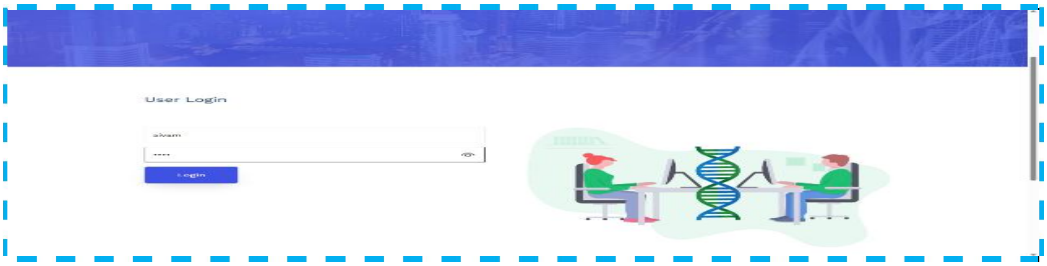

Fig.15 USER LOGIN:

description: In this fig.15, Then, the user will login with his/her details

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

Fig.16 DOWNLOADING FILE:

description: In this fig.16, After logging, the user can access the file.

Fig.17 DECRYPTING FILE:

description: In this fig.17, Then it will decrypt it in the reverse order.

Fig.18 DECRYPTION ID:

description: In this fig.18, Then, the user need to enter the public key.

Fig.19 RECOVERY ALGORITHM:

description: In this fig.19, It will convert it and encrypt the data

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

Fig.20 DNA CODE (2):

description: In this fig.20, Then, it will convert it into DNA code.

Fig.21 BINARY CONVERTION (2):

description: In this fig.21, Then, it will convert the file into binary.

Fig.22 ASCII CONVERTION (3):

description: In this fig.22, It will convert it into ASCII value.

Fig.23 USER FILE ACCESS:

description: In this fig.23, Then, the user can download the compressed file and can access the file.

IV. CONCLUSION

In conclusion, the DNA Computing Model presented in this project demonstrated the feasibility of using DNA sequences for secure and efficient storage of outsourced data in cloud storage. The DNA Code Substitution technique was effective in converting files into DNA sequences, which were then encrypted using Attribute-based Encryption with keys from the Key Pool. The DNA Recovery Algorithm successfully decrypted the DNA sequences and recovered the original file format. The DNA Attribute-based Decryption was also effective in decrypting the

encrypted DNA sequences. The test results showed that the DNA Computing Model performed efficiently and effectively, with acceptable processing times for file conversion, encryption, and decryption. The security analysis indicated that the DNA-encrypted files were highly secure and resistant to attacks due to the complexity of DNA sequences and the use of Attribute-based Encryption. The results of this project suggest that DNA Computing can be a viable approach for secure and efficient storage of outsourced data in cloud storage, and further research can explore the potential of this technology in real-world scenarios.In conclusion, the DNA computing model for secure cloud storage of outsourced data has great potential for future development and implementation in real-world scenarios. The DNA-based approach offers a new paradigm for data storage, security, and privacy, and we are optimistic about its future prospects.

REFERENCES

[1]. J. Jeong, S.-J. Park, J.-W. Kim, J.-S. No, H. H. Jeon, J. W. Lee, A. No, S. Kim, and H. Park, ‘‘Cooperative sequence clustering and decoding for DNA storage system with fountain codes,’’ Bioinformatics, vol. 37, no. 19, pp. 3136–3143, Oct. 2021.

[2]. N. Weinberger and N. Merhav, ‘‘The DNA storage channel: Capacity and error probability,’’ 2021, arXiv:2109.12549.

[3]. Y. Dong, F. Sun, Z. Ping, Q. Ouyang, and L. Qian, ‘‘DNA storage: Research landscape and future prospects,’’ Nat. Sci. Rev., vol. 7, no. 6, pp. 1092–1107, Jun. 2020.

[4]. A. Lenz, P. H. Siegel, A. Wachter-Zeh, and E. Yaakobi, ‘‘Coding over sets for DNA storage,’’ IEEE Trans. Inf. Theory, vol. 66, no. 4, pp. 2331–2351, Apr. 2020.

[5]. L. Ceze, J. Nivala, and K. Strauss, ‘‘Molecular digital data storage using DNA,’’ Nature Rev. Genet., vol. 20, no. 8, pp. 456–466, Aug. 2019.

[6]. L. Organick et al., ‘‘Random access in large-scale DNA data storage,’’NatureBiotechnol., vol. 36, pp. 242–248, Mar. 2018.

[7]. R. Heckel, I. Shomorony, K. Ramchandran, and D. N. C. Tse, ‘‘Fundamental limits of DNA storage systems,’’ in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2017, pp. 3130–3134.