IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

Secure Data Storage in Cloud using DNA Outsourced Cryptosystem

Prof. Chetan Kumar G S[1], Prof. Rachna HB[2], Abdul Waseem Ilahi[3]

Assistant Professor, Department of MCA, University BDT College of Engineering, Davangere, Karnataka, India[1]

Assistant Professor, Department of E and I, University BDT College of Engineering, Davangere, Karnataka, India[2]

MCA Student, Department of MCA, University BDT College of Engineering, Davangere, Karnataka, India[3]

ABSTRACT: The main goal of this research is to come up with a way to use DNA sequences to make data encryption and decryption more secure and complicated by using a software point of view in cloud computing environments. In the cloud, a secure data storage system using the DNA Cryptosystem is planned to be put in place. By taking advantage of some interesting features of DNA sequences, this is done. The algorithm that has been suggested here is based on binary coding and complementary pair rules, which are two types of rules. There is also a secret piece of data D hidden in the DNA sequence. In the end, D"' is able to upload to cloud environments because of some steps that were taken. It starts when clients decide to use data that is hidden in the DNA reference sequence D.

KEYWORDS: DNA. encryption, decryption, reference sequence.

I. INTRODUCTION

Nucleotides in a DNA sequence are Cytosine (C), Adenine (A), Thymine (T), and Guanine (G). They make up the DNA sequence (G). By adding A and G, you get purine and pyrimidine. By adding C and T, you get pyrimidine, which is made by C and T. In the Watson-Crick base-pairing criteria, A is linked to T, and G is linked to C, as shown in the figure. In a paper called Wang et al., Y. Wang et al. came up with a way to hide data that used recombinant DNA (rDNA) methods and DNA sequencing. One mapping rule table is used to put the message on one DNA sequence, which makes it more likely to be found. Then, a process called rDNA moves the message into the DNA molecule.
From this paper [3,] I came up with DNA Encryption and Decryption techniques that used the Three Phase Process (TPP), which is explained in Research Methodology in a quick way.
If you want to encrypt most existing ABE schemes, you'll need to do a lot of modular exponentiations, which adds up to a lot of time and money. The cost of generating a transformation key in the most common ABE with outsourced decryption grows linearly with the number of attributes that a user's private key has. For mobile device users, these computations are too expensive, which stops the ABE from being used.

From this, I came up with the idea to outsource the encryption and decryption process so that the client devices don't have to work so hard.

Remote data integrity auditing (RDIA) is a good way to make sure that all of the information you store in the cloud is real. If you use a cloud service, like Electronic Health Records (EHRs), some of your private information may be in the cloud files. When a cloud file is accessed, private information should not be shown to anyone else. Shen et al. came up with an identity-based RDIA method for secure cloud hosting in their article [20]. This method allows information to be exchanged while keeping confidential material hidden through a sanitizable signature, and it makes it easier to keep your certification up to date.
The user needs to be sure that the file that the data owner uploaded is the same content that he is downloading. Integrity checking is a must for this. There is a way to do this with the help of Hashing.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

In the proposed system, DNA cryptosystem will be used to keep data safe in the cloud. Both the encryption and decryption of DNA is done on a different server so that the client devices, like phones and tablets, don't have to do a lot of work. Encryption and decryption of DNA are both done in a Three Phase Process (TPP). There are three people in this system, and they are the Trusted Authority (TA), Data Owner (DO), and the User. Hashing is used to make sure that the User is downloading the same content that the Data Owner put on the Internet (DO). Even the person who downloaded the data from the cloud server has a DNA Secret key that can be used to decrypt the data. The data decryption is done by someone else. It must be the same hash signature on both the file that the DO uploaded and the one that was downloaded by the User in order for the Integrity Check Test to be passed. Figure 1 shows this process very well.

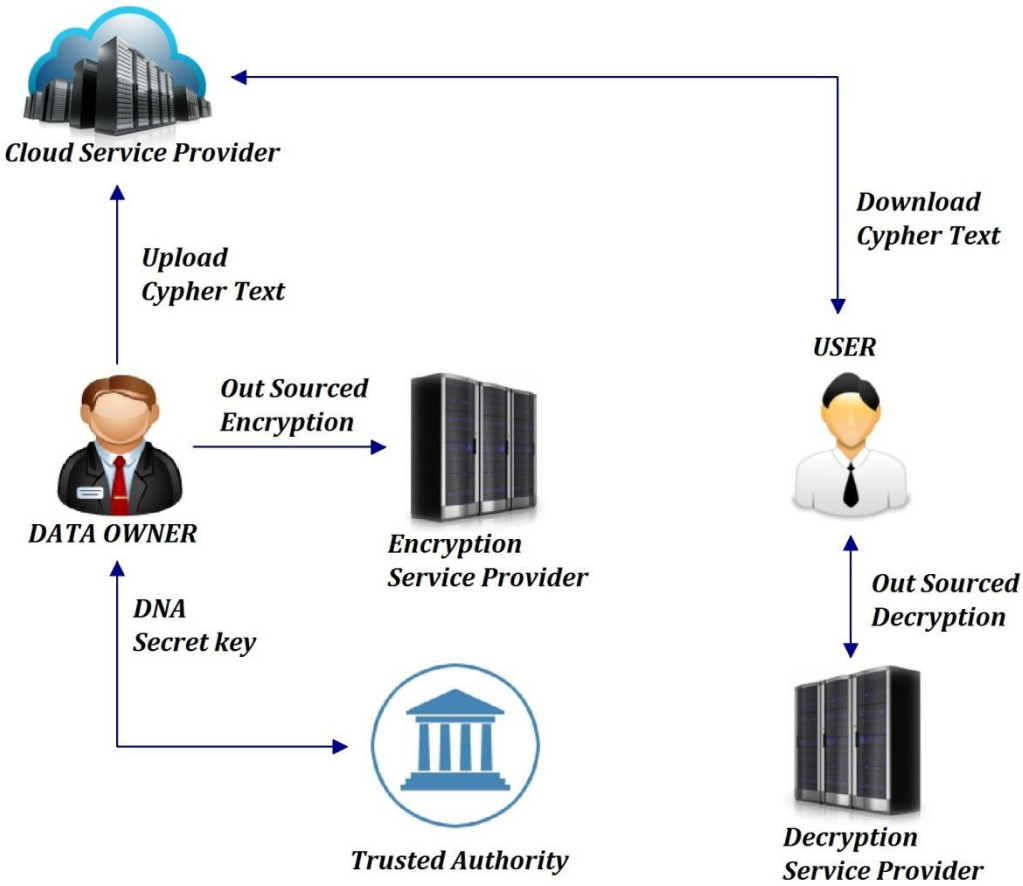


Figure 1: System Model of Proposed Work

II. LITERATURE REVIEW

In paper [1,] C. Zou et al. showed a Rossler chaotic structure that used an optimum formal reaction network that was made by moving DNA strands (DSD). In cryptography, the DSD circuit is used as a chaotic generator to make random sequences. They used the density of the signal stranded DNA to turn chaotic patterns into binary patterns in the encryption method. Analysis of security shows that both the ciphertext and the decrypted text are vulnerable to key differences. Because the ciphertext is arbitrary, the encryption schemes can withstand brute-force attacks and statistical attacks very well. The proposed encryption method can withstand errors in the rate of a reaction tracking, the concentration monitoring deviation, and noises because it is based on a robust method analysis.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

With the development of DNA computing, people are more likely to get images, videos, and texts that aren't supposed to be there. This opens the door to new ways to keep information safe. When M. Samiullah et al. wrote a paper called [2,] they said that colour photos could be encrypted with just one key. As a way to make the colour image encryption process more secure and effective, they used three different chaotic methods: 4D Lorenz-type, Piecewise Linear Chaotic Map (PWLCM), and Lorenz, which are all chaotic methods. They used these methods to make the colour image encryption process more secure and effective (LFSR). The significance and benefits of the suggested system can be seen in its better security test results, ability to withstand possible security threats, bigger key space, and sensitivity to private keys that aren't in the right order.

In paper [4], Fu et al. came up with a way to keep images safe that used DNA encryption and a double chaos technique that used optical chaos and linked map lattices to keep them safe (CML). In 1989, mathematician Mathews added chaos to cryptography. Picture encryption with chaos is good enough for complexity, entropy, and responsiveness. Optical chaos is better than electrical chaos because it has a bigger bandwidth, less distortion, and a higher level of chaos, which makes it good for picture encryption. They used the CML chaotic system to change the order of the optical chaotic sequence in an effort to get the best out of optical chaos. There were a lot of things that showed that the suggested method was good. These things included a bigger key space, key hypersensitivity, distribution, and data randomness. This means that it can withstand a lot of attacks, like brute force, statistical, and differential.

Cloud computing is used by both cloud service providers (CSPs) and people all over the world as a way to back up their files. In paper [5,] Alouffi et al. did an in-depth look at the security issues that people who use cloud computing (CC) services face. It took them a look at 80 publications that have been published in the last 10 years to find the answers to the study questions that they had. They found seven major security flaws in CC services, with hacking and spilling being the most common. The CC environment had more problems, like how data was stored and how it could be accessed. The findings of this SLR show that both CSPs and users have a problem with having their data outsourced. Blockchain technology was found to be the new technology that could help solve the CC security problems.

Using the Internet of Things (IoT) is a popular way to use cloud computing. It allows physical things like sensors, technology, and software to connect through the internet or communication networks to share information with other devices and systems, but this still adds a lot of time to the process. It's when we use "edge computing," which is also known as "fog computing." This reduces latency by moving data from the network edge to the local data centre, but it also raises security and privacy concerns. The Attribute-based Encryption (ABE) method allows for a wide range of access control to support the security and privacy of data at the edge of the network. In paper [6,] Cui et al. proposed a method called proxy-aided ciphertext policy ABE (PA-CPABE), in which the decryption workloads of ABE cipher-texts are given to an unreliable proxy like an edge device without using safe networks for key exchange. This method could be easily added to the edge of the network to achieve fine-grained access control, and it doesn't need to be complicated.

There are a lot of ways to protect your private information when you use biometric authentication. These include fingerprints, iris patterns, and face patterns. Biometric authentication is used in cloud computing, where the data owner can send a lot of biometric data to the cloud in order to save money on processing and storage costs. [4]: Zhu et al. came up with a biometric ID verification system that is both effective and safe, and that can withstand level 2 and level 3 conspiracy attacks from people who don't want to use the system and from the cloud. To be safe and efficient, they build a network and defence model that is well thought out. They used fingerprint authentication by letting the person who owns the data cypher the data and send it to the cloud service, which then performs the identifying process on the encrypted data and only sends the results back to the person who owns the data.

Network coding seems to be a good way to store cloud backups when compared to other backup methods. It can get data back with very little bandwidth and great reliability. Regardless of how the data is retrieved, the communication path between the local data centre and its backup location is easy for someone to listen in on. It's called "link eavesdropping" in the paper [8]. Chen et al. came up with a way to figure out what data system characteristics are important to get back in every level of security for this network-coded cloud service. A network-coded backup platform has a lot of important system features that can be customised for different levels of security. These include the number of storage units and the ability to link the local data centre to the backup cloud.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

There is a big rise in the security and privacy risks of data when cloud servers become the main place to store it. Public CSPs aren't very trustworthy because they may not be able to keep users' data safe from hackers or other people who want to use it. Basic security evaluation methods, on the other hand, only look at external security issues and don't pay attention to the reliability of CSPs. We don't know of any studies that have looked into how safe third-party services (TSPs) are. Also, we don't know of any research that has looked into how safe these services are. They do this by using equilibrium methods to look at the security of open-source CSPs and TSPs in their paper, which is called "Wu et al." They used the models to look at the security benefits and drawbacks of a number of well-known cloud storage platforms, such as Dropbox and Google Drive. Using a Nash equilibrium method, a game between users and CSPs in a cloud environment is judged. Results show that this study has a lot of ways to make real-world apps more secure.

Businesses and the government are worried about how vulnerable cloud computing environments (CCEs) are to threats that keep coming back (ACTs). [10] is a paper by Gonzales et al. that talks about a cloud application model that includes a variety of security measures and practise guidelines, as well as a security evaluation method called Cloud-Trust. Cloud-Trust predicts the maximum security measure that can be used to evaluate CCEs or CSPs' level of privacy and trust. Cloud-Trust was used to check the level of security of the four Infrastructure as a Service (IaaS) cloud structures that were provided with different cloud security mechanisms. Cloud-Trust was used to look at the security of IaaS CCEs and CSPs service offerings, as well as to figure out how ACT intrusion and detection would affect them. These pictures show two of the most important security measures for IaaS CCEs, such as integrity and confidentiality.

Cloud technology has a lot of technical and institutional advantages, but its widespread use is limited by the lack of security and openness given by the CSPs. Cloud systems can be described in legal terms, such as Service level agreements (SLAs). An agreement between the customer and the Cloud service providers (CSPs) is called a Cloud security SLA. People who wrote a paper called "Quantitative Policy Trees" and "Quantitative Hierarchical Process" came up with two ways to try to figure out and measure the security standards that Cloud Customers want from their service providers. They came up with these two methods, called Quantitative Policy Trees (QPT) and Quantitative Hierarchical Process (QHP). Using two different scenarios, they looked at how useful the QPT and QHP approaches were. They looked at how useful they were for both the CSP and the cloud customer. To help CSPs, a sensitivity analysis is done on the Cloud secSLAs. The proposed strategies help to improve security needs descriptions by giving customers a flexible and basic framework that allows them to recognise and express their own safety needs. Finally, they showed a sample of a web service that could help Cloud Customers make decisions about which Cloud Service Providers to choose based on their security promises and a list of common security needs.

In a Cloud computing environment (CCE), the traditional way of encrypting data by using the binary method increases the risk of data being stolen because there are many people who could be bad on the web. DNA technology, which encrypts files using DNA nucleotides, is one of the best ways to improve digital safety. Another thing to think about is how long it takes to find and look at data. [12]: Suyel Namasudra came up with a new way to keep DNA safe and fast. DNASF-ACM keeps a table or list for quick data access, which cuts down on the time it takes to access and search for data. The CSP keeps a list so that you can quickly get to the data you need, which cuts down on the time it takes to find and look at it. In this case, the user's personal information is used to make a 1024-bit DNASF random key, which is then used to encrypt the data. DDoS threats, phishing scams, and other types of scams are all stopped by DNASF-ACM. The proposed ACM is better than other current methods in terms of overall performance, according to the empirical studies that were done.

For the paper [13], Osama Ahmed Khashan came up with OutFS, which is an encrypting file model for users that uses the FUSE cloud platform, which gives any data a "transparent" encryption. OutFS uses both symmetrical and asymmetrical encryption methods, where key management is supposed to be simple and practical, but it doesn't work out that way for everyone. There is also a "identity-based encryption" (IBE) and "OutFS" data exchange scheme that allows safe data exchange in FUSE between the right people. OutFS is meant to keep offshore information and the database design of the system files safe from different types of attacks. In general, it can read and write 8.8 megabytes per second on average, and 10.5 megabytes per second when reading and writing exported files.

CP-ABE is a good way to keep data safe when it's being sent in CCE. Key escrow and arbitrary state attribute expression are two of its flaws, but they're not the only ones. In a paper called [14], S. Wang et al. came up with a new CP-ABE method called ciphertext-policy weighted ABE system with removal escrow (CP-WABE-RE). First, they

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

came up with a better two-main generating system that makes sure both the key authority (KA) and the CSP can't see a user's entire private key. Second, they made the weighed attribute to improve the expression of the attribute, which shows both the arbitrary-state and also reduces the complexity of CP, which reduces storage and time costs in encryption. Finally, for the CP-WABE-RE scheme, they did a lot of research and found that it was a lot better than the previous version.

process of letting the cloud server (CS) make sure the data goes to the right owner through remote data integrity checks is called that (RDIC). Key management has been a problem for many RDIC techniques because they need a costly public key infrastructure (PKI) to work. This could make it difficult to use them in practise. Yu et al. came up with a new identity-based (ID-based) RDIC method. They used an asymmetrical shared key exchange between the CS and the third-party authority (TPA). They talked about two important parts of the ID-based RDIC security paradigm, like reliability and complete data protection. It doesn't tell the verifier about the stored information during the RDIC process. Within a generalised model, this new design has been shown to be safe against a rogue CS and to keep the verifier's information private. The ID-RDIC technique is completely safe and can be used in real-world systems, as a result of a lot of security testing and development.

Cloud storage solutions must be able to deal with data access delays and make sure internet data applications can meet their deadlines. In paper [16], Liu et al. came up with a statistical framework to figure out how long it would take for each server to respond to a request for data. This helped them meet the existing model of service level objects (SLO). It is called DGCloud, and it has three Deadline Guaranteed features: a deadline-aware load balancer, task consolidation, and data placement optimization. They added three more techniques to the DGCloud to make it better, including a dynamic load balancing, a data request queue improvement, and a wakeup server selection method. Each of these techniques cut down on the power costs and communication costs of data duplication and communication. From all of their tests, it was clear that the DGCloud was better than Amazon EC2 and simulation.

Privacy is now a big problem because big data operations are moving to the mobile cloud quickly. It talks about data transmission efficiency and security in the article, which is number 17. In order to solve this problem, Gai et al. came up with the Dynamical Data Encryption Strategy (D2ES) paradigm, which intelligently encrypts files in order to make sure there aren't a lot of encrypted files while still meeting deadlines and then using the right tools and data centres. The Weight Modelization (WM) technique, the S Table Generation (STG) technique, and the Dynamic Encryption Determination (DED) technique were all used in this D2ES scheme. They used these three methods to constantly change data plans for encryption standards with different time limits.

[18]: Z. Li and his colleagues came up with an idea for an ABE system that could outsource both encryption and decryption work. This would make it easier for data owners and consumers to do their work, which would save them money. The idea is called ABE-VOED. Fix: They also lowered the charge for the consumer to change a key to a charge. Finally, they did an operational and security assessment of the ABE-VOED system. They found that it was good for mobile use and that it worked well for both the people who used it and the people who used it.

CP-ABE is a great crypto method for controlling access to cloud services, and Timed-Release Encryption (TRE) can be used to release access privileges at a certain time. In their study, Hong et al. suggested TAFC, which is a timing and attribution component with a way to control access to time-sensitive media in the cloud network. It gets the fine granular feature from CP-ABE. Second, it uses the trapdoor technique while still having the TRE's role as a timed event. They also came up with a good way to design access rules for time-sensitive media when they had to meet a lot of different accessibility standards.

III. RESEARCH METHODS & SPECIFICATIONS

In a cloud environment, clients need to upload data to the cloud in a way that keeps their data safe. So, the clients need to find a way to keep their data more private. This research proposes an algorithm for encrypting and decrypting data using DNA sequences to make it more private and difficult, which makes it more safe.

Encryption:

Encryption is the process of changing data into a form that can't be read. It is used to keep private information safe so that only people who are supposed to see it can see it.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

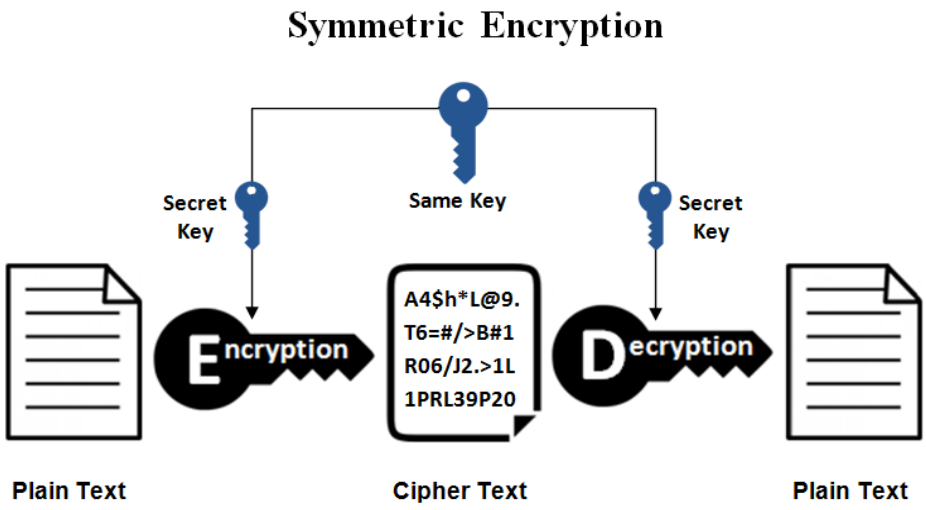
| DOI: 10.15680/IJIRCCE.2022.1005007|

Decryption:

If encrypted data is put back into its original form, it is called decryption. It is usually a process that goes backwards from encryption.

Symmetric algorithm:

Use the same cryptographic keys for both encryption and decryption. Symmetric-key algorithms are cryptographic algorithms that use the same keys for both encryption and decryption.



- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

International Journal of Innovative Research in Computer and Communication Engineering

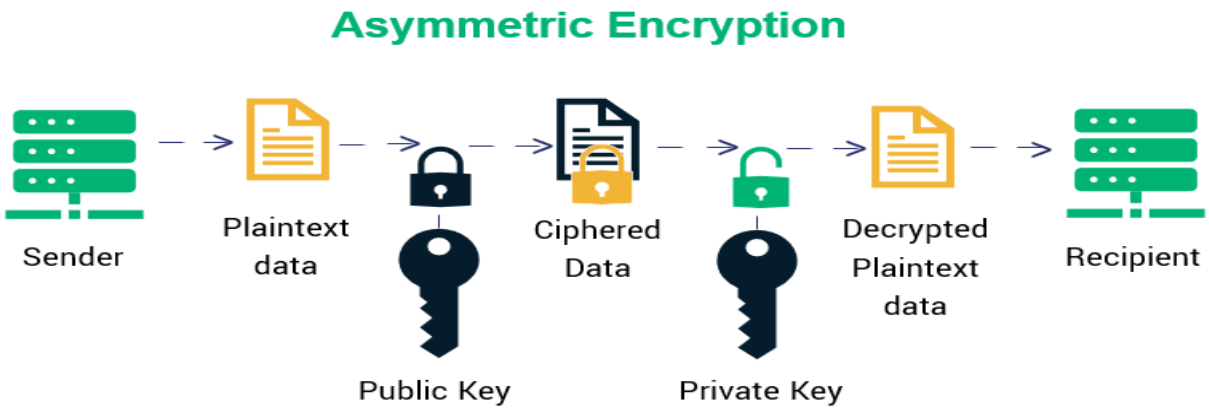
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

Asymmetric algorithm

The term "public-key algorithms" refers to asymmetric-key algorithms. It's called "public and private keys." They use two mathematically linked keys called "public and private keys." For encryption, one key is used and the other is used for decryption.



- Rivest Shamir Adleman (RSA)
- The Digital Signature Standard (DSS), which incorporates the Digital Signature Algorithm (DSA)
- Elliptical Curve Cryptography (ECC)
- The Diffie-Hellman exchange method.
- TLS/SSL protocol.

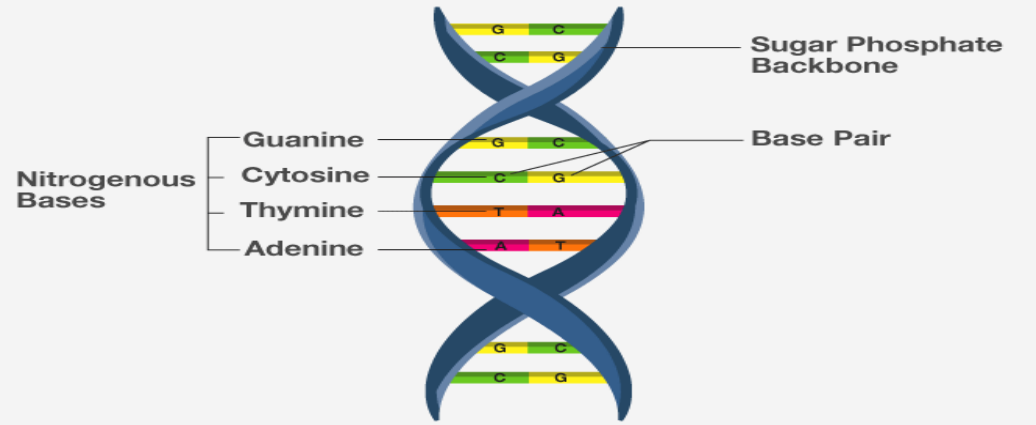
Hashing technique:

Hashing is a way to make sure that the file the user is downloading is the same one that the person who owns the data put on the internet. When the file is uploaded to the cloud, the data owner gets a hash code. Users get a hash code when they want to download the same file from the cloud. Files that are both uploaded and downloaded should have the same hash codes, which are used to make sure they are safe.

DNA algorithm:

DNA Cryptography is a way to hide data in terms of the DNA sequence. This is how cryptography works: Each letter of the alphabet is turned into a different combination of the four bases that make up the DNA in our bodies (DNA).

So, how do you put data into a DNA strand that is mostly made up of four nitrogenous bases?:



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

1. Adenine (A)
2. Thymine (T)
3. Cytosine (C)
4. Guanine (G)

The easiest way to encode is to represent these four units as four figures:

1. A(0) –00
2. T(1) –01
3. C(2)–10
4. G(3)–11

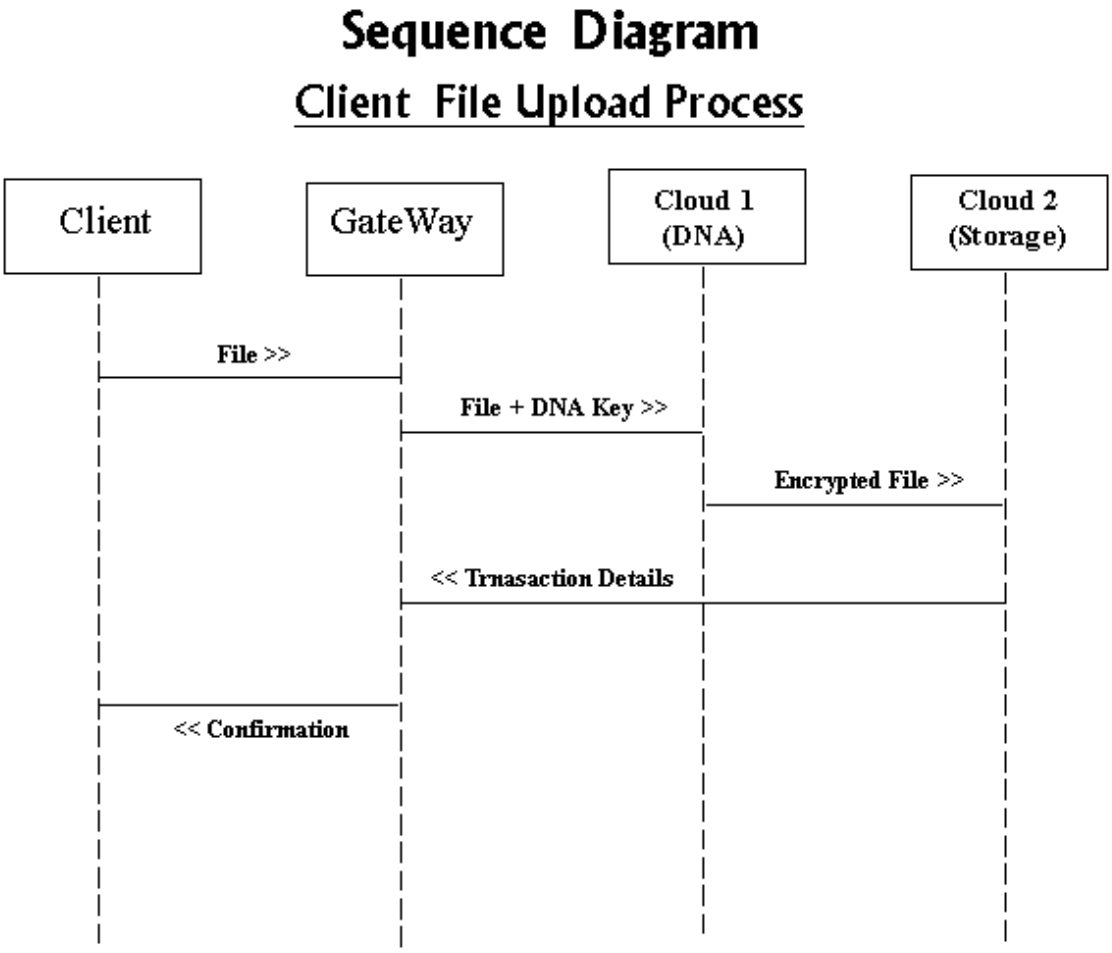


Figure 2: Upload Process Sequence Diagram

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

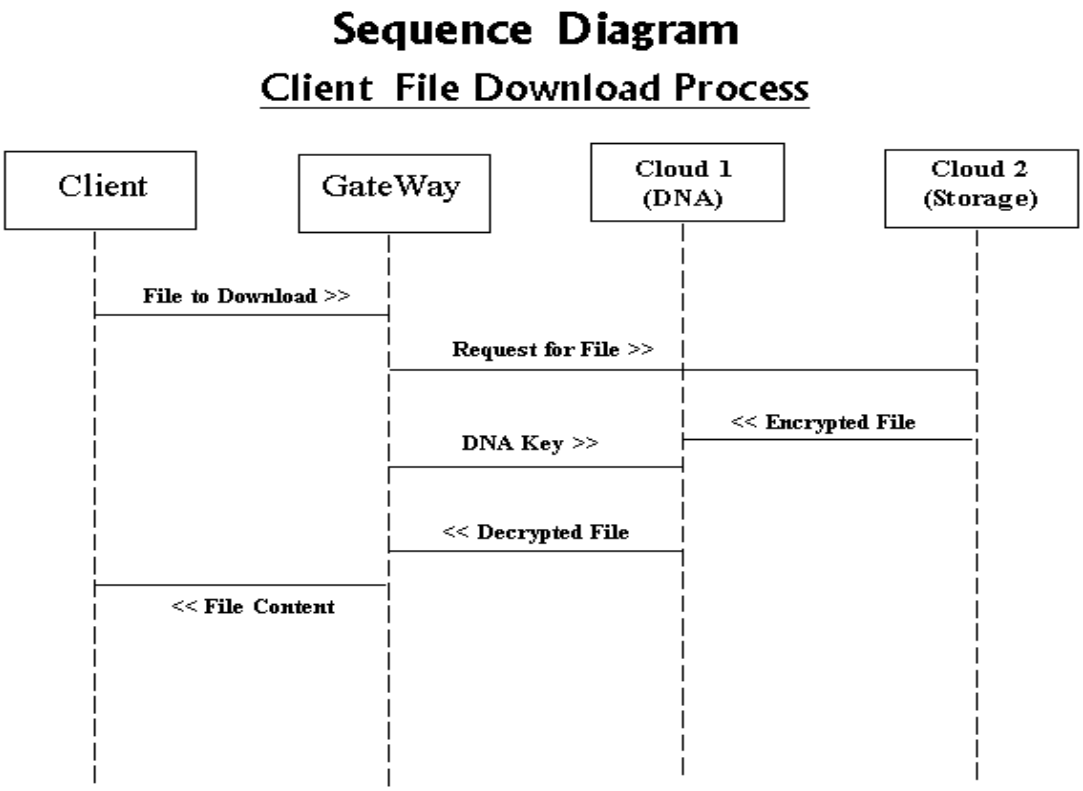


Figure 3: Download Process Sequence Diagram

Encrypting Secret Data

In order to explain the Encryption Process, it has been broken down into three stages that are then broken down into sub-phases, which is the best way to show the current method. In the figure below, the sub-phases have been shown, one by one.

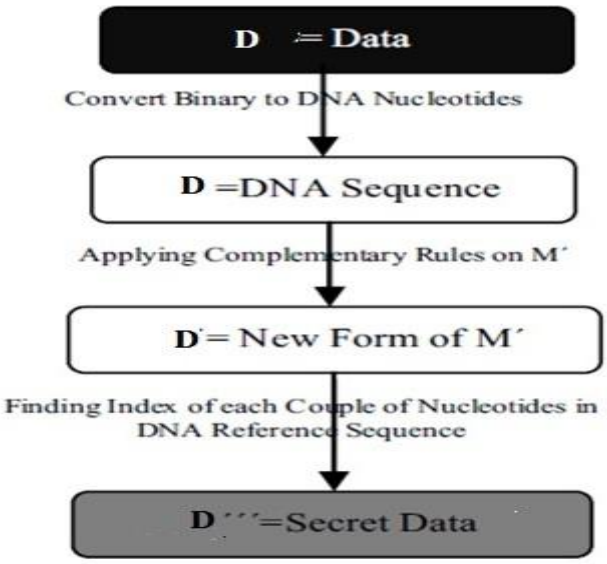


Figure 4: Encryption Process

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

M is the original data that the client decides to put into the cloud computing environments through a network. So, there are three steps to get the final form of M, which is M''', and put it on the cloud. As an integer, the data M is read. Then, it is changed into binary form.

Use the base pairing rules to turn binary data into amino acids that make up DNA. In biology, making nucleotides is done in the same way every time.

Algorithm for Encryption:

Phase 1: Convert binary data to DNA sequences.

Data to be Encrypted: 000001111001

A=00,

T=01,

C=10, and

G=11.

Phase 1DNA strand: AATGCT

Phase 2: Complementary pair rule.

Complementary pair rule is a unique equivalent pair which is assigned to every nucleotides base pair.

Example:

Complementary rule: ((AC) (CG) (GT) (TA))

Phase 1DNA strand: AATGCT

Apply the complementary rule on Phase 1 DNA strand to get Phase 2 DNA Strand CCATGA.

Phase 3: Representing DNA sequences as numeric data.

We extract the index of each couple nucleotides in DNA reference sequence, numerically.

Phase 2 DNA Strand:CCATGA.

Group it in two pairs each: CC-AT-GA

Example:

Assume the reference sequence to be $CT_1GA_2TC_3CC_4GC_5AT_6TT_7$.

Then the numerical representation will be 040602.

In this case, the Trusted Authority creates a unique DNA sequence for each Data Owner (DO), which is a unique DNA key for each DO. This DNA key is used to encrypt the files that are being uploaded to the cloud storage.

Example:

Assume original data D=01000001(Binary Value of Char 'A') should be uploaded to the cloud.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

DNA Secret Key Sequence:

```
[TG, TA, AT, GC, CT, GA, CA, AC, AA, GT, CG, AG, CC, TT, TC, GG]
```

DNA Secret Key Sequence after Indexing

$[TG_{00},TA_{01},AT_{02},GC_{03},CT_{04},GA_{05},CA_{06},AC_{07},AA_{08},GT_{09},CG_{10},AG_{11},CC_{12},TT_{13},TC_{14},GG_{15}]$

- D=01000001 (Original data).
- **Sub-phase1 (Base pairing rule)**

  (A= 00, T= 01, C= 10, G= 11): D´= TAAT
- **Sub-phase 2 (Applying complimentary rule)**

  ((AC) (CG) (GT) (TA)): D´´= ACCA
- **Sub-phase3 (Indexes):**

  D´´´= 0706**(Encrypted data**)

Extracting Original Data (Decryption Process)

Some numbers are sent to Client 2 as a secret message from Client 1. For the purpose of getting the original data from the DNA reference sequence, phase 2 with its subphases will get the original data, as shown in Figure 5.

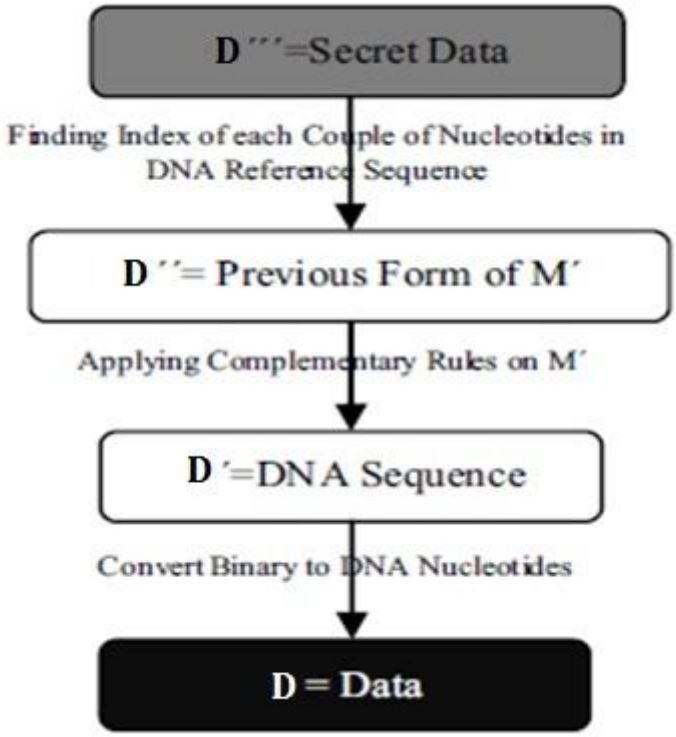


Figure 5: Decryption Process

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

To upload a file to the web server, the user must first go to the DNA Encryption Service, which is running on cloud server 1. Cloud server 1 will encrypt the file, and the encrypted file must be sent to cloud server 2 using the web service concept. Cloud server 2 will store the encrypted file.

Algorithm for Decryption:

Phase 1: Convert numeric data to DNA sequences.

We extract the couple nucleotides in DNA reference sequence according to the index read from the file.

Phase 2: Complementary pair rule.

Complementary pair rule is a unique equivalent pair which is assigned to every nucleotides base pair.

Phase 3: Convert DNA sequences to binary data.

Example:

DNA Reference Sequence:

[TG, TA, AT, GC, CT, GA, CA, AC, AA, GT, CG, AG, CC, TT, TC, GG]

$[TG_{00},TA_{01},AT_{02},GC_{03},CT_{04},GA_{05},CA_{06},AC_{07},AA_{08},GT_{09},CG_{10},AG_{11},CC_{12},TT_{13},TC_{14},GG_{15}]$

- D´´´=0706 (Input)
- By referring the DNA sequence:

  Sub-phase1 (Indexes): D´´= ACCA.
- By using Complementary rule:

  Sub-phase2 ((AC) (CG) (GT) (TA)): D´= TAAT
- By using Base Pair Rule:

  Sub-phase 3(A= 00, T= 01, C= 10, G= 11): D=01000001

(A)**(Output)**

Web users can download files from the web server, but when they do, the corresponding file has to be retrieved from cloud server 2 and sent to the service that decrypts DNA. This service is running on cloud server 1. Afterwards, the file will be downloaded to the user's machine.

REFERENCES

[1] C. Zou, X. Wei, Q. Zhang, C. Zhou and S. Zhou, "Encryption Algorithm Based on DNA Strand Displacement and DNA Sequence Operation,"*in 2021 IEEE Transactions on NanoBioscience (IEEE Nano)*, pp. 223-234

[2] M. Samiullah, W. Aslam, H. Naziret al., "An Image Encryption Scheme Based on DNA Computing and Multiple Chaotic Systems,"*in 2020 IEEE Access*, pp. 25650-25663

[3] Y. Wang, Q. Han, G. Cui and J. Sun, "Hiding Messages Based on DNA Sequence and Recombinant DNA Technique,"*in 2019 IEEE Transactions on Nanotechnology*, pp. 299-307

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005007|

[4] X. -Q. Fu, B. -C. Liu, Y. -Y. Xie, W. Li and Y. Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos,"*in 2018 IEEE Photonics Journal*, pp. 1-15

[5] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies,"*in 2021 IEEE Access*, pp. 57792-57807

[6] H. Cui, X. Yi and S. Nepal, "Achieving Scalable Access Control over Encrypted Data for Edge Computing Networks,"*in 2018 IEEE Access*, pp. 30049-30059

[7] L. Zhu, C. Zhang, C. Xu, X. Liu and C. Huang, "An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing,"*in 2018 IEEE Access*, pp. 19025-19033

[8] Y. Chen, L. Wang and C. Liao, "Eavesdropping Prevention for Network Coding Encrypted Cloud Storage Systems,"*in 2016 IEEE Transactions on Parallel and Distributed Systems*, pp. 2261-2273

[9] Y. Wu, Y. Lyu and Y. Shi, "Cloud storage security assessment through equilibrium analysis,"*in 2019 Tsinghua Science and Technology*, pp. 738-749

[10] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds,"*in 2017 IEEE Transactions on Cloud Computing*, pp. 523-536

[11] J. Luna, A. Taha, R. Trapero and N. Suri, "Quantitative Reasoning about Cloud Security Using Service Level Agreements,"*in 2017 IEEE Transactions on Cloud Computing*, pp. 457-471

[12] Suyel Namasudra, "Fast and Secure Data Accessing by using DNA Computing for the Cloud Environment,"*in 2020 IEEE Transactions on Services Computing*

[13] Osama Ahmed Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," in 2020 IEEE Access, pp. 210855-210867

[14] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu and W. Xie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing," *in 2016 IEEE Transactions on Information Forensics and Security*, pp. 1661-1673

[15] Y. Yu, M. H Au et al., "Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage,"*in 2017 IEEE Transactions on Information Forensics and Security*, pp. 767-778

[16] G. Liu, H. Shen, H. Wang and L. Yu, "Towards Deadline Guaranteed Cloud Storage Services,"*in 2021 IEEE Transactions on Services Computing*, pp. 915-929

[17] K. Gai, M. Qiu and H. Zhao, "Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing,"*in 2021 IEEE Transactions on Big Data*, pp. 678-688

[18] Z. Li, W. Li, Z. Jin, H. Zhang and Q. Wen, "An Efficient ABE Scheme With Verifiable Outsourced Encryption and Decryption,"*in 2019 IEEE Access*, pp. 29023-29037

[19] J. Hong, K. Xue et al., "TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud,"*in 2020 IEEE Transactions on Services Computing*, pp. 158-171

[20] W. Shen, J. Qin, J. Yu, R. Hao and J. Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage*," in 2019 IEEE Transactions on Information Forensics and Security*, pp. 331-346

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details