Fuzzy Systems and Soft Computing
ISSN : 1819-4362

NOVEL APPROACH FOR DATA SECURITY OF CLOUD STORAGE USING HASARA ALGORITHM

Naveenraj. V PG & Research Department of Computer Science, Dr. Ambedkar Government Arts College, India. Email : naveen.nice.1990@gmail.com
A. Murugan PG& Research Department of Computer Science, Dr. Ambedkar Government Arts College, India.

Abstract.
Cloud computing file storage is provided by a network of distant file servers housed online. Massive amount of material may be processed, managed, and stored in the cloud without the need for local servers or desktop computers. It involves putting the data in a way that makes it invisible to everyone but the people with the proper authority. Users' data security is the primary use case for cryptographic processes, which protect data from abduction or modification. Utilising a distinct mechanism for each file, this paper argues in favour of encryption and decryption utilising a set of policies. Several intermediary processes are involved in this procedure; the files were encrypted by creating random ideas and seeing information in binary coded form. The proposed algorithm uses both key and passcode. Binary-coding to encrypt the communication. The practice of concealing personal information from hackers and identity thieves is common in both public and private institutions. It ensures that data is transmitted securely and privately on the server.

Keywords:
Het ApenSpel, Cryptography, Encryption, Decryption, Data Security, etc.,

1. Introduction

Cloud computing is the organised, rapidly evolving technology that grows more and more.The cloud storage for files is a technique for data retrieval and storage in the cloud allowing applications and servers with shared file system access. Favourable storage, on-demand resources, affordability, straightforward storage administration, and user-friendly maintenance are among the benefits of cloud storage [1]. Since the data centres where the cloud data is kept are geographically dispersed and have different locations, the user's file will not be under their control there. To manage user access to their cloud-stored data, sufficient policies and access control methods are required. The cloud service provider sets these restrictions, which require that only authorised users of the file be permitted access to their data. The highly secure access control and protection protocols are required because of the secret nature of the cloud-stored content [8]. The scalability, interoperability, affordability, and resource availability of cloud file storage are its main advantages.

As transmission applications have grown so successfully, data security is important in communication systems. Using encryption, the original text message can be changed into an unidentified format. Transforming encrypted data back to its original state is known as decryption. Data is encrypted and decrypted using a technology called cryptography, sometimes referred to as cryptology. On the sender side, encryption is completed before data is transmitted to the network, and on the recipient side, decryption is completed [2]. With the help of the key-value system and the cryptographic algorithm that is employed to both encrypt and decrypt the results, the data can be securely encrypted using the present cryptographic technique. The numerical code and tag are utilised for the cryptographic process in order to retrieve the original message [9].

Since the use of the internet is growing daily and is occurring not just on desktops but also on smartphones, individuals and organisations alike are expecting a great deal of new technologies and resource optimization[3]. A new technology is required to meet the demands of high storage, random key generation for encryption, and decryption by enabling more secure and dependable communication. As data loads increase on networks, so does the likelihood of data being captured, stolen, altered, or cracked by an attacker or intruder.

2. Related Works

In accordance with Sreelakshmi et al. [4][10], file cryptography is built on employing image steganography techniques to conceal text values. The picture steganography file is then processed via RSA public key encryption. Text cryptography processing takes longer than other cryptography processing methods because of the created RSA encryption file that is fed into the DNA encryption technique.

Rohit and Rahul Gupta [5] [11] developed the RIT integral approach for encryption and decryption. The key 'R' is a unique key that has been generated prior to the start of the encryption procedure. Instead of assigning certain fixed values like ASCII. General numbering method follows by assigning the characters in the message. Modulus idea is used in repeated mode. Attackers can then easily predict the process once the message values have been applied for the encryption method.

Mohankumar et al. [6][12] proposed an encryption method that uses a user-based key technique. The encryption process happens when DNA values match according to the fixed number of DNA nucleotide pairs. The ASCII form of binary conversion will be processed by the algorithm. After applying that pair of values to substitute the converted ASCII number, Finally 1's complement is applied to the result found in the converted text.

Applying both private and public keys, Melvin Vector et al. [7][13] develop a state-of-the-art encryption technique. The proposed approach integrates the best aspects of Advanced Encryption Standard (AES), Post Quantum Cryptography (PQC), and Elliptic Curve Cryptography (ECC). A benefit of the algorithm is that it has a solid base. This technique lowers the possibility of a cyber-attack. Because three extremely large algorithms were employed in the implementation of the suggested system, it requires extra time.

3. Methodology

The proposed HASaRA method has two major processes: the HAS and ReArrange algorithms. The major algorithms receive inputs as message, key, and passcode. Both algorithms were converting the message into seven-bit binary numbers. After that, the process of the algorithm requires reversing the process of binary to ASCII characters. Both algorithms use a 2D rectangular array for its process. In this method, different repositioning and diffusing techniques are used.

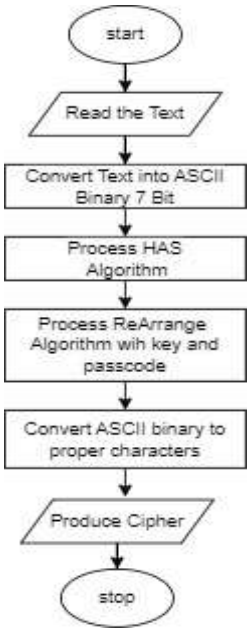

Figure 1: Encryption

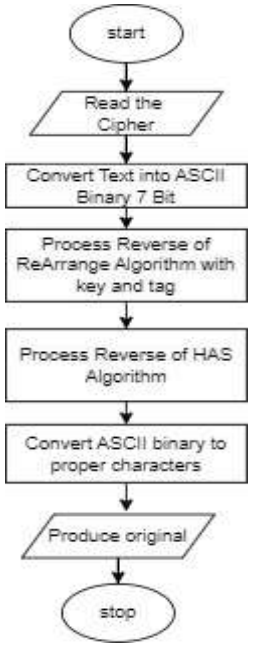

Figure 2: Decryption

3.1.1 HAS

Het ApenSpel Monkeys Apes c.1900 is a Dutch board game. The player (monkey) who collects coconuts in the cub and reaches the pyramid wins the game. In the event that all the coconuts are used up and the game ends, the player whose card has the most number of coconuts in the cups wins. The participant who performed last won the game when there were tied coconuts. Inspired by the ideology of root, we were chosen to travel with a monkey in a 10 x 7 array. That method plots the binary bits in normal 2D array order and is taken from the outcome of a spiral with even and odd positions separately stored and combining binary values. To match the size of the array, you need to adjust the salting content of the delimiter, pin, and passcode. Decryption algorithm is the reverse process of that algorithm in reverse mode in the following procedure.

Algorithm 1 : HAS
Input : Message, pin, passcode
Output : Partial encrypted Cipher

```
Begin
SetMessage=Message+":+;"+pin+tag
SetMessage=lengthof10s(Message) // convert length into 10's character span
Set streambit= converttobinary(Message) // function convert the  binary value string
  Set inta[7][10] // for process het apenspel spiral
Do
        {
                Do
                {
                        a[j][k]=nextChar(streambit)
                        Set j=j+1
                } Until k<10
                Set k=k+1
        }Until j<7
Set t= spiralOrder(a[j][k])
Do
  {
                if(i%2==0)
                        s1+=nextChar(t)
                else
                        s2+=nextChar(t)
        }Until i<t.length
 Set s=s1+s2;
 Set Result=Converttoascii(s)
End
```

3.1.2 ReArrange Algorithm

ReArrange algorithm used for repositioning the values in the message as given. Based formula given below.

$Pos_i = pf * (pin+i) \% L$ (1)

The ReArranage Algorithm processes the random position of after getting Het ApenSpel algorithm output. The above given formulation manipulates the unrepeated position of input given to the algorithm. Pos_i returns the next position of string reposition. The *pf* means that the prime factor has the next prime value of the pin. *L* is the length of input. The ReArrange algorithm processed in two cycles one is based on the pin. Next one is based on the passcode. The tag value is likewise pin tag ASCII values computed as some calculation made then instead of processing the pin for the cycle 2 procedure.

Algorithm 2 : ReArrange

Input : Partial Encrypted Cipher, pin, passcode
Output : Result Cipher

Begin

Set streambit= converttobinary(Message) // function convert the binary value string
//Cycle 1
Set pf=nextPrime(pin) // calculate next prime factor of pin
Do
{
Pos[i] = pf * (pin+i) % L
Set res[i]=charAtPostion(Pos[i]) //this function returns the character position as given
Set i=i+1
} **until** i< L
//Cycle 2
Set tagprocess=sumofAscii(passcode+passcode) // this function totals the values of every character
Set tagprocess = tagprocess *7
Set pin=tagprocess
Repeat cycle 1with pin generated
Set Result=Converttoascii(res)

End

4. Results and Discussion

The suggested approach is implemented in java since it has relatively short execution times and minimizes code size. The plain text included in the text is both encrypted and decrypted. This algorithm is not a complete encryption technique. It is implemented for secure file storage in cloud file storage on the server end. Input of the algorithm already encrypted on the client encryption based on their user attributes. It is a second phase encryption technique. The given below measures not a complete measure of full phase only the second phase metrics. Tested in Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz processor with windows 11 pro operating System. But, the servers have 32, 16 cores, this processor having 2 cores only. That's why time is taken for processing.

Table 1 : Performance of Encryption and Decryption

Size of Input (letter)	Encryption (ms)	Decryption (ms)
10	32	31
100	160	156
1000	1130	1072

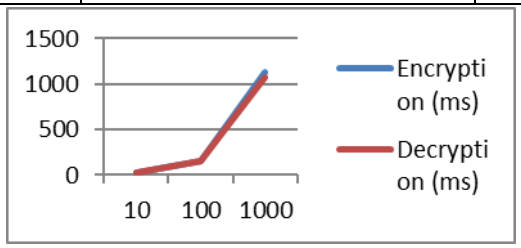

Fig 3 : Performance of Encryption and Decryption

5. Conclusion

The technique is very robust against different types of attacks since a randomly created key and tag used for the server decrypts the cipher text. But, the original information has not yet got to the server authorities. Because, the implemented method for server to secure files. The content is already encrypted by the user based on encryption. It's a second phase algorithm. The key and tag may get different for different region servers. Common cryptanalysis techniques have difficulty breaking the suggested methodology. This method offers better temporal and computational complexity, enhanced

reliability, and two-stage security. In, future the concept will be implemented for image and other formats of data.

6. References

[1] Shalu mall and sushilkumarsaroj. A New Security Framework for Cloud Data. *Elsevier*.2018. procedia computer science 143.

[2] BahubaliAkiwate and LathaParthiban. A Dynamic DNA for Key- based Cryptography. *International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS*). IEEE. 2018. PP 223-227. ISBN: 978-1-5386-7709

[3] Pushpa B R. A New Technique for Data Encryption using DNA Sequence. *International Conference on Intelligent Computing and control(I2C2)*. 23-24 June 2017. EISBN: 978-1-5386-0374-1. Coimbatore, India

[4] Sreelakshmi S and Tinu Thomas. File Encryption and Decryption Using Cryptanalysis. *ICCIDT - 2023 Conference Proceedings*. 11(1). Managalam College, Kottayam, Kerala

[5] Rohit Gupta and Rahul Gupta. Securing data transmission by cryptography using Rohit integral transform. *International Journal of Engineering & Technology*. 2023. 12(2). PP 109-111.

[6] B.Mohankumar, B.Ramya and G.M.S.A.Katamaraju. File Encryption and Decryption Using DNA Technology. *Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020)*. IEEE. 5-7 March 2020. ISBN: 978-1-7281-4167-1. DayanandaSagar College of Engineering, Bengaluru, Karnataka, India

[7] Melvin Victor, D David WinsterPraveenraj and Sasirekha R. Cryptography: Advances in Secure Communication and Data Protection. *E3S Web of Conferences* 399. ICONNECT-2023. 27-28 April 2023. Tiruchirappalli, Tamil Nadu, India

[8] Information Center Veritas. File Encryption 101: Safeguarding Your Sensitive Data. *https://www.veritas.com/ information-center/file-encryption*.Veritas Technologies LLC . 2024

[9] Menaka, K. Message Encryption Using DNA Sequences. *2014 World Congress on Computing and Communication Technologies*. doi:10.1109/wccct.2014.35. PP 182 – 184. Trichirappalli, India

[10] Srilatha, N and Murali, G. Fast three level DNA Cryptographic technique to provide better security. *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. doi:10.1109/icatcct.2016.7912037. 21-23 July 2016. SJB Institute of Technology, Bengaluru, Karnataka, India

[11] Uttam Dattu Kharde. An Application of the Elzaki Transform in Cryptography.*Journal for Advanced Research in Applied Sciences*, October 2017. 4(5). PP 86-89. ISSN (ONLINE): 2394-8442

[12] Priya, S. V. K. and Saritha, S. J. A robust technique to generate unique code DNA sequence. *International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*. doi:10.1109/icecds.2017.8390178. 2017. PP 3815-3820. Chennai, India

[13] Smith, J. Cryptography: An Overview of Secure Communication Protocols. *Journal of Network Security*, 2022. 15(3). PP 45-62.

Authors' background

Your Name	Title*	Research Field	Personal website
Naveenraj V	Protection of Cloud File Storage	Cloud Computing	Nil
Murugan A	Data mining Techniques	DNA Computing	Nil