Volume: 11 Issue: 04 Pages: 4374-4377(2020) ISSN: 0975-0290

Fibonacci Technique for Privacy and Security to Sensitive Data on Cloud Environment

Harikrishna Bommala
Assistant Professor
Computer Science and Engineering
Chalapathi Institute of Engineering and Technology, Guntur.
Email: haribommala@gmail.com
Dr. S. Kiran
Assistant Professor & Co-Ordinator
Computer Science and Engineering
YSR Engineering College of Yogi Vemana University, Proddatur
Email: rkirans125@gmail.com
T.Venkateswarlu
Assistant Professor
Computer Science and Engineering
Chalapathi Institute of Engineering and Technology, Guntur.
Email: venkat543@gmail.com
M. Asha Aruna Sheela
Assistant Professor
Computer Science and Engineering
Chalapathi Institute of Engineering and Technology, Guntur.
Email: ashaarunasheela@gmail.com

ABSTRACT

Cloud computing is increasingly popular in the distribution of the computing environment. Process and implement cloud storage data to become a global movement. Software as an organization Software as a Service (SaaS) has many commercial applications and in our day to day, we can only say that it is disruptive technology [1]. Data security has become a major problem in the field of cloud ecosystems because data is available in various parts of the world to access the Internet for free as it progresses. The global security record for mid-2018, with a cloud data migration of approximately 86.67%, a global analyst estimates that this range can be 100% [8, 9]. Change the data of two or more people, so that unauthorized people can access real data. There are many different ways to perform this conversion, but the method there has proposed a text input method so that the recipient can access the original information. Encryption has become a solution and alternative encryption algorithms play an important role in the security of data in the cloud. In this process, the process investigation operation is designed to obtain data to avoid breaking an unauthorized person. In this way, you can protect any type of files using the Fibonacci series. The proposed algorithm s is encryption and decryption process takes a less of time compare with other traditional security algorithms.

Keywords - **Fibonacci, Security, Cloud, Confidentially, Symmetric key**.

Date of Submission: Feb 14, 2020 Date of Acceptance: March 07, 2020

I. INTRODUCTION

Cloud Computing is becoming fashion in the area of distributed Technology. The processing and storage of data in a cloud environment is intended to promote global mobility [3]. As a general data structure for describing the relationships between devices, a diagram has been increasingly used to show complex entities and to model datasets without schemas, Conversely, the knowledge necessity be moderated, although it can capture the knowledge and Personal communication network, a database that works to protect users' privacy. These private data must be encrypted before sending to the cloud [5]. Almost all information is shared to be shared with trusted partners of all organizations. Data and storage are dangerous because all illegal users can change and access them. There is a need for protected information. Information is protected if it meets three criteria: (i) integrity (ii) privacy (iii) accessibility means that the information received by the recipient must be in the same form and submitted by the sender. Prevent an illegal user from messing around. Privacy means that information is understandable to everyone else, that it can be trashed. It helps to submit unauthorized permission for sensitive information [6]. Availability refers to the guarantee that the user has access to information and to all systems at the same time. In the cloud, confidentiality is achieved through cryptography [2].

II. LITERATURE REVIEW

B. Harikrishna et al. [1] Service in Internet-based access to use as a paid, and is managed in the cloud IT industry. In

Volume: 11 Issue: 04 Pages: 4374-4377(2020) ISSN: 0975-0290

particular, for every organization the website is reliable; however, the information should flow but not contain the information [6]. B. Harikrishna et al. When sensitive information is stored in the public domain, problems arise when consumers leave the environment altogether because they are not sure that the information is on the cloud [10]. Different encoding techniques such as AES, DES and RSA in the name of various statistics as required in memory and computer time [9]. AES requires less time to be evaluated without RSA and DSA. The analysis shows that to be able to provide secure communication with neighbors and enter standard text passwords and MD5 authentication buttons [3]. Plaintext passwords are used to debug, while MD5 authentication buttons can prevent successful network protocol exchange. The sender uses this key and the encryption algorithm to encrypt the data, the recipient uses the same key and the corresponding algorithm to interpret this data [4]. Sender's public key is used to encrypt the sender; the recipient has decrypts the text using a private key.

III. PROPOSED METHODOLOGY

Fibonacci Technique

The Fibonacci method is an emerging field in data protection, basic statistical modeling, and several methods have been found to obtain the highest order terms of this method. The general idea of Fibonacci encryption is based on the Fibonacci functionality of the sequence of text data in the original message encryption.

In the proposed Fibonacci and Random key technique, it is used to encrypt a solid key file. The input text file is converted to a non-Fib Encryption algorithm file, but the key used in the encryption process is produced by Random and Diffie-Hellman to help reproduce and upload the Random Key to the Cloud. After successful key matching, the client is able to translate text messages with this button to find the original text file.

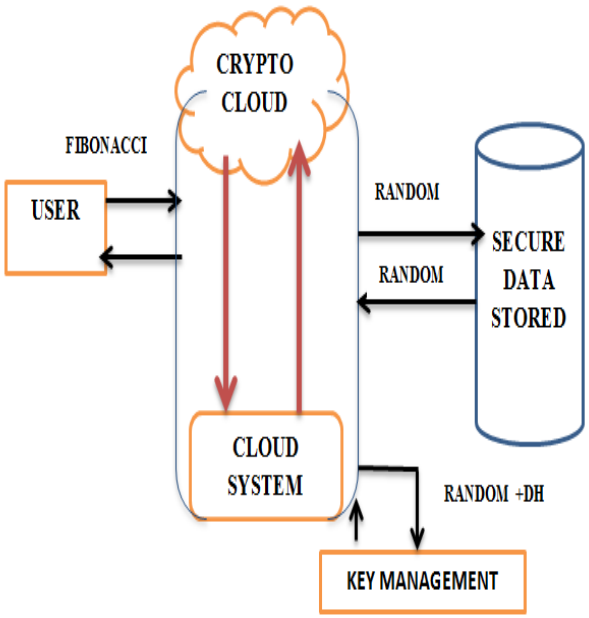

Figure 1: Proposed Model

The main purpose of the proposed project is to protect the system so that only an unauthorized user can access the Cloud when an unauthorized user tries to access our private Cloud can view the IP address and MAC of the device and try to completely block access to our private Cloud [4]. It is proposed a process in which the original data is converted into data not referenced by the Fibonacci process. In that original data, each distance or character is converted to digits by the encryption process to take a Fibonacci random key sequence key.

Time Complexity:

$T(p<=1) = O(1)$

$T(p) = T(p-1) + T(p-2) + O(1)$

Base: p = 1 is obvious

Assume $T(p-1) = O(2^{p-1})$, therefore

$T(p) = T(p-1) + T(p-2) + O(1)$ which is equal to

$T(p) = O(2^{p-1}) + O(2^{p-2}) + O(1) = \mathbf{O(2^p)}$

Or

$f(p) = f(p-1) + f(p-2)$

Each leaf will take O(1) to compute, T(p) is equal to Fib(p) x O(1).

$M^p == M(^{p-1}) + M(^{p-2})$

Divide through by $M(^{p-2})$:

$M^2 == M + 1$

Solve for 'M' and you get **(1+sqrt (5))/2 = 1.6180339887**, otherwise known as the golden ratio.

The Fibonacci sequence itself **$(\sim\theta(1.6^p))$.**

Algorithm for Fibonacci Encryption

1. start
2. read plain text
3. key generated by rand function with embed to plaintext
4. Generate Fibonacci series for number of characters in plain text from 1,1,2,3,5…
5. convert each character in plain text to ASCII value that append to previous and next vale by using Fibonacci to kept to decrypt file.
6. Check the character getting ASCII values go to step 5 with to convert decimal to ASCII value
7. Value to convert binary formate and position based split to even and odd formate.
8. Even and odd binary number to convert decimal and to perform right shift operator get decimal value
9. To convert decimal to ASCCI number
10. to store the decrypt file
11. stop

Volume: 11 Issue: 04 Pages: 4374-4377(2020) ISSN: 0975-0290

Algorithm for Fibonacci Decryption

1. Start
2. Read decrypt file from user input
3. Each character in Decrypted File (DF) to find and convert decimal to ASCII value.
4. Generate Fibonacci series from 1,1,2,3,5
5. Extract key from Decrypt File
6. Based on Fibonacci series follow add to character in decrypted files like letters previous and after the values added.
7. Subtracted key from ASCII value of each character in decrypted file
8. The result convert to binary number
9. Split even and odd binary number formate
10. To convert decimal value and perform left shift operator to get ASCII value
11. To convert ASCII to decimal to kept in plain text file
12. Continue from step 6 for all ASCII values in decrypted file.
13. Stop

IV. RESULTS AND ANALYSIS

Performance evolution is performed by determining the amount of time required to perform different cryptographic algorithm. Crypt-Cloud is one of the Cloud platforms, Fibonacci + Random Algorithm is used to analyze different file size tests, find encryption and computational results and compare it with other cryptography algorithms.

The bottom of table 1 and Figure 2 show the various file sizes encrypted using the different cryptography algorithms and the proposed Fibonacci algorithms. Based on the proposed results, the algorithm takes less time for the encryption process. All attackers are not hacking the file.

Table 1: performance encryption for different file size

FILE SIZE(Kilo Bytes)	DES	AES	RSA(SEC)	FIBONACCI(SEC)
10	0.012	0.023	0.051	0.003
20	0.056	0.059	0.065	0.005
30	0.068	0.067	0.073	0.009
40	0.073	0.076	0.082	0.012
50	0.079	0.084	0.092	0.019
60	0.088	0.092	0.098	0.029
70	0.1007	0.1002	0.102	0.034
80	0.1027	0.1034	0.143	0.038
90	0.117	0.113	0.165	0.045

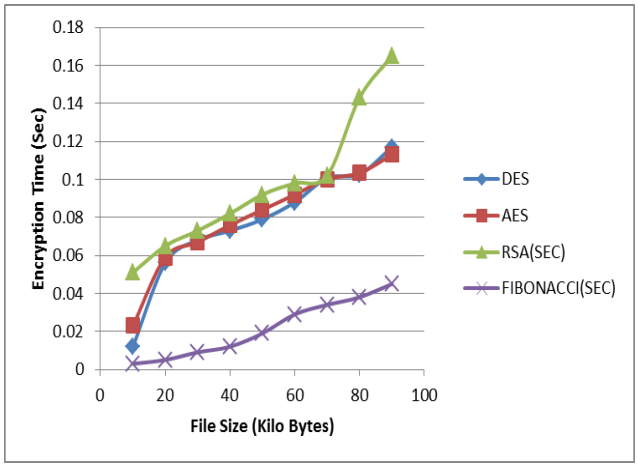

Figure 2: File Size (Kilo Bytes) Vs Encryption Time (Sec)

Below Table 2 and Figure 3, shows different file size has encrypted by using different cryptography algorithms and proposed Fibonacci decryption algorithms. Based on the results proposed algorithm is taken less time for decryption process.

Table 2: performance Decryption for different file size

FILE SIZE(Kilo Bytes)	DES	AES	RSA(SEC)	FIBONACCI(SEC)
10	0.013	0.019	0.045	0.002
20	0.049	0.051	0.056	0.0049
30	0.052	0.057	0.0632	0.00834
40	0.067	0.062	0.072	0.0112
50	0.077	0.082	0.082	0.01672
60	0.082	0.085	0.0875	0.01875
70	0.100134	0.10006	0.1012	0.028
80	0.10125	0.1028	0.143	0.0356
90	0.121	0.134	0.165	0.0421

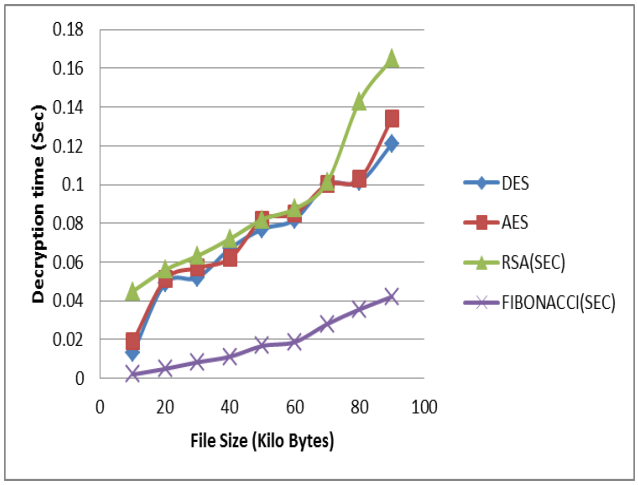

Figure 3: File Size (Kilo Bytes) Vs Encryption Time (Sec)

Volume: 11 Issue: 04 Pages: 4374-4377(2020) ISSN: 0975-0290

V. CONCLUSION

Cryptography provides data securely, to an unauthorized person. Therefore, many cryptography methods are available to provide data security to third parties. In this research work, proposes a Fibonacci method of requesting sensitive data to be protected by hackers. In this algorithm key is automatically generated and hidden in quotation marks that provide privacy and reduces the maximum burden on the user. The proposed Fibonacci algorithm is used to secure input files of various sizes. It allows secure communication between two entities, one of the text data being able to convert unreadable data that encapsulates the measurement key in the cloud environment. The results show that Fibonacci encryption / encryption is much faster among symmetric algorithms and does not hack the data from the hackers. Therefore, the algorithm used finds its place in a wide range of applications such as e-commerce, banking, and online applications, large and large industries, Internet communications, multimedia systems, medical imaging, tele-medicine, tele-communications, Military, software developers, personal use, education, business, and Banking etc.

VI. BIBLIOGRAPHY

[1]. Harikrishna B, Kiran S, Murali G, Pradeep kumar Reddy R (2016) Security issues in service model of cloud computing environment. Procedia Comput Sci 87:246–251.

[2]. Atul Kahate, “Cryptography and Network Security”, Tata McGraw-Hill, 2003.

[3]. Aamer Nadeem, Dr. M.Y.Younus Javed, “A Performance Comparison of Data Encryption Algorithms”, 2005 IEEE.

[4]. A.P. Stakhov, “Fibonacci Matrices, A Generalization of the “Cassini Formula”, and new coding theory”, Chaos, Solitons and Fractals, Volume 30, Issue 1, 2006.

[5]. Dr. V. Sundaram, “Secured Communication through Fibonacci Numbers and Unicode Symbols” International Journal of Scientific & Engineering Research, Vol.3,Issue 4,April 2012,pp.490-494.

[6]. B. Harikrishna, S. Kiran and R. P. kumar Reddy, "Protection on sensitive information in cloud — Cryptography algorithms," 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2016, pp. 1-5.

[7]. Syed Khutubuddin Ahmed Khadri, Debabrata Samanta, Mousumi Paul, “Approach of Message Communication Using Fibonacci Series: In Cryptology”, Engineering and Technology Publications”, Vol. 2, No. 2, June 2014, pp. 168-171.

[8]. Harikrishna B, Kiran S, Deep KM (2018) Network as a service model in cloud authentication by HMAC algorithm. Int J Adv Netw Appl 9(6):3623–3631.

[9]. Bommala, Harikrishna & Sk, Kiran. (2020). Sensitive Information Security in Network as a Service Model in Cloud-IPSec. 10.1007/978-3-030-24322-7_29.

[10]. Bommala, Harikrishna & Sk, Kiran & Pujitha, M. & Reddy, R.. (2019). Performance of Evaluation for AES with ECC in Cloud Environment. International Journal of Advanced Networking and Applications. 10. 4019-4025. 10.35444/IJANA.2019.10056.

[11]. Bommala, Harikrishna & Sk, Kiran. (2019). Client Authentication as a Service in Microsoft Azure. International Journal of Engineering and Advanced Technology (IJEAT), Volume-8 Issue-2, ISSN: 2249 – 8958.