Security of Data using Crypto Cloud Multilayer Blowfish DNA Technique

Mohammed Basheer Khan
Research Scholar,
CSE, SIRTE, Bhopal, India

Sneha Soni
Asst Prof.
CSE, SIRTE, Bhopal, India

Kalpana Rai, PhD
HOD CSE,
CSE, SIRTE, Bhopal, India

ABSTRACT
Information is the most valuable thing in today's life. It has the power to change the world, in the digital world each and everyone using the cloud to Store baulk of data in the form of E-mails, cloud drives, social sites, apps etc. because of easy access durability, but it depends on the internet, the internet is nothing but large network your information is on it. Therefore Data security is very important. Cryptography key way to protect data but an older Algorithm is not enough in this technique proposed a Cloud crypto MBDNA (Multilayer Blowfish DNA) Technique, With Java.

General Terms
Security of Data, Cloud Computing, Multilayer Cryptography, DNA Cryptography, Blowfish.

Keywords
Cloud Computing, Data Security, Algorithms, Cryptography, DNA Technique, Blowfish Cryptography.

1. INTRODUCTION
Cloud computing is computing resources as a service through the internet. Computing resources can be defined as Infrastructure (hardware capacity), Platform (environment), and Software (application software's).according to which Cloud Computing service models are named Infrastructure As A Service (IAAS), Platform As A Service, Software As A Service. According to the maker, broker, users Cloud is categorized as Privet, Public, Hybrid cloud, Privet cloud is a cloud used made by a person or organization for self-use only, Public cloud is a type of cloud where complete infrastructure is for all users. Like a mail and social site. A hybrid cloud is a cloud that is partially used by self and partial for the user.

1.1 Data Security, Algorithms & Cryptography:

Digital data can be secure by basically 3 ways password protection & Transform into non-understandable format & both password Protection transformation into non-readable format for unauthorized user. Step by step instruction & blue print of Process to secure the data know as algorithm, and process of transform the original data into secured data (non-accessible, non-readable format) & back to its original form for authorized user know as Cryptography.

Hash, Symmetric key, Asymmetric key cryptography is 3 basic types of the cryptography. DES, AES & RSA are well known & basic famous cryptography Algorithms.

So the Quotations arise why world need new cryptography algorithms? Because cryptography as famous as among users it also big Challenge among the Hackers. They develop ways to break it. Somewhere they are successes therefore Cloud technology need to develop and upgrade security systems. This technique proposing new Crypto Cloud Multilayer Blowfish DNA Technique (CCMBDNA).it is inspired by biological information store system in living beings DNA & traditional cryptography Blowfish algorithm previous research scholars work [1,2,3] and Conclusions in section 5 & 6.

1.2 Related Work

This work describes in [sec.3] it based on DNA and blowfish encryption techniques to encrypt original data, and then upload it to Google drive. In this paper text file only used as data set but it suggested a work plan using other data and multi-level encryption algorithms to improve cloud security. Using new code which is free from the dictionary, vowels consonants & usual words. You can use periodic tables, color code to develop and on different media or multimedia.

2. SECURITY ASPECT CLOUD COMPUTING
There are 3 expectations from the Algorithm

1. **Availability:** information avails for an Authorized person effectively.
2. **Confidentiality:** Other than authorized person information should not be accessible.
3. **Integrity**: intruder & unauthorized person must not be altering information.

The cloud and Data Encryption

In this proposed technique CCMBDNA, data is encrypted before storing in the cloud. In this technique, the data is stored securely in the cloud. Many encryption algorithms were used to provide security for the data of cloud users [1]. the aim of this technique is to protect data from unauthorized users & advantaged threats.

2.1 Encryption Algorithms' Used

- DNA

Since 1994, the computational properties of DNA have become an area of Research of cryptography. More recently, encryption using DNA computing has been considered a promising new field of encryption. So the past few years shows the increased use of DNA computing because of its suitable advantage for encryption [1].

- Blowfish

Blowfish is a symmetric encryption technique it takes key size from 32 bits to 448 bits and uses a similar key both for encryption and decryption. This technique securing data was

developed by Bruce Schneier in 1993. It contains 16 rounds & each round comprises an XOR operation & has encryption and key expansion technique [2].

3. CCMBDNA TECHNIQUE

Could computing provide large data storage to their users for storing data to the cloud so they can access it from anywhere? Here this technique provides security to data. As discus in part [1.1] it is much more secure effective against dictionary attack, brute force technique & Updated processing power. [1]

In this paper CCMBDNA are proposed different encryption strategy for the cloud sensitive data security. User first encrypts their data using CCMBDNA then uploads it to the web based cloud. In CCMBDNA using 2 encryptions of the original data first apply DNA encryption technique then blowfish algorithm. Pictorial Representation of CCMBDNA is given below.

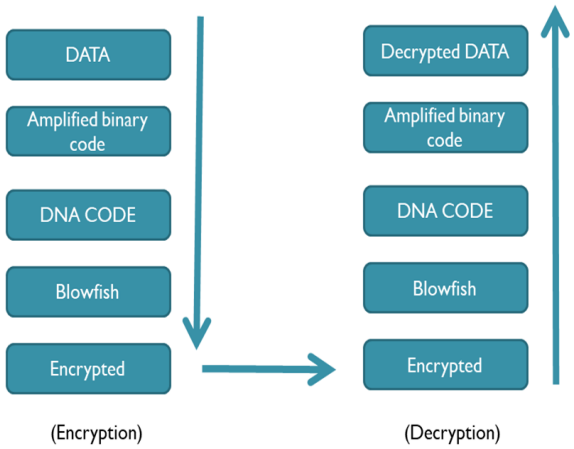

Fig 1. CCMBDNA Encryption & Decryption

4. PERFORMANCE & COMPARISON

The following parameters were used by different file size to determine the time needed to encrypt & decrypt data file table (1).

Table 1. DNAES Vs CCMBDNA Encryption & Decryption Performance.

File Name	File Size	Encryption Decryption DNAES time in Seconds	Encryption Decryption CCMBDNA time in Seconds
Input1.txt	1KB	2	1.4
Input2.txt	5KB	13	1.7
Input3.txt	15KB	30	3
Input4.txt	25KB	43	5.454
Input5.txt	50KB	77	17

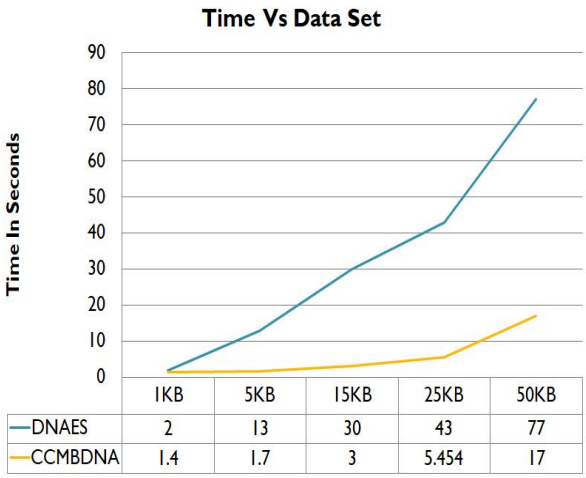

Fig 2. CCMBDNA Encryption & Decryption Performance Graph.

- CCMBDNA Technique has advantage Strength.
- The data sent to the cloud has been encrypted from the source to the destination.
- CCMBDNA Scheme is based on Blowfish Algorithm which characterized by Strength, Confidentiality and Simplicity & has not been broken so far.
- Enhance Security by change the key frequency.

5. CONCLUSIONS

Most cloud computing user has fear about their data. Is it safe on internet? What happened if it is hacked? Or company used and accesses their confidential data. But after using this technique user can be sure that except authorized person no one can understand data. After all information is also a property of user though may be it is photo graph, letters, vacations video etc. it is safe. User can use cloud computing without fear. Here the company & user both are satisfied on their end. Because key can be manage at the user end encryption and decryption at user end. Cloud owner also does not need bulk data processing. At their end not need to store key. It is also a research point improve on exception cases like user forget password. But in this paper it is clear that above performance we conclude that it is much better version of multi level encryption technique with DNA cryptography. As compared to AES- DNA (DNES), blowfish DNA (CCMBDNA) is much faster. It has simple processing. According to User computer it is better option to adapt it.

6. REFERENCES

[1] "New Secure Encryption Technique for Cloud Computin g" Nadia MD ; Najla 2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA) Year: 2019 | Conference Paper | Publisher: IEEE.

[2] "Implementation of DNA cryptography in cloud computi ng and using socket programming",Prajapati Ashishkumar B. ; Prajapati Barkha ,2016 International Conference on Computer Communication and Informatics (ICCCI) Year: 2016 | Conference Paper | Publisher: IEEE

[3] "A novel DNA sequence dictionary method for securing data in DNA using spiral approach and framework of DNA cryptography" ,Shipra Jain ; Vishal Bhatnagar

,2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014) Year: 2014 | Conference Paper | Publisher: IEEE.

[4] "DNA Sequence Based Medical Image Encryption Sche me"Jan Sher Khan ; Jawad Ahmad ; Saadullah Farooq Abbasi ; Arshad ; Sema Koc Kayhan 2018 10th Computer Science and Electronic Engineering (CEEC) Year: 2018 | Conference Paper | Publisher: IEEE.

[5] "An efficient implementation of SHA processor includin g three hash algorithms (SHA-512, SHA-512/224, SHA-512/256)" Sang-Hyun Lee ; Kyung-Wook Shin 2018 International Conference on Electronics, Information, and Communication (ICEIC) Year: 2018 | Conference Paper | Publisher:IEEE.

[6] "An efficient implementation of SHA processor includin g three hash algorithms (SHA-512, SHA-512/224, SHA-512/256)" Sang-Hyun Lee ; Kyung-Wook Shin2018 International Conference on Electronics, Information, and Communication (ICEIC)Year: 2018 | Conference Paper | Publisher: IEEE

[7] "Avoiding Data Replication in Cloud Using SHA-2"R. Raju ; S. Aravind Kumar ; R. Manikandan 2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC) Year: 2018 | Conference Paper | Publisher: IEEE

[8] "Failure Management for Reliable Cloud Computing: A Taxonomy, Model, and Future Directions" Sukhpal Singh Gill ; Rajkumar Buyya Computing in Science & Engineering Year: 2020 | Volume: 22, Issue: 3 | Magazine Article | Publisher: IEEE

[9] Modified AES using Dynamic S-Box and DNA Cryptography Y. Bhavani ; Sai Srikar Puppala ; B.Jaya Krishna ; Srija Madarapu 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) Year: 2019 | Conference Paper | Publisher: IEEE.

[10] A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem Md. Rafiul Biswas ; Kazi Md. Rokibul Alam ; Ali Akber ; Yasuhiko Morimoto 2017 4th International Conference on Networking, Systems and Security (NSysS) Year: 2017 | Conference Paper | Publisher: IEEE.