Securing Cloud Data by DNA Cryptography

Bindu V S, S Heyshanthinipandiyakumari

Mtech Cse, Nhce, Vtu University, Banglore, India

vsbindu23@gmil.com

Asst. Professor, Cse, Nhce, Banglore, India

shanthininhce@gmail.com

***Abstract*— Collection of various node in an area accomplishes a network. Networks of networks is said to be internet. Cloud helps in accessing data from anywhere at any time. It gives services like software as a service, infrastructure as a service, platform as a service. Various companies are competing in today's world and are providing free access for users on cloud. When requirement like more space is required and privacy to data stored, security to data stored in these cases cloud services are provided for payed ones. Due to data securityissues as the data placed on the cloud services provider's servers. To solve this issue various approach came into picture and this is one of new approach that is securing data by DNA cryptography method. In this we do encrypt data using advanced bi-directional encryption algorithm and then decrypt too**

***Keywords*— Cloud computing, Cloud data security, DNA digital coding, Bi-Directional DNA Encryption Algorithm, binary to DNA digital coding.**

I.INTRODUCTION

Cloud has a connectivity to various data servers where in it creates an environment where it can connect them. Finally finds a way to extract results from all of them and provide service to the user. We do have different types of clouds like public cloud, private cloud and hybrid cloud. In Public cloudwe have to pay and access.In private cloud, the computing service is distributed for particular society. In Hybrid cloud, the computing services is used by both private cloud service and public cloud service.

Cloud computing has three types of services. Software as a Service (SaaS),Software as a Service, also branded as cloud application services, symbolise the commonly used option for commerce in the cloud market. SaaS makes use of the internet facility to provide facilities to the user, which there forth manipulated by the third party person. Here it allows the user to make use the applications that are developed using service providers. Most of the SaaS applications are run directly over the web browser, and don't consider any downloads or installations on theend of client side.SaaS provides plenty of advantages to professionals, employees and corporate people to greatly reduce the time and money spent on monotonous tasks like downloading, installing, managing, and upgrading software.

By this technical team can spend time with pressing matters and other issues in the organization.Platform as a Service (PaaS), which provides Cloud platform services is meant for cloud components to certain software while being used mainly for applications. PaaS provides a framework for Building the customized applications. Not bothering about the size occupied by the company in developing and storing the new application and their services, there are several advantages for using PaaS as its information is stored in one part of cloud it can discloses the work done.Makes the development and deployment of apps simple and cost-effective, Scalable, Highly available services, Gives developers the ability to create customized apps without the headache of maintaining the software, Greatly reduces the amount of coding done,Allows easy transversal to the hybrid model,ensures the privacy to the confidentially developed application.

The third service of the cloud is Infrastructure as a Service (IaaS), Cloud infrastructure services, known as Infrastructure as a Service IaaS, are made of highly scalable and automated compute resources. It provides facilities to deploy and run the isolated software which include operating system and other applications. IaaS provides fully self-service for retrieving and monitoring things like compute, networking, storage, and other services, and it allows businesses to purchase resources on-demand and as-needed instead of having to buy hardware outright. The services offered by this delivery models are load balancing, web services, virtual instances, server hosting services, storage, connect with computer hardware, internet access and bandwidth provisions.

II. LITERATURE SURVEY

In cloud computing the major issue is to provide the security of data. In Cloud computing data security is prepared by the Authentication, Encryption & Decryption, Message authentication code, Hash function, and Digital signature and so on. So here we discuss about some security problems and their solutions.

A. Encryption Based On The Concept Of DNA

This technique is mainly used to safeguard the confidentiality of data that is present within the cloud which is the stored data in cloud. Encryption refers to the suppression of information that is converting the plain text to the cyper text A paper by Prajapati has discusses about an algorithm which will convert original text to cipher text by usage of DNA code.

In the genetic build up of an organisms it is found that DNA which is the building block is made of the nucleotides Adenines, Thymine, Cytosine and Guanines. These are represented in small notations as A, T, G, and C respectively. By this type of encryption method text data can be easily covered. The algorithm goes through a series of stages to undergo this conversion and accordingly makes use of a opposite series of steps to decrypt the data.

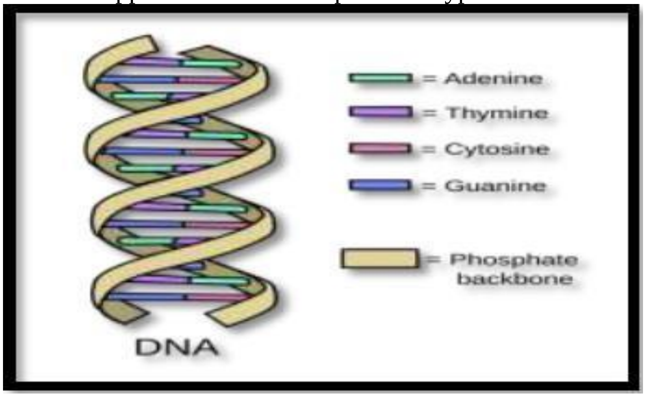


Fig1- DNA

B. *Combination of Diffie Hellman and ECC techniques*

This procedure has been suggested by Neha and in which the use of Diffie Hellman is made which is popular in use of general networking areas. The new user has to create an account which going authenticate the person in prospect.

From the next time the person tries to log in the server checks the Diffie Hellman version of the user's identity. On verification user is granted access. Then further if follows the procedure sand uses elliptic curve cryptography.

III. METHODOLOGY

The main aim is to secure the data present in the cloud. This can be done by DNA cryptographic method. The data when entering into the cloud will be of alphanumeric type. In later stage while entering this can be encrypted using the Bi-serial DNA encryption method which provides two layer security. Which we are improvising it to the three layer data security.

By this method of encryption the data when accessed also cant be known as it provides the high level of security. Then the data is stored in the cloud without any tautness. When the user is in need to retrieve the data the decryption process occurs any the plain text is retrieved. The several procedures that occur in bi-serial encryption is given how exactly the conversion takes place is mentioned step by step in below diagram.

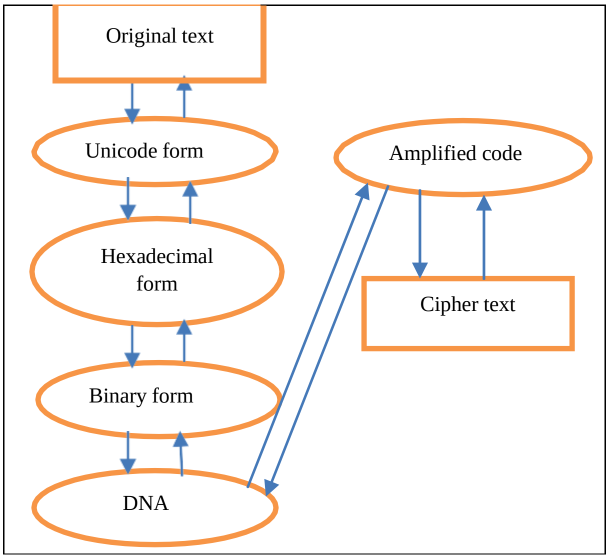


Fig2: Data Flow

A. *DNA To Digital Coding*

As we know DNA means di-oxy ribonucleic acid. It is a molecule which is composed of two chains that coil around each other to form a double helical structure. Which carries the genetic information. This has four nucleotides namely adenine, guanine, thymine, cytosine. The helical structure of DNA is given in figure 1.

This can be mapped to the binary form which consists of two states 0 and 1. DNAdigital coding can be encoded by four kind of base. Those are ADENINE (A) and THYMINE (T) orCYTOSINE (C) and GUANINE (G). The possible combination are 4!=24 pattern by encoding format like [0123/ATGC].

TABLE 1.
DNA DIGITAL CODING

Binary value	DNA digital coding
00	A
01	T
10	G
11	C

B. *Key Combination*

Keys are taken and represented by using nucleotides. Each and every bit is combined with all such combinations. The initial values are taken as two bits like A=00, T=01, G=10, and C=11 and by using these combinations generate and give numbering respectively as given intable. This can be done by using Diffie Hellman key sharing algorithm.in this the key and the value will be randomly changed.

TABLE 2:
KEY COMBINATION

Key Combination	Patterns	Values
AA	0101	5
AT	0011	3
AG	0001	1
AC	0010	1
TA	0110	6
TT	1111	15
TG	0111	7
TC	1001	9
GA	1010	10
GT	0100	4
GG	1000	8
GC	1100	12
CA	1110	14
CT	1011	11

CG	0000	0
CC	1101	13

B. Encryption Procedure

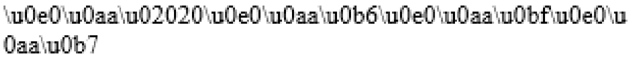
To perform the encryption process we follow the steps before it we need to take input – h as the plain text and then perform the encryption operation.

The Plaintext**:** Hello technoarete
Plain text – is the text before the encryption which is in human readable format.

Unicode uses hexadecimal to express a character.its a unique code in java to express all text elements. The Unicode for the following input is
Unicode**:-**àª†àª¶àª¿àª·

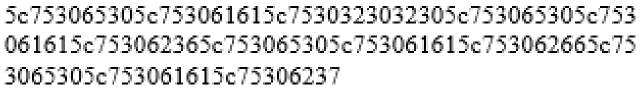
ASCII is the American standard code for information interchange. Which is the character encoding standard for electronic communications. The ASCII value for the following Unicode is

The ASCII value:



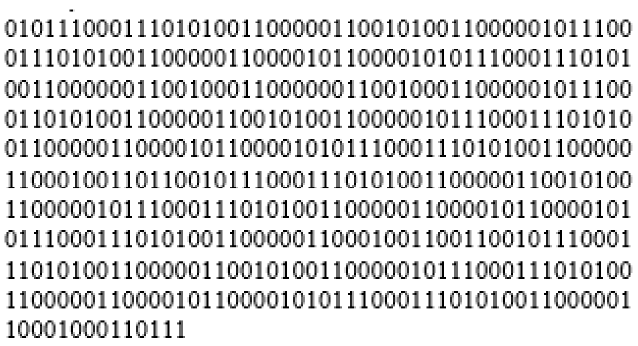
\u0e0\u0aa\u02020\u0e0\u0aa\u0b6\u0e0\u0aa\u0bf\u0e0\u0aa\u0b7

Hexadecimal is the positional numeral system with radix that is base of 16. The hexadecimal value for the ASCII code is
The Hexadecimal value:



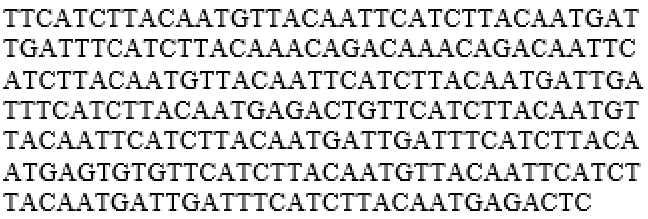
```
5c753065305c753061615c7530323032305c753065305c753
061615c753062365c753065305c753061615c753062665c75
3065305c753061615c75306237
```

The base 2 numerical system is the positional notation with radix 2 which has two universal values 0 and 1. The binary value for the hexadecimal value is
The Binary value:



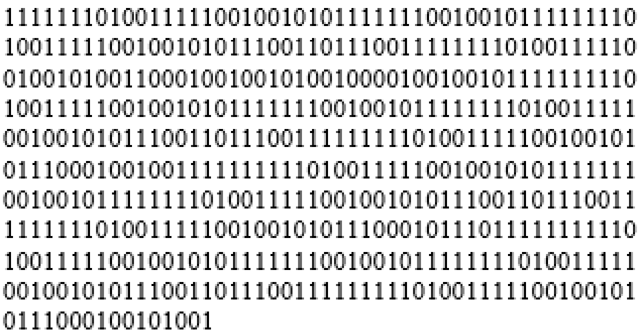
```
010111000111010100110000011001010011000001011100
011101010011000001100001011000010101110001110101
001100000011001000110000001100100011000001011100
011010100110000011001010011000001011100011101010
011000001100001011000010101110001110101001100000
110001001101100101110001110101001100000110010100
110000010111000111010100110000011000010110000101
011100011101010011000001100010011001100101110001
110101001100000110010100110000010111000111010100
110000011000010110000101011100011101010011000001
10001000110111
```

Using the key combinations the elements from the nucleotides are combined with the digital values.
DNA Digital coding:



```
TTCATCTTACAATGTTACAATTCATCTTACAATGAT
TGATTTCATCTTACAAACAGACAAACAGACAATTC
ATCTTACAATGTTACAATTCATCTTACAATGATTGA
TTTCATCTTACAATGAGACTGTTCATCTTACAATGT
TACAATTCATCTTACAATGATTGATTTCATCTTACA
ATGAGTGTGTTCATCTTACAATGTTACAATTCATCT
TACAATGATTGATTTCATCTTACAATGAGACTC
```

The Amplified Message:
From the key combination we can generate amplified message



```
111111101001111100100101011111111001001011111110
100111110010010101110011011100111111110100111110
010010100110001001001010010000100100101111111110
100111110010010101111111100100101111111101001111
001001010111001101110011111111101001111100100101
011100010010011111111110100111110010010101111111
001001011111111010011111001001010111001101110011
111111101001111100100101011100010111011111111110
100111110010010101111111100100101111111101001111
001001010111001101110011111111101001111100100101
0111000100101001
```

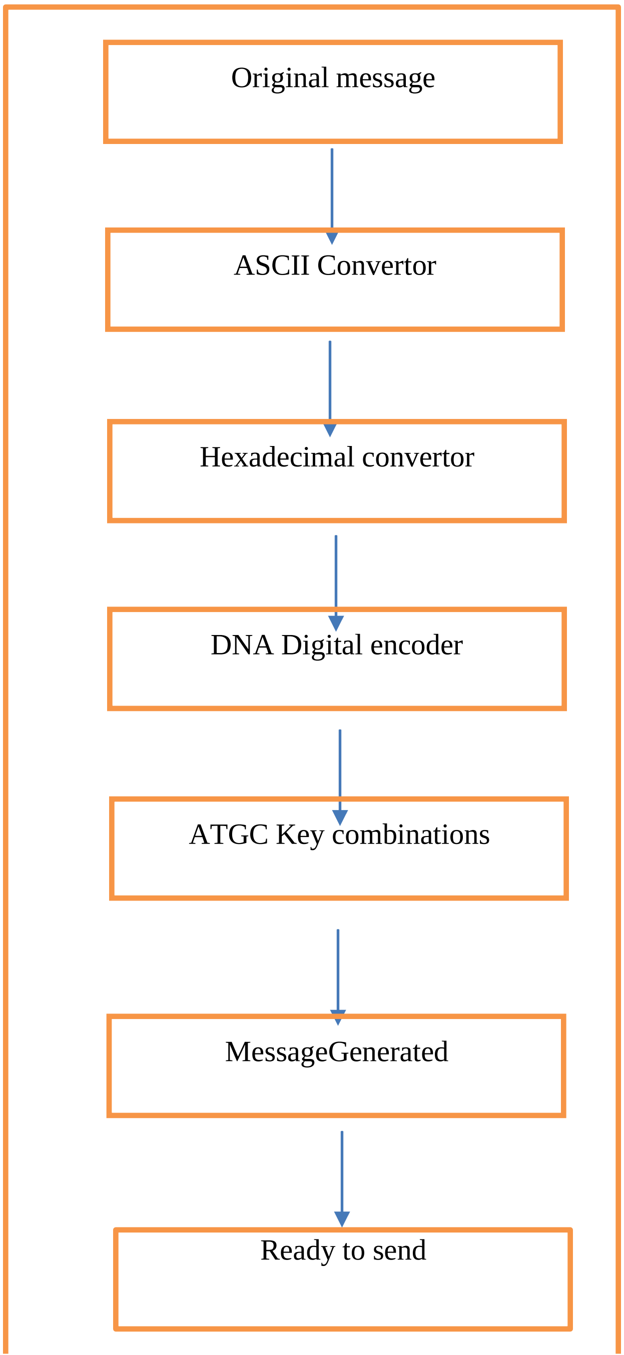


Fig3: Encryption process

C. *Decryption Procedure*

At receiver side, the receiver will get the amplifiedMessage, the ATGC key for decryption

The Amplified Message:
The output of the encryption process results the amplified message which goes as follows

```
1111111010011111001001010111111100100101111111110
1001111100100101011100110111001111111110100111110
0100101001100010010010100100001001001011111111110
1001111100100101011111110010010111111111010011111
0010010101110011011100111111111010011111100100101
0111000100100111111111110100111110010010101111111
0010010111111111010011111001001010111001101110011
1111111010011111001001010111000101110111111111110
1001111100100101011111110010010111111111010011111
0010010101110011011100111111111010011111100100101
0111000100101001
```

Using ATGC key combination, the retrival original DNA Digital code.

The DNA Digital code:

```
TTCATCTTACAATGTTACAATTCATCTTACAATGAT
TGATTTCATCTTACAAACAGACAAACAGACAATTC
ATCTTACAATGTTACAATTCATCTTACAATGATTGA
TTTCATCTTACAATGAGACTGTTCATCTTACAATGT
TACAATTCATCTTACAATGATTGATTTCATCTTACA
ATGAGTGTGTTCATCTTACAATGTTACAATTCATCT
TACAATGATTGATTTCATCTTACAATGAGACTC
```

From the table of DNA digital coding we can generate.

The Binary value:

```
0101110001110101001100000110010100110000001011100
0111010100110000011000010110000101011100011101 01
0011000000110010001100000011001000110000001011100
0111010100110000011001010011000000101110001110101
0011000000110000101100001010111000111010100110000
0110001000110110010111000111010100110000001100101
0011000000101110001110101001100000110000101100001
0101110001110101001100000110001001100110010111 00
0111010100110000011001010011000000101110001110101
0011000000110000101100001010111000111010100110000
0110001000110111
```

The Hexadecimal value:

```
5c753065305c753061615c7530323032305c753065305c753
061615c753062365c753065305c753061615c753062665c75
3065305c753061615c75306237
```

The ASCII value:

```
\u0e0\u0aa\u02020\u0e0\u0aa\u0b6\u0e0\u0aa\u0bf\u0e0\u
0aa\u0b7
```

Unicode:àª†àª¶àª¿àª·

Plaintext:Hello technoarete
Finally after the decryption process the plain text is obtained. Hence by this process the data in the cloud is secured.

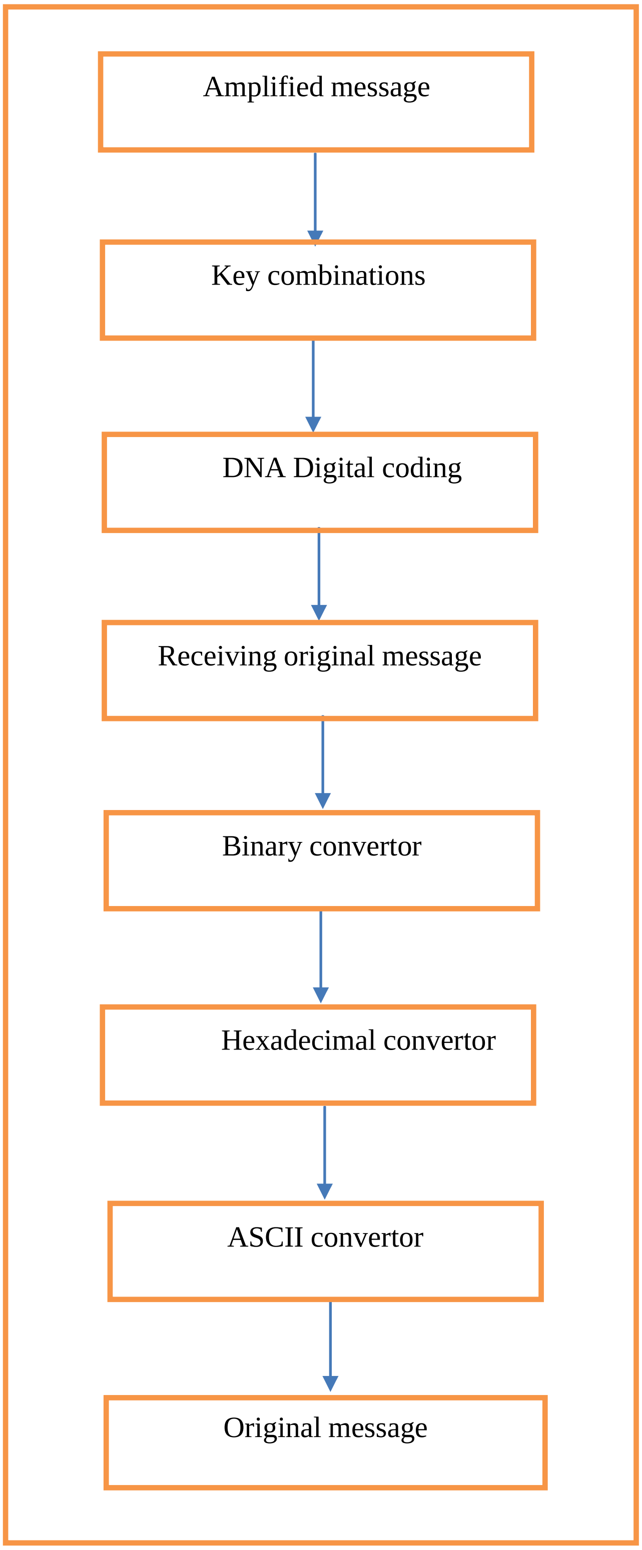


Fig 4:Decryption process

VI. Conclusion

Securing the data present in the cloud is one of the main challenging issue. This was overcome by proposing variety of algorithms like RSA, Diffie-Hellman, DNA encryption. In this we have brought the method of securing the data in cloud by extending the bi directional encryption algorithm which is providing 2 layer security for the ASCII character set.

Original data to Unicode and later the role of others is taken place. The future work will focus on the possible attacks and cryptanalysis of the cipher text and measure its strength.

References

[1] PrashantRewagad, YogitaPawar, ―Use of Digital Signature with Diffie-Hellman Key Exchange and AES Encryption Algorithm to EnhanceData Security in Cloud Computing‖ 2013 International Conference onCommunication System and Network Technologies (IEEE ComputerSociety).

[2] Uma Somani, Kanika Lakhani, ManishaMundra, ‖ImplementingDigital Signature with RSA Encryption Algorithm to Enhance the DataSecurity of Cloud in Cloud Computing‖-2010 IEEE 1st InternationalConference on Parallel, Distributed and Grid Computing (PDGC-2010).

[3] Mehdi Hojabri& Mona Heidari―Union of RSA algorithm, DigitalSignature and KERBEROS in Cloud Computing‖ InternationalConference on Software Technology and Computer Engineering(STACE-2012).

[4] Ashish Prajapati, Amit Rathod ―Enhancing security in cloud computingusing Bi-Directional DNA Encryption Algorithm‖, InternationalConference on Intelligent Computing, Communication & Devices.(ICCD-2014), Springer.