Implementation of "BDEA-A DNA cryptography" for securing data in cloud

Hema N[1] **Sonali Ulhas Kadwadkar[2]**

[1]*Assistant Professor, Dept of Information Science Engineering, RNSIT Bangalore, Karnataka, India*

[2]*Student, M.Tech in Computer Networks and Engineeriing, RNSIT Bangalore, Karnataka, India*

ABSTRACT

Distributed computing is one of the latest technologies which are used in cloud computing. It provides many services such as online and on-demand storage, services on network, platform services and etc. The data security is one of the main issues so that many organizations are unenthusiastic to use services in the cloud as the data resides on cloud services provider's servers. To address this issue, there have been several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The socket programming is used for strengthen security, it provides mechanism to communicate between two computers using TCP. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters.

Keywords:- *Cloud computing, Data security issues, Bi-Directional DNA Encryption Algorithm, DNA digital code, Socket Programming*.

1. INTRODUCTION

Cloud computing is very popular and has recently developed into a major trend in IT as it has vast amount of storage. It is based on internet and distributed computing which provides the resources to be shared among different computers on demand. It has capability to store and process the data either in private owned data center or third party data center. The cloud models are private, public and hybrid. Pay per use model is used in public cloud. In private cloud, the service is used for single society. In Hybrid cloud, the computing services is used both by private cloud and public cloud service. Cloud computing has three types of services. Software as a Service (SaaS), in which one service is run on a single cloud, then multiple users access this service as per on demand. Platform as a Service (PaaS), in which, it provides the platform to creates and maintains the application. Infrastructure as a Service (IaaS), it provides the data storage, rent storage, Network capacity,Data centers etc. It is also known as Hardware as a Service (HaaS).

Cloud computing security has set of technologies, policies which controls, protect the applications. The storage in cloud will be processed in thirty-party data center. SaaS,PaaS and IaaS service models provides capabilities to store, process and maintain the security of data. The security is main concern in the cloud computing the issued will be faced by either cloud providers (organizations using software, infrastructure and platform-as-a-service via cloud) and security issued faced by users(companies or organizations which store data in cloud). The infrastructure of the cloud should be secured by the providers so the client's data will be protected. The users should ensure the security of the cloud by giving the strong password to login in the cloud and use some algorithm for encrypting the data in the cloud.

Privacy and the security should be maintained in cloud computing. In cloud computing the major issue is to provide the security of data. The data stored in cloud is unenthusiastic to use cloud services due to data security issue. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques which increase the security in the cloud[1].

The Bi-directional DNA Encryption Algorithm (BDEA) provides two level securities. Firstly it provides DNA digital coding In information science, the binary digital coding encoded by two state 0 or 1 and a combination of 0 and 1. But DNA digital coding can be encoded by four kind of base as That is ADENINE (A) and THYMINE

(T) or CYTOSINE (C) and GUANINE (G). Second is key combination 16 possible key combination is produced out of 4 bases[1].

ARCHITECTURE

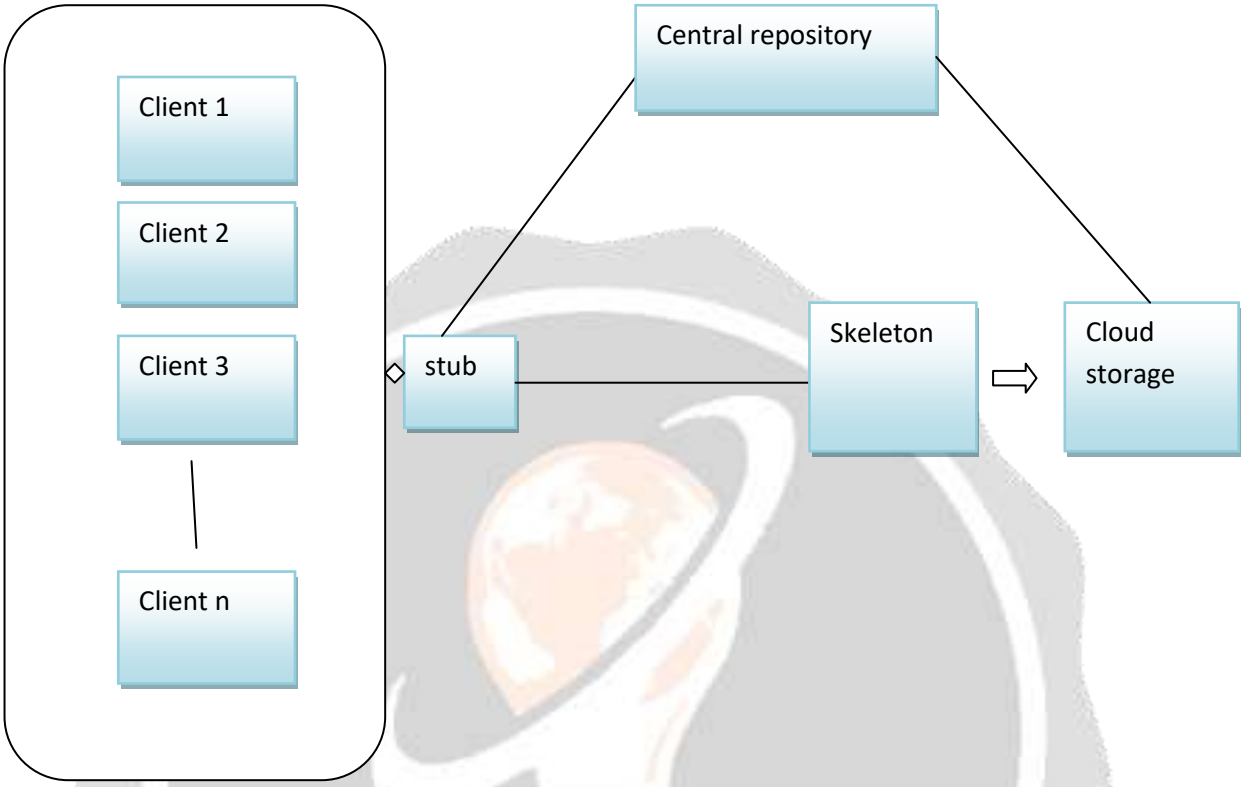

Fig-1: Architecture of BDEA

The architecture consists of one or more of clients the entry point of the client is the stub and the server side is skeleton. RMI uses a standard mechanism (employed in RPC systems) for communicating with remote objects*: stubs* and *skeletons*. A stub for a remote object acts as a client's local representative or proxy for the remote object. The caller invokes a method on the local stub which is responsible for carrying out the method call on the remote object. In RMI, a stub for a remote object implements the same set of remote interfaces that a remote object implements.

The central repository contains all the keys for the message which is stored in the cloud. The stub will store all the keys in the central repository and that can be easily accessed by the cloud storage and the skeleton is the entry point of the server or the client which is used. The data in the client will be stored in the cloud storage in the encrypted form by the central repository which stores all the keys of the message stored.

2. PROPOSED WORK

The Bi-serial DNA encryption algorithm is performing, that providing the two level of security
.

DNA DIGITAL CODING In information science, the binary digital coding encoded by two state 0 or 1 and a combination of 0 and 1. But DNA digital coding can be encoded by four kind of base as shown in Table 1. That is ADENINE (A) and THYMINE (T) or CYTOSINE (C) and GUANINE (G). There are possibly 4! =24 pattern by encoding format like (0123/ATGC).

Table-1: DNA Digital Coding

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

Key Combination: Here in key combination ATCG is the key which will be stored in the central repository. Every bithave 2 bits like A=00, T=01, G=10, and C=11 and by using ATGC, key combinations is generated and give numbering respectively that is given into table 4.1. From the Table 2, we can generate 64 bit key values and adding ATGC, we can generate 72-bit key (64 bits of key combination and 8 bits of ATGC). ATGC key is sending to the receiver side.

Table-2: Key Combination

KEYCOMBINATION	**PATTERNS**	**VALUES**
AA	0101	5
AT	0011	3
AG	0001	1
AC	0010	2
TA	0110	16
TT	1111	15
TG	0111	7
TC	1001	9
GA	1010	10
GT	0100	4
GG	1000	8
GC	1110	12
CA	1011	14
CT	1010	11
CG	0000	0
CC	1101	13

Encryption Process : Message encryption is the process of transmitting the message stealthily. In the message encryption, the original message is transformed into an equivalent alternative by a definite encoding mechanism. This message is then send to the receiver. An encoding scheme by incorporating the important chemical characteristics of biological DNA (Deoxyribonucleic Acid) sequences or structure of purines and pyrimidines could serve as an effective stealth transmission of an message would be so secure that it could not be easily cracked.

A DNA sequence is a sequence composed of four distinct letters, A, C, G and T. Each nucleotide contains a phosphate attached to a sugar molecule (deoxyribose) and one of four bases, adenine (A), cytosine (C), guanine (G), or thymine (T). It is the arrangement of the bases in a sequence, for instance like ATTGCCAT, that determines the encoded gene. The natural sequence pattern with complementary coding and chemical classification of the nucleotides can be used to shield the message.

In the proposed algorithm, a DNA sequence or structure is initial randomly taken and complementary rules are framed so the secrete message to be sent is encoded at the sender's aspect. At the receiver's aspect, the decryption method is completed and therefore the original message is extracted out. Firstly in the encryption process that is the original message 16bit Unicode is converted in equivalent ASCII character that is combination of two 8bits message. Then the ASCII is converted into equivalent hexadecimal value by using hexadecimal convertor. This value will be converted into binary convertor after binary conversion message is split into 4 parts as shown in figure 3. Then all the parts will be formed to be the message then the DNA digital coding is done using the 4 base in a sequence, for instance like ATTGCCAT, that determines the encoded gene then the digital encoding is undergone through 16 key combinations. From this 16 key combinations the encrypted message is formed that message which is in encrypted form is ready to send. The message which is send is fully in the encrypted form the other unauthorized person cannot guess the original message which is to be send.

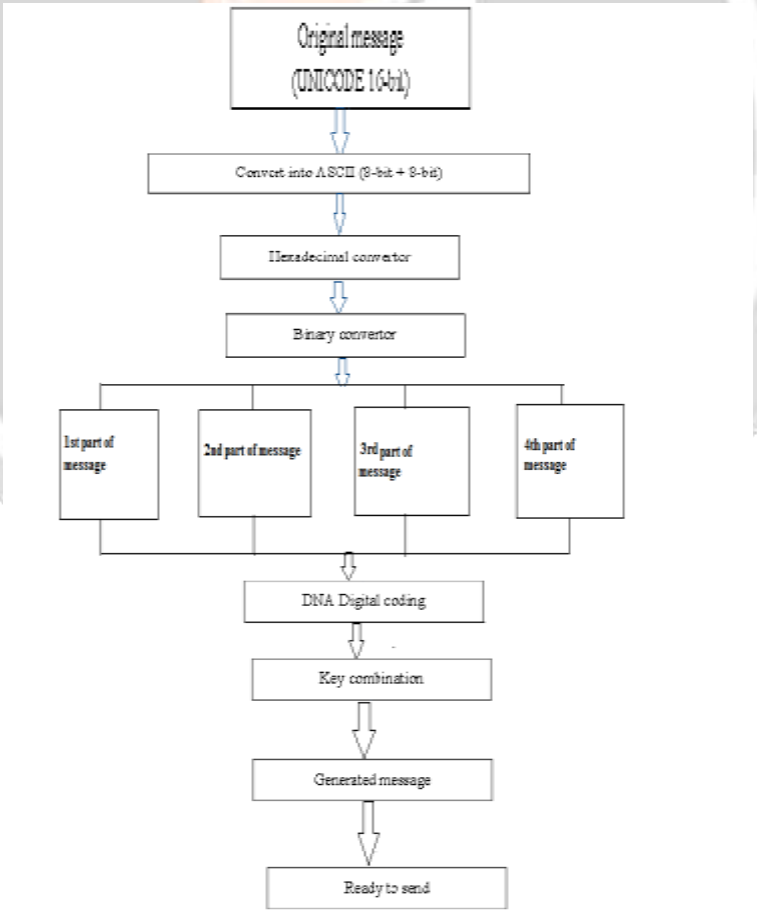

Fig-2: Encryption process

After the encryption process the file which is encrypted should be uploaded in the dropbox cloud. Dropbox cloud manages all the files and the images we can upload a file in dropbox and share it managing the file in the dropbox is easy. Dropbox is an awesome service. We can back your files up to the cloud, sync them between computers, and share them with your friends. Using Dropbox on your computer is just like using any other folder on your hard drive, except the files you drag into your Dropbox folder automatically sync online and to any other computers or mobile devices linked to your account. The app automatically watches your Dropbox folder and keeps your files in sync for you. After uploading the files in the cloud if we want to retrieve the data the key will be generated to get the file using that key. The decryption process is opposite of encryption process.

3. EXPERIMENTAL RESULTS

Fig-3: Uploading the file in dropbox cloud and applying dna algorithm

Fig-4: Listing the file uploaded in cloud, applying DNA decryption and entering the key

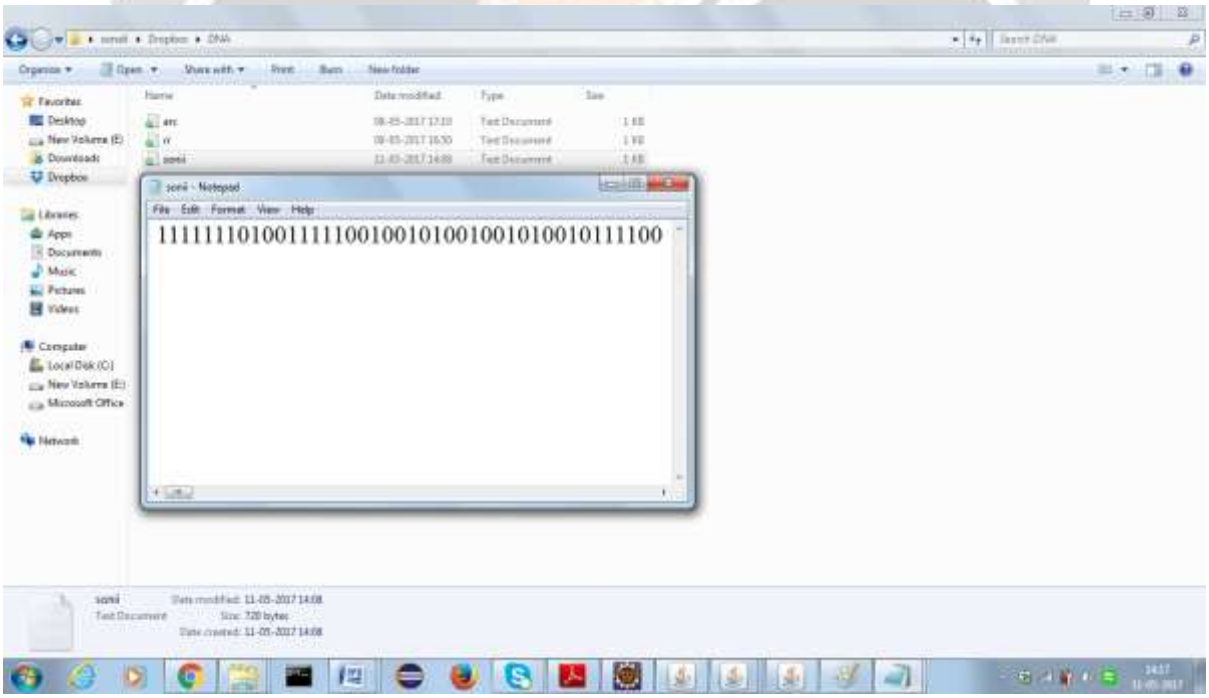

Fig-5: Dropbox cloud which has stored the files in encrypted form

Fig-6: Original text after decryption

4. CONCLUSION AND FUTURE SCOPE

Data security is the main challenge for cloud usability. Various algorithms like RSA, Diffie-Hellman, DNA encryption etc. are available to provide data security for the data stored on cloud. Digital signatures, Extensible Authentication Protocols are used for authentications. Using BDEA algorithm, achieve 2-layer security for ASCII character sets. The cloud used can be AWS or JAX-WS which increases the storage of the data of the users. The proposed system focuses on extending the BDEA algorithm to be used with Unicode character set. This can help reach to the wider community of the cloud users.

The future work will focus on the possible attacks and cryptanalysis of the cipher text and measure its strength and while sending the data or the image in the cloud we can compress the data or the image while sending so that the less memory data will be sent and the encryption process will be done fast and processing time will be fast. Even while decryption of data and image the processing time will be fast and the less memory will be utilised to save the data or the image.

5. RFFERENCES

[1]. Prajapati Ashishkumar B, Prajapati Barkha Implementation of dna cryptography in cloud computing and using socket programming 2016 International Conference on Communication System and Network Technologies (IEEE Computer Society).

[2] PrashantRewagad, YogitaPawar, "Use of Digital Signature with Diffie-Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing" 2013 International Conference on Communication System and Network Technologies (IEEE Computer Society).

[3] Tushar Mandge, Vijay Choudhary. "A DNA encryption technique based on matrix manipulation and secure key generation scheme". Information Communication and Embedded Systems (ICICES), International Conference on 21-22 Feb 2013.

[4] Olga Tornea, and Monica E. Borda, "Security and complexity of a DNA-based cipher," IEEE Roedunet International Conference (RoEduNet), 11th, pp. 1-5, 2013.

[5] Ashish Prajapati, Amit Rathod "Enhancing security in cloud computing using Bi-Directional DNA Encryption Algorithm", International Conference on Intelligent Computing, Communication & Devices. (ICCD-2014), Springer.