IMPLEMENTATION OF DNA CRYPTOGRAPHY IN CLOUD COMPUTING AND USING SOCKET PROGRAMMING

Priyanka agarwal[1], sachin sharma[2], Ritik sharma[3]

[1]Associate Professor, Dept. of ECE, Arya Institute of Engineering & Technology, Jaipur, Rajasthan, India
[2,3]Student, Dept. of ECE, Arya Institute of Engineering & Technology, Jaipur, Rajasthan, India

---

Abstract- *In the field of distributed computing Cloud computing is the latest technology which provides various online and on-demand services for data storage & network services and etc. lots of organizations are excited to use cloud services cause of data security problems as the data lives on the cloud services provider's servers. The BDEA (Bi-directional DNA Encryption Algorithm) is one of data security techniques. However, the presenting techniques eye on only for ASCII character set, ignoring the non-English user of the cloud computing*

Keywords-Cloud computing, Data security issues, Bi-DirectionalDNAEncryptionAlgorithm,DNAdigitalcode, SocketProgramming.)

1. INTRODUCTION

Cloud computing has newly reached status and developed into a chief trend in IT. We execute such a systematic analysis of cloud computing and explain the technical tasks facing in this paper. In Community cloudthe "Payper use" proto typical is used. In private cloud, the computing service is disseminated for a single culture. In Hybrid cloud, the computing services is expended both the private cloud service and public cloud service. Cloud computing has three types of services. Software as a Service (SaaS), in which client ready one service and run on a single cloud, then multiple customer can access this service as per on request. Platform as a Service (PaaS), in which, it delivers the platform to generate application and keeps the application. Infrastructure as a Service (IaaS), as per period suggest to delivers the data storage, Network size, rent storage, Data centers etc. It is a.k.a. Hardware as a Service (HaaS).

2. LiteratureSurvey

In cloud computing the main problem is to deliver the security of data. In Cloud computing data safety is arranged by the Authentication, Encryption & Decryption, Message authentication code, #function, and Digital signature and soon. So here we debate about some security difficulties and their answers.

Use of Digital Autograph with Diffie Hellman MainConversationandAESEncryptionAlgorithmtoEnhanceData Safety in Cloud Computing[1].

Mr.PrashantRewagad and Ms.YogitaPawar [1]. Here in this paper, the assistant using three way design protection patterns. Initially Diffie-Hellman algorithm misused to generate keys for key exchange step. Then digital signature is used for confirmation, there after AES encryption algorithm is cast off to encrypt or decrypt user's data file. Diffie- Hellman key exchange algorithm is vulnerable to main in the central round. The most thoughtful limitation is the lack of the authentication.

Grouping of RSA algorithm, Arithmetical Signature and Kerberos in Cloud Safety[2].

Mehdi Hoja briand Mona Heidari[2].Now in this rag, the researcher first completes the idea of Kerberos authentication services. At the next step the Validate Server (VS) of Kerberos do confirms users and created the permitgrantingticketandsessionkeyanditdirectedtotheusers. The next step users send the ticket granting ticket and session key to Ticket Granting Server (TGS) for receiving the facility. Then TGS send ticket and session key for operator. In last step the operators send the request service to cloud service supplier for using the cloud service and also cloud service, deliver service to users. After doing this step user can used the cloud facility worker. But for more safety they completed RSA algorithm for encryption & decryption and then they use Digital Signature for Verification.

ExecutionDigitalsignwithRSAEncryption algorithmtodeveloptheDatasecurityofcloudinCloud Computing [3].

Uma Somani, Kanika Lakhani, and Manish Mundra [3]. In this rag,, there are two creativities and B. An originality A has some data that are public data and creativity has public cloud. Now B wants some protected data from A's cloud. So RSA algorithm and Digital signature are used for safe communication. In this way, creativity A takes data from cloud, which B needs. Now the data or document is rumpled into little line using # code function that is called Message digest. Then A encodes the message digest inside private key the outcome is in the Digital signature method. Using RSA algorithm, A will encode the digital signed signature with B's public key and B will decode the code text to basic text with his private key and A's public key for confirmation of signature.

3. PROPOSEDSYSTEM

Earlier piece defines the study about the cloud computing, fundamentals of cloud computing and security problems happens in cloud. Then study certain papers to crack these safety problems. Here in this paper, the Bi-serial DNA encryption algorithm is execution, that giving the two level of safety.

DNA DIGITAL CODING

In info science, the binary digital encoding coded by two levels 0 or 1 and a mixture of 0 and 1. But DNA digital coding can be programmed by four types of base as shown in table 1. That is (A) ADENINE and (T) THYMINE or (C) CYTOSINE and (G) GUANINE. There are possibly 4! =24 outline by encoding setup like (0123/ATGC)[4].

Table 1.DNA Digital Coding

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

KEY COMBINATION

Now in this exertion, we are consuming ATGCasakey. Each bit have 2 bits like A=00, T=01, G=10, and C=11 and by consuming ATGC, key mixtures is produced and give numbering individuallythatisgivenintotable.Fromthetable2,wecan produce 64 bit key standards and adding ATGC, we can produce72-bitkey(64bitsofkeymixtureand8bitsof ATGC). ATGC key is transfer to the receiver side by using Diffie Hellman key allocation algorithm. In this work, whenever the key value will be arbitrarily transformed.

Table 2: Key combination

KEY COMBINATION	PATTERNS	VALUES
AA	0101	5
AT	0011	3
AG	0001	1
AC	0010	2
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

A. ENCRYPTIONPROCESS

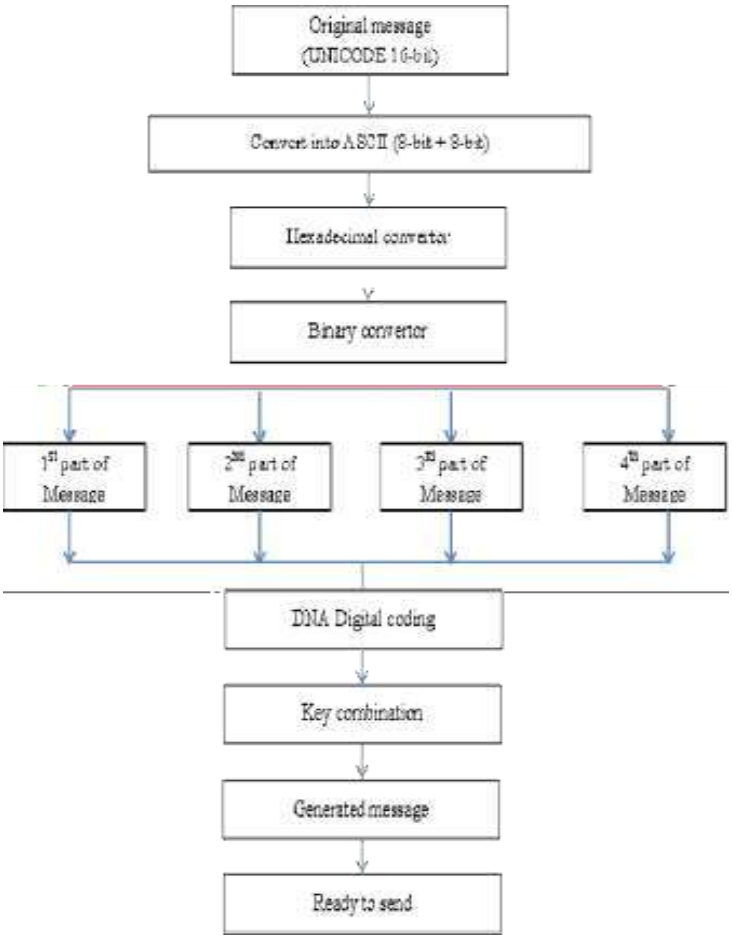

Fig 1: Encryption process

To know the scenario of projected work flow chart we reflect one sample. In this the sample plain text is "Hello Technocrete" and execution encryption operation

Plaintext:

Hello Technocrete

Unicode:

à³†à³¶à³¿à³·

ASCII:

\u0e0\u0aa\u02020\u0e0\u0aa\u0b6\u0e0\u0aa\u0bf\u0e0\u0a a\u0b7

Hexadecimal value:

5c753065305c753061615c7530323032305c753065305c

753061615c753062365c753065305c753061615c753062

665c753065305c753061615c7530623

Binary value:

0101110001110101001100000110010100110000010111 0

0011101010011000001100001011000010101110001110 1

0100110000001100100011000000110010001100000101 1

1000111010100110000011001010011000001011100011 1

0101001100000110000101100001010111000111010100 1

1000001100010001101100101110001110101001100000 1

1001010011000001011100011101010011000001100001 0

1100001010111000111010100110000011000100110011 0

0101110001110101001100000110010100110000010111 0

0011101010011000001100001011000010101110001110 1

0100110000011000100011 0111

DNA Digital coding:

From Table 1 we can write

TTCATCTTACAATGTTACAATTCATCTTACAATGATTGAT
TTCATCTTACAAACAGACAAACAGACAATTCATCTTACAATG
TTACAATTCATCTTACAATGATTGATTTCATCTTACAATGAG
ACTGTTCATCTTACAATGTTACAATTCATCTTACAATGAT
TGATTTCATCTTACAATGAGTGTGTTCATCTTACAATGTT
ACAATTCATCTTACAATGATTGATTTCATCTTACAATGAG
ACTC

Now from table 2, the amplified message is generated, Amplified Message

1111111010011111100100101011111110010010111111111

0100111110010010101110011011100111111010011111

0010010100110001001001010010000100100101111111 1

1010011111001001010111111100100101111111010011

1110010010101110011011100111111110100111110010

0101011100010010011111111110100111110010010101 1

1111100100101111111010011111001001010111001101 1

1001111111101001111100100101011100010111011111 1

1111010011111001001010111111100100101111111010

0111110010010101110011011100111111111010011111 0

0100101011100010010100

B. DECRYPTIONPROCESS

Now at receiver side, the receiver receives the amplified message and ATGC key for decryption.

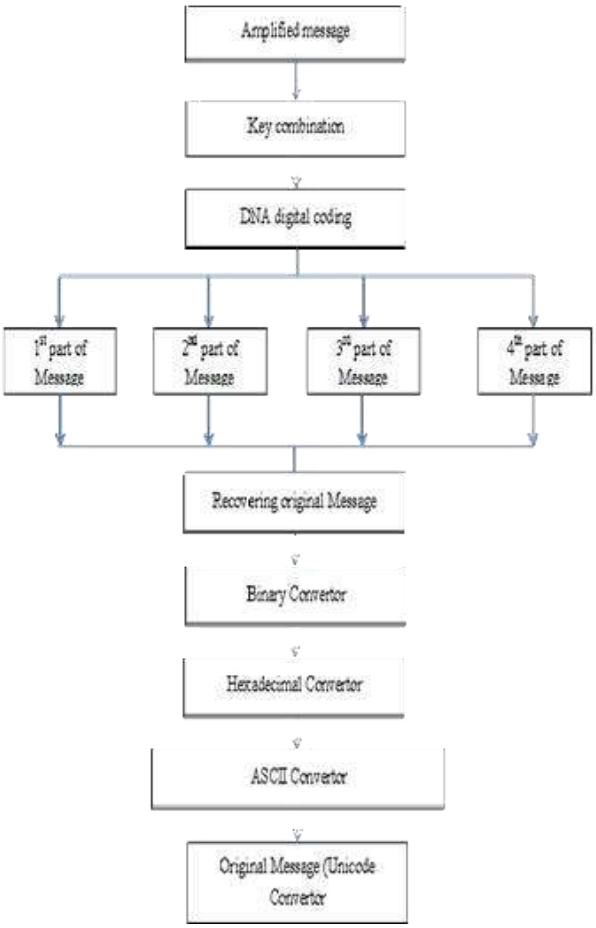

Fig: 2: Decryption process

Amplified Message

1111111010011111100100101011111110010010111111
1110100111111001001010111001101110011111111101
0011111001001010011000100100101001000010010 0
1011111111101001111100100101011111110010010 1
1111111010011111100100101011100110111001111 1
1110100111111001001001110001001001111111111 01
0011111001001010111111100100101111111101001 1
1110010010111100110111001111111110100111110 0
1001010111000101110111111111101001111100100 1
0101111111001001011111111010011111001001010 1
1001101110011111111101001111100100101011100 0
100101001

Now using ATGC key and key combination, retrieve original DNA Digital code.

TTCATCTTACAATGTTACAATTCATCTTACAATGATTGATT
TCATCTTACAAACAGACAAACAGACAATTCATCTTACAATG
TTACAATTCATCTTACAATGATTGATTTCATCACAATGAGAC
TGTTCATCTTACAATGTTACAATTCATCTTACAATGATTGAT
TTCATCTTACAATGAGTGTGTTCATCTTACAATGTTACAATTC
ATCTTACAATGATTGATTTCATCTTACAATGAGACTC

From the table of DNA digital coding we can generate.0101110001110101001100000110010100110000010110001110101001100000110000101100001010111000111010100110000001100100011000000110010001100000101110001110101001100000110010100110000010111000111010100110000011000010110000101011100011101010011000000110001000110110010111000111010100110000011001010011000000101110001110101001100000110000101100001010111000111010100110000011000100110011001011100011101010011000000110010100110000010

111000111010100110000011000010110000101011100011101010011000000110001000110111

Hexadecimal value:

5c753065305c753061615c7530323032305c753065305c75

3061615c753062365c753065305c753061615c753062665c

753065305c753061615c75306237

ASCII:

\u0e0\u0aa\u02020\u0e0\u0aa\u0b6\u0e0\u0aa\u0bf\u0e0\u0a a\u0b7

Unicode:

àª†àª¶àª¿àª·

Plaintext:

Hello Technocrat

4.SNAPS OF PROPOSED WORK(ENCRYPTION)

Fig. 3: Encryption operation

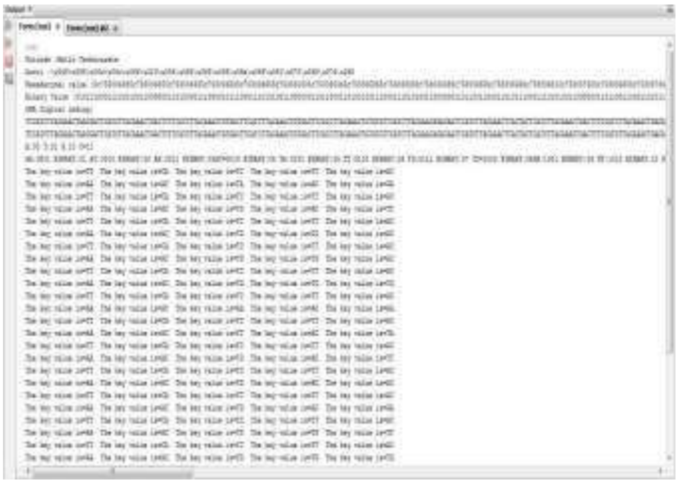

Fig.4: Encryption flow

5. SNAPS OF PROPOSED WORK(DECRYPTION)

Fig.5: Decryption Process

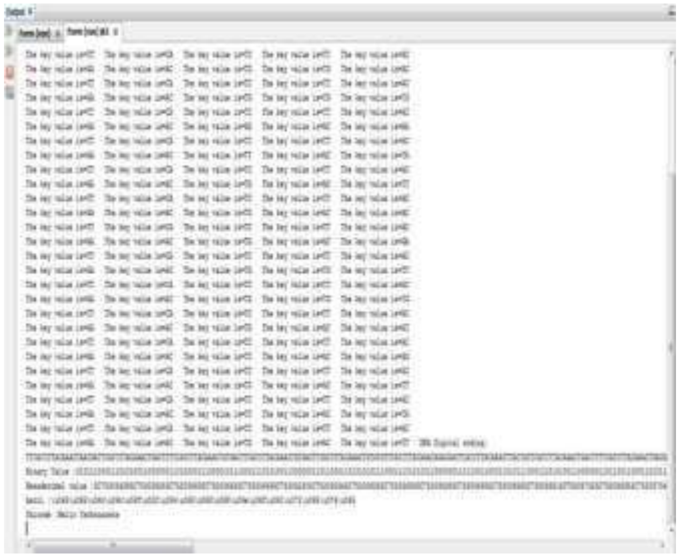

Fig.6: Decryption flow

WORKING ON AMAZON WEB SERVICE

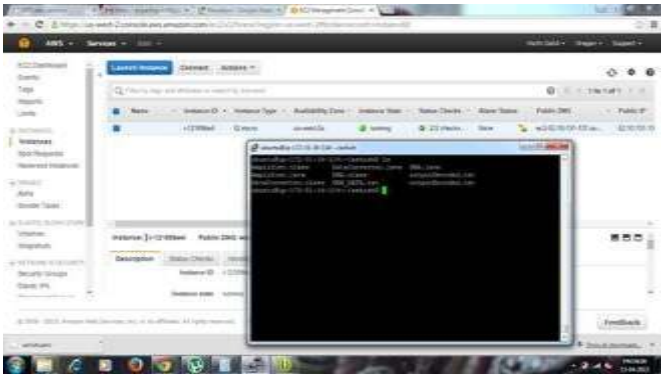

Fig.8: Encryption inAWS

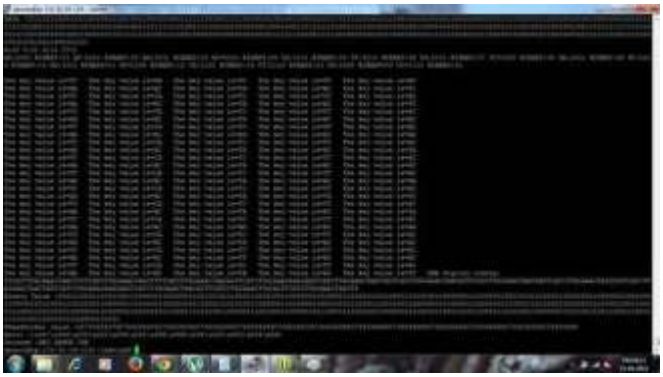

Fig.9: Decryption in AWS

6. CONCLUSION

Data safety is the important task for cloud usability. Various algorithms like RSA, Diffie-Hellman, DNA encoding etc. are obtainable to deliver data security for the data kept on cloud. Digital signatures, Extensible Verification Procedures are used for verifications. Using BDEA algorithm, we achieve 2-layer safety for ASCII character sets. The future system focuses on spreading the BDEA process to be used with Unicode personality set. This can help reach to the wider public of the cloud operators. The upcoming work will focus on the likely attacks and cryptanalysis of the cipher text and amount its asset.

REFERENCES

1. Prashant Rewagad, YogitaPawar, "Use of Digital Sign with Diffie-Hellman Key Exchange and AESEncryptionAlgorithmtoEnhanceDataSeftyinCloudComputing"2013global session on Communication System and Network Technologies (IEEE ComputerSociety).

2. Uma Somani, Kanika Lakhani, Manisha Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing"-2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC-2010).

3. Mehdi Hojabri& Mona Heidari "Merger of RSA algorithm, Digital Sign and KERBEROS in Cloud Computing" Global Session on Software Skill and Computer Engineering (STACE-2012).

4. 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.