IMPLEMENTATION OF DNA CRYPTOGRAPHY IN CLOUD COMPUTING AND USING SOCKET PROGRAMMING

Prajapati Ashishkumar B.
Assistant Professor,
Computer Engineering Department,
Babaria Institute of Technology,
Vadodara, India
er.ashishprajapati@gmail.com

Prajapati Barkha
Student,
Computer Engineering Department,
Sardar Vallabhbhai patel Institute of Technology,
Vasad, India
prajapatibarkha2629@gmail.com

***Abstract*—Cloud computing is the latest technology in the field of distributed computing. It provides various online and on-demand services for data storage, network services, platform services and etc. Many organizations are unenthusiastic to use cloud services due to data security issues as the data resides on the 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 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.

I. INTRODUCTION

Cloud computing has recently reached popularity and developed into a major trend in IT. We perform such a systematic review of cloud computing and explain the technical challenges facing in this paper. In Public cloud the "Pay per use" model is used. In private cloud, the computing service is distributed for a single society. In Hybrid cloud, the computing services is consumed both the private cloud service and public cloud service.Cloud computing has three types of services. Software as a Service (SaaS), in which customer prepared one service and run on a single cloud, then multiple consumer can access this service as per on demand. Platform as a Service (PaaS), in which, it provides the platform to create application and maintains the application. Infrastructure as a Service (IaaS), as per term suggest to provides the data storage, Network capacity, rent storage, Data centers etc. It is also known as Hardware as a Service (HaaS).

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.

Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing [1].

Mr.PrashantRewagad and Ms.YogitaPawar [1]. Here in this paper, the researcher using three way architecture protection schemes. Firstly Diffie-Hellman algorithm is used to generate keys for key exchange step. Then digital signature is used for authentication, thereafter AES encryption algorithm is used to encrypt or decrypt user's data file. Diffie- Hellman key exchange algorithm is vulnerable to main in the middle attack. The most serious limitation is the lack of the authentication.

Union of RSA algorithm, Digital Signature and Kerberos in Cloud Security [2].

Mehdi Hojabri and Mona Heidari [2]. Here in this paper, the researcher first performs the concept of Kerberos authentication services. At the next step the Authenticate Server (AS) of Kerberos do verifies users and created the ticket granting ticket and session key and it sent to the users. The next step users send the ticket granting ticket and session key to Ticket Granting Server (TGS) for getting the service. Then TGS send ticket and session key for user. In final step the users send the request service to cloud service provider for using the cloud service and also cloud service, provide

978-1-4673-6680-9/16/$31.00 ©2016 IEEE

service to users. After doing this step user can used the cloud service provider. But for more security they performed RSA algorithm for encryption & decryption and then they use Digital Signature for Authentication.

Implementation Digital signature with RSA Encryption algorithm to enhance the Data security of cloud in Cloud Computing [3].

Uma Somani, Kanika Lakhani, and Manish Mundra [3]. In this paper, there are two enterprises A and B. An enterprise A has some data that are public data and enterprise has public cloud. Now B wants some secure data from A's cloud. So RSA algorithm and Digital signature are used for secure communication. In this method, enterprise A takes data from cloud, which B wants. Now the data or document is crushed into little line using Hash code function that is called Message digest. Then A encrypts the message digest within private key the result is in the Digital signature form. Using RSA algorithm, A will encrypt the digital signed signature with B's public key and B will decrypt the cipher text to plain text with his private key and A's public key for verification of signature.

PROPOSED WORK

Previous section describes the study about the cloud computing, basics of cloud computing and security problems occurs in cloud. Then study some papers to solve these security problems. Here in this paper, 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) [4].

Table 1. DNA Digital Coding

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

- **KEY COMBINATION**

Here in this work, we are using ATGC as a key. Every bit have 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. 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 by using Diffie Hellman key sharing algorithm. In this work, every time the key value will be randomly changed.

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. ENCRYPTION PROCESS

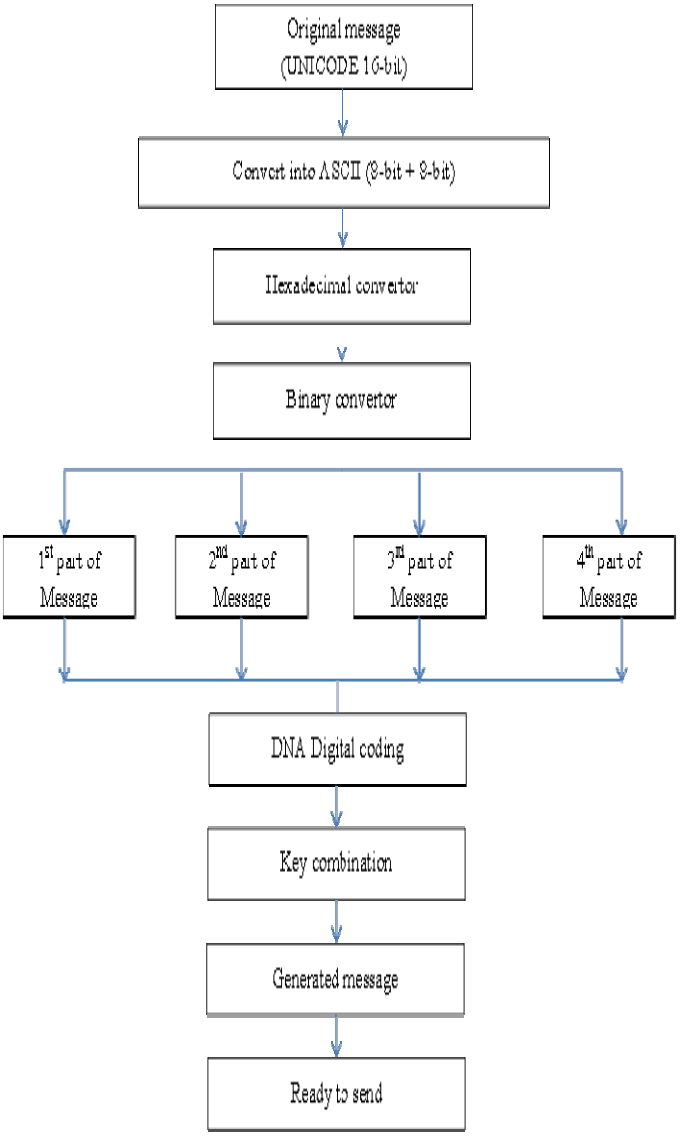

Fig 1: Encryption process

To understand the scenario of proposed work flow chart we consider one example. In this the example plaintext is આશિષand performing encryption operation.

Plaintext:

આશિષ

Unicode:

à³†à³¶à³¿à³·

ASCII:

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

Hexadecimal value:

5c753065305c753061615c7530323032305c753065305c7530
61615c753062365c753065305c753061615c753062665c7530
65305c753061615c75306237

Binary value:

0101110001110101001100000110010100110000010111000 1
1101010011000001100001011000010101110001110101001 1
0000001100100011000000110010001100000101110001110 1
0100110000011001010011000001011100011101010011000 0
0110000101100001010111000111010100110000011000100 0
1101100101110001110101001100000110010100110000010 1
1100011101010011000001100001011000010101110001110 1
0100110000011000100110011001011100011101010011000 0
0110010100110000010111000111010100110000011000010 1
1000010101110001110101001100000110001000110111

DNA Digital coding:

From Table 1 we can write

TTCATCTTACAATGTTACAATTCATCTTACAATGATT
GATTTCATCTTACAAACAGACAAACAGACAATTCAT
CTTACAATGTTACAATTCATCTTACAATGATTGATTT
CATCTTACAATGAGACTGTTCATCTTACAATGTTACA
ATTCATCTTACAATGATTGATTTCATCTTACAATGAG
TGTGTTCATCTTACAATGTTACAATTCATCTTACAAT
GATTGATTTCATCTTACAATGAGACTC

Now from table 2, the amplified message is generated,

Amplified Message

1111111010011111001001010111111100100101111111101 0
0111110010010101110011011100111111110100111110010 0
1010011000100100101001000010010010111111110100111 1
1100100101011111110010010111111110100111110010010 1
0111001101110011111111101001111100100101011100010 0
1001111111111010011111001001010111111100100101111 1
1110100111110010010101110011011100111111111010011 1
1100100101011100010111011111111110100111110010010 1
0111111100100101111111101001111100100101011100110 1
1100111111111010011111001001010111000100101001

B. DECRYPTION PROCESS

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

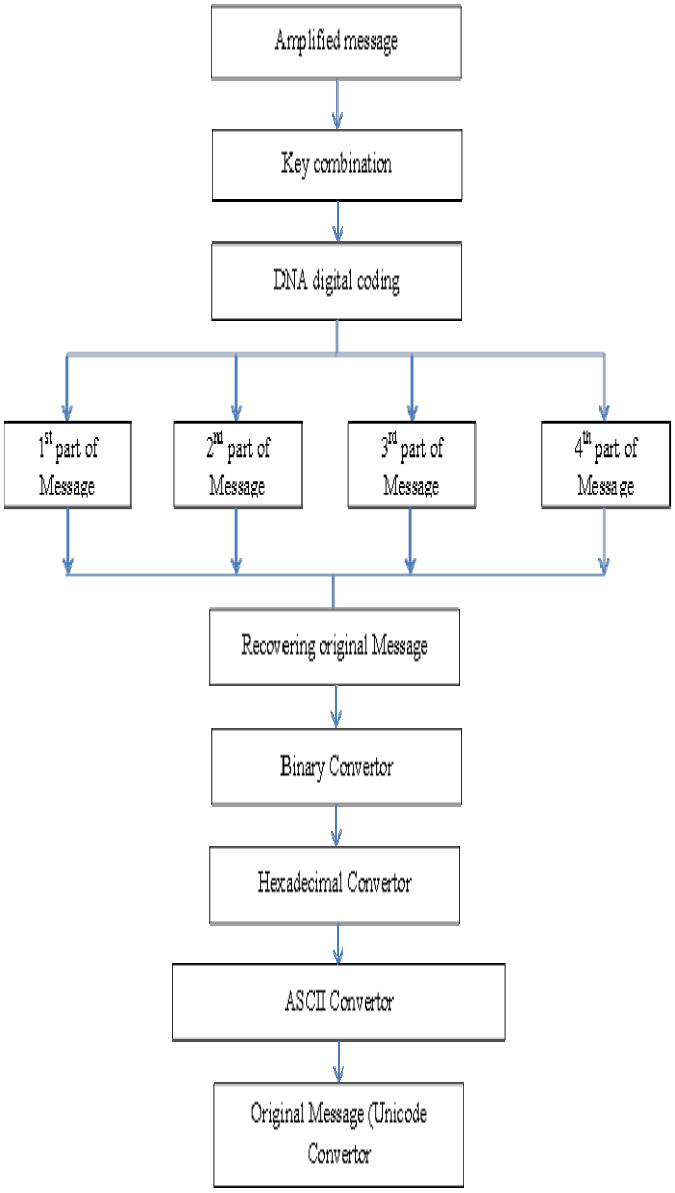

Fig: 2: Decryption process

Amplified Message

1111111010011111001001010111111100100101111111110100111111001001010111111100100101111111110100111110010010101110011011100111111111010011111001001010111000100100111111111101001111100100101011111111001001011111111101001111100100101011100010111011111111110100111110010010101110011011100111111111010011111001001010111000100100111111111101001111100100101011100010111011111111110100111110010010101110011011100111111111010011111001001010111000100101001

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

DNA Digital coding:

TTCATCTTACAATGTTACAATTCATCTTACAATGATT
GATTTCATCTTACAAACAGACAAACAGACAATTCAT
CTTACAATGTTACAATTCATCTTACAATGATTGATTT
CATCTTACAATGAGACTGTTCATCTTACAATGTTACA
ATTCATCTTACAATGATTGATTTCATCTTACAATGAG
TGTGTTCATCTTACAATGTTACAATTCATCTTACAAT
GATTGATTTCATCTTACAATGAGACTC

From the table of DNA digital coding we can generate.

0101110001110101001100000110010100110000010111000111010100110000011000010110000101011100011101010011000001100001011000010101110001110101001100000110001000110110010111000111010100110000011001010011000001010111000111010100110000011000010110000101011100011101010011000001100001011000010101110001110101001100000110001000110110010111000111010100110000011001010011000001010111000111010100110000011000010110000101011100011101010011000001100001011000010101110001110101001100000110001000110111

Hexadecimal value:

5c753065305c753061615c7530323032305c753065305c753061615c753062365c753065305c753061615c753062665c753065305c753061615c75306237

ASCII:

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

Unicode:

àªàªàªàª¿àª·

Plaintext:

આશિષ

IV SNAPS OF PROPOSED WORK (ENCRYPTION).

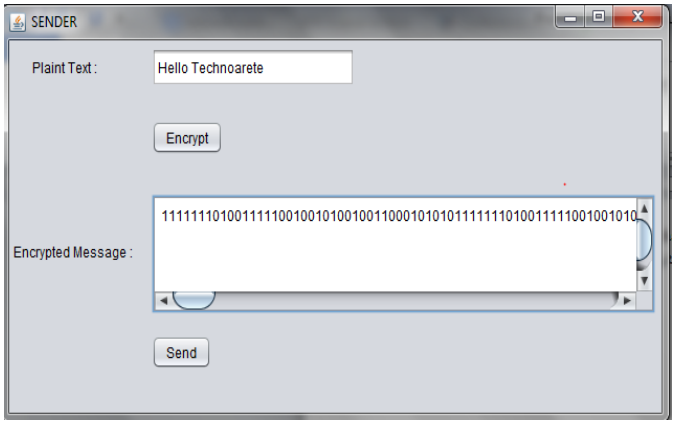

Fig. 3: Encryption operation

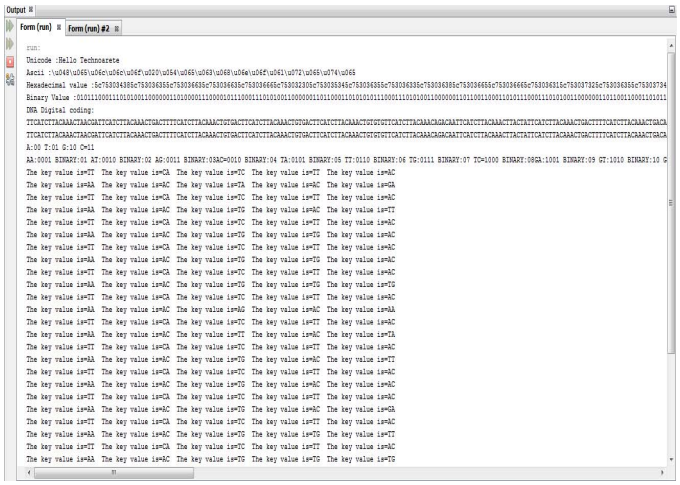

Fig.4: Encryption flow

V SNAPS OF PROPOSED WORK (DECRYPTION).

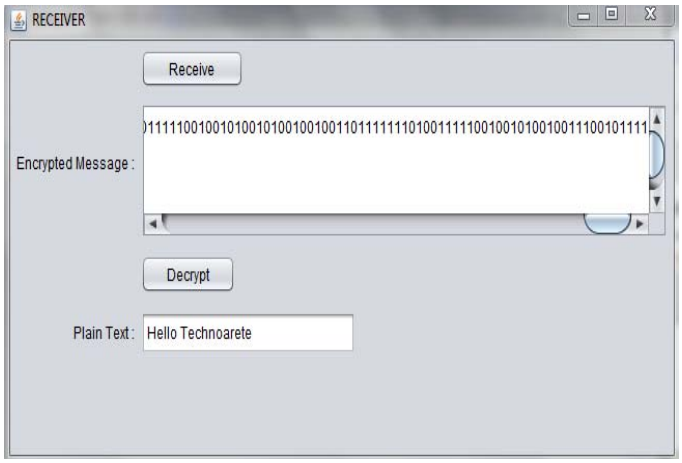

Fig.5:Decryption Process

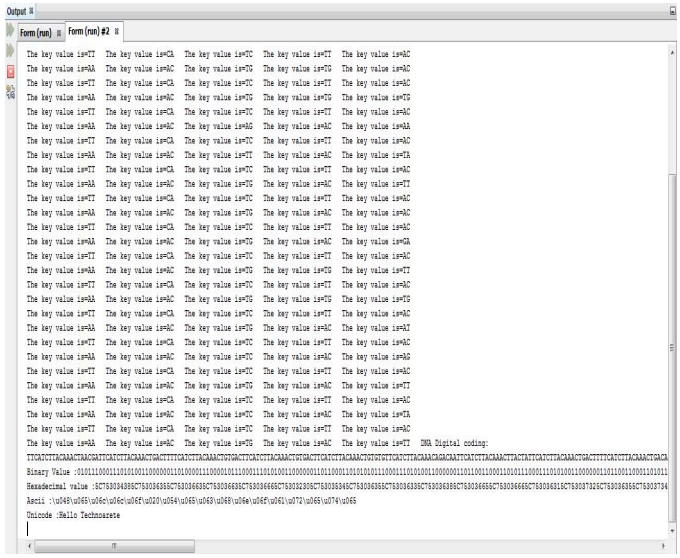

Fig.6: Decryption flow

WORKING ON AMAZON WEB SERVICE.

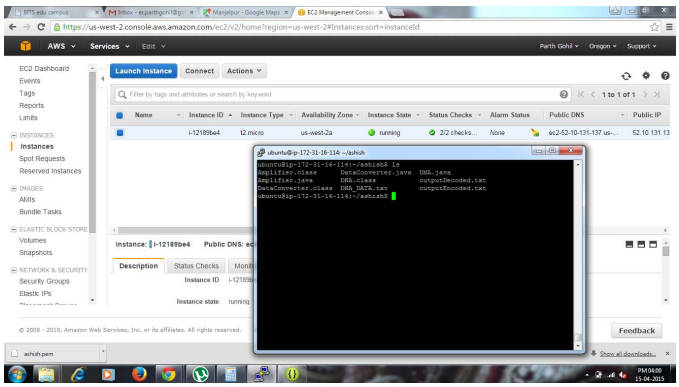

Fig. 7: Run instance in AWS

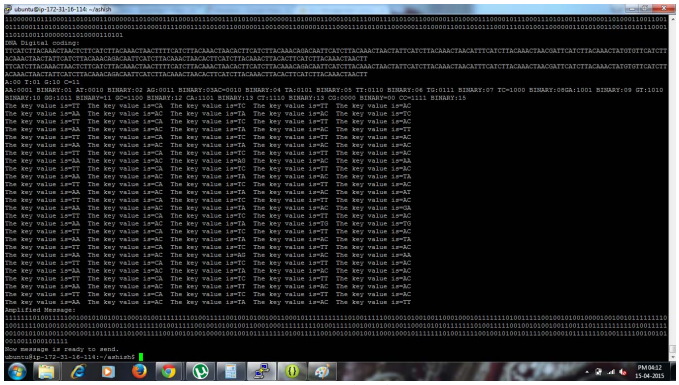

Fig.8: Encryption in AWS

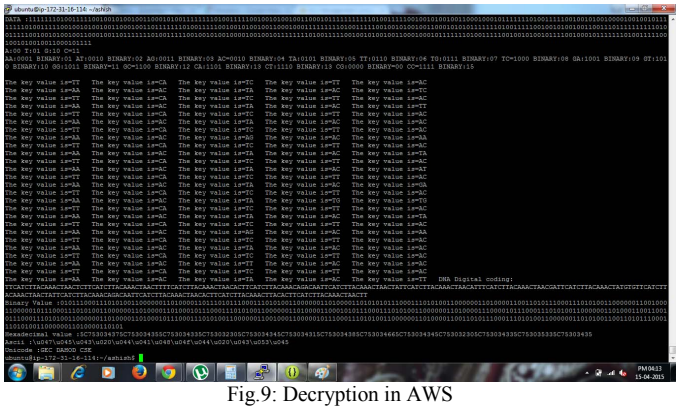

Fig.9: Decryption in AWS

CONCLUSION & FUTURE WORK

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, we achieve 2-layer security for ASCII character sets.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.

REFERENCES

[1] 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).

[2] Uma Somani, Kanika Lakhani, ManishaMundra, "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"Union of RSA algorithm, Digital Signature and KERBEROS in Cloud Computing" International Conference on Software Technology 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.