Journal of Green Engineering (JGE)

Volume-10, Issue-3, March 2020

Improving User Level Security in Green Cloud Environment Using EDNA Cryptography

[1]K Dhinakaran , [2]R. Gnanavel, [3]T.Rajasekaran, [4]S Durgadevi

[1,2]Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, India.
E-mail: [1]maildhina.k@gmail.com,[2]rgvelu22@gmail.com,
[3]Assistant Professor, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India.
E-mail:raja5891.t@gmail.com
[4]UG scholar, Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, India.
E-mail: durgadevi.s.2017.cse@ritchennai.edu.in

Abstract

Past decade cloud is a developing technology in public and corporate clients. In web environment client verification and security has a significant job, this paper propounds a technique called a novel cryptography to maintain a strategic distance from malevolent client going into cloud application for improving the client level security. There are different cryptographic strategies, calculations, and systems for approving the client for getting to information or working cloud applications, which have been proposed by existing examination works. Yet at the same time there are different malicious client exercises like sybil, Distributed Denial of Service, Economic Denial of Sustainability, specific sending, etc., are expanding step by step in cloud. This paper thinks about the above issues as a significant issue and urge to give a superior arrangement

Journal of Green Engineering, Vol.10_3,769-791.

Alpha Publishers

which disposes of the malignant client movement in cloud. To do this, the EDNA (Enhanced Deoxyribo Nucleic Acid) cryptography technique is utilized for producing a solid key for client and information encryption – decoding process. For creating string key and information encryption, User data is changed over into human deoxyribonucleic acid form. Open stack is utilized to do the execution of the proposed approach and the trial results are confirmed. In view of the picked up results the performance is investigated by contrasting and the current outcomes. The proposed method also is applicable for hardware and green engineering environment.

Keywords : Cryptography, Green Cloud User level security, Enhanced Deoxyribo Nucleic Acid Encryption.

1 Introduction

Secretness, verification and data cohesion, and data signature are the process involved in security services. Suppose one user need to communicate with another user with security, the above-mentioned security service mechanism is needed to follow. The secretness is confidentiality for providing a security to the data using two kinds, they are symmetric and asymmetric methods which are represented had block cipher and stream cipher. In Symmetric method, the encryption and decryption are done by using a single key {K}, whereas in asymmetric method, encryption and decryption process is done separately by using set of keys {KU, KR}. Symmetric method includes conventional data encryption [1-4] and facilitated standard encryption [1-4] algorithms. Asymmetric methods like Rivest–Shamir–Adleman algorithm that uses both the keys for cryptography. The authentication is verification for validating the data that shared. For unification, the conversion of plaintext into an unreadable format is done using a predetermined value of length. Message Digest [5], Secure Hash Algorithm -512 [6] and keyed-hash message authentication code [7] algorithms are used to acquire the fixed length value. Generally, in integrity, the modification is not done by anyone in the network must be trusted by receiver. For encrypting the data, the sender uses the own private key to send to the final node which can be performed with the help of DSA algorithm..

Figure-1. Existing Cryptographic Algorithms

For the safety of data in an application, the Figure-2 exhibits the classification of algorithm in cryptographic for the motive of security. According to the applications to improve the security in any type of meshwork, the corresponding algorithms are selected.

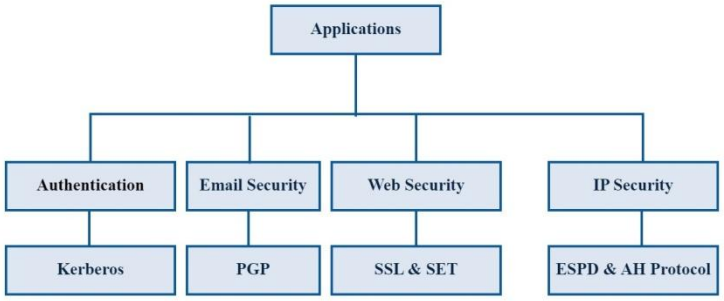

Figure-2. Categorization of Security Application Algorithms

Better privacy, Transfer of Electrons in secure way, fixed Sockets Layer Many users in the web infrastructure require highsecurity for their data while sharing. Making the data unreadable format is one of the methods. Author in [8] replaces each character in the message by the alphabets to transmission from one node to another node. For instance, every time letters like A, B are replaced by D, E respectively and so on. In the network, few systems that validates to allow only authorized user to transmit and receiving the information. Here, some of the user cane becomes a sinkhole (binds all the data by himself) [9]. For transmitting the data securely there are various procedures, methodologies, and processes in recent days of IT. Deoxyribonucleic acid (DNA)

cryptography [11-12], is the procedure used for the transfer of data with high security to protect the information. Author in [10] introduced the DNA cryptography. It is the method of converting an ordinary plaintext into incomprehensible text and in contrariwise. Cryptography is the primitive technique found in history of Egyptian that uses non- conventional for epitaph or carving. Applications that gives protection to data that is transmitting is very tedious and becomes a challenge for organizations. Cryptography always discuss about CIA triad. Contemporary cryptography also contains the further features called nonrepudiation. The mathematical expression is provided by the Cryptography and techniques associated with security of information such as,

- Surreptitiousness [13],
- Data cohesion,
- Individual verification And
- Data Origin verification.

The listed procedures that require to upgrade unusually large nowadays along with improved technology and computation power also increased. In cryptography, Encryption is a way of converting information into a code, especially to prevent it from unauthorized user. It is used to take care of safe exchange of information. So that data is protected by the unauthorized user. The word encrypts means that the data or information is converted into symbol in order to make it secret.

$$En \rightarrow "tomake"$$

$$Crypt \rightarrow "secret"$$

$$Encrypt \rightarrow "tomakesecret"$$

In order to access the encrypted file, secret key must be known for the decryption of data. The encryption procedure can be performed using two kind algorithms are:

- Public Key Cryptography [14-17].
- Secret key cryptography [14-17].

2 Traditional Cryptography Challenges

In present-day mainframes, information gets stored as a binary format. The key length is too big which is used in recent cryptographic. Cracking a key is

exceedingly difficult as it need to execute huge amount of computations at a same instance of a time which is the fusion to crack key as it is large and consume a longer time. In order to store the data using quantum bits a new phenomenon is used which is called Quantum computation. Thus, calculations are performed amazingly fast and hence to break the code, it takes more time which id used to crack speedily. The quality of the algorithm, key size and infrastructure are few disputes of traditional cryptographic methods. To solve a security problem, there are various traditional algorithm has been used by considering the infrastructure or platform. Recent days the security for the data protection and validation are most needed by the cloud computation and some network applications. User validation means, by validating the user by providing them the authentication. Due to the severe security problem in traditional encryption algorithm, there is latest way for data protection is given by the field of information security. Cryptography which is based on DNA has examined as new way for protecting the data that is in form of DNA fragments for burring of information. To provide more high security while sharing of data over a network is the main purpose of DNA cryptography. This paper examines about cryptography, distinguishing both traditional and DNA Cryptography, the work performed using DNA Cryptography.

The computation of information and DNA are differentiated that are demonstrated in Figure-3.The conversions of numerical, alphabets and alpha-numerals into a 0's and 1's is done only by the processor in the computing industry. Similarly, information that are represented as DNA molecules with the help of AGCT (A-Adenine, C-Cytosine, G-Guanine, T-Thymine letters) which is coded. This paper mainly concentrated on usage of computation of DNA, where the hardback materials for the microprocessors of next generation are created by this computation. In 1994, with the help of DNA, HDPP (Hamiltonian Directed Path Problem) is solved by Dr.Adleman [18]. DNA is acting as the massive memory, as it is not directly used in computation. He illuminates that any of the combinatorial problem can be solved with the solution of molecular combinations. It is completed by demonstrating the computational system of DNA which is the replicate one for combinatorial problems. The determination of DNA is acceptable for a solving the combinatorial problems is proved by Adleman , where this paper also trying to provide a better security for the user level in cloud applications by using DNA computing.

It is understood that computation of DNA [19-20] which is used to store vast amount of data with the help of re-combinative characteristics of DNA from many Adleman's tutorials or experimental explanation. A DNA of brevity can maintain enormous amount of parallel interactions rapidly. It is parallel linear processing. The operations such as connecting, categorising and pasting

are done by using AND, OR, NOR and NOT operations fitting with DNA. Complementarities are one of the functions makes the DNA as distinctive. It can also be used for the development of distinct key or in correcting the errors. The DNA calculation ability compared with other computers is given in Table-1, it displays that for parallel process across huge amount of data at high speed, DNA is suitable.

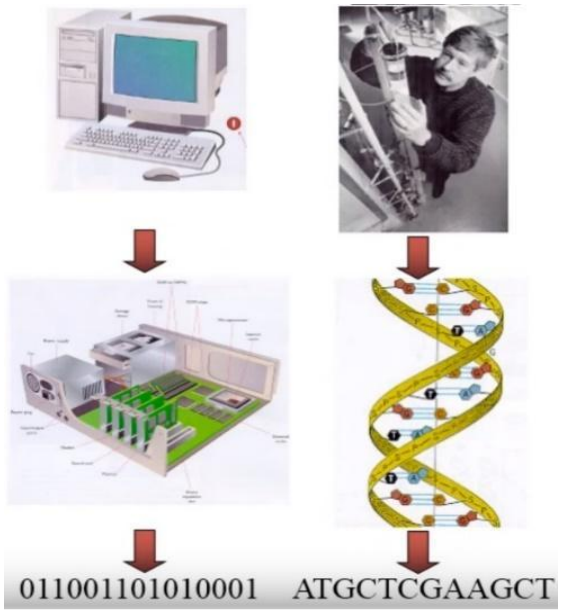

Figure-3. DNA Computing

There are four nucleotides such as "A-Adenine", "C-Cytosine", "G-Guanine", and "T-Thymine" for representing the data in DNA computer. Here chemical properties of molecules replace the electrical impulses. It is used to investigate about the data and its templates. For instance, for user identity and validation, the information is transformed binary format by converting it into ACGT form which gives incorruptible password that provides high user-level security and data-level security. But this proposed model is designed only for user-level security alone.

Table-1. DNA Computing capability matching with other Computing

Processor	**Capacity**
Desktop	10^6 operation / second
Super Computer	10^{12} operation / second
1 μmol of DNA	10^{26} operation / second
1 Joule of Energy	2 x 10^{19} operations
Memory Capacity	1 bit / cubic nanometre

3 Proposed System

In propounded system, a key is generated which is based on EDNA for providing the user entry with authentication key and authorization for the accessibility in the application of green cloud. The latest proposed method of encryption is to create an EDNA pattern by using random number generation. The generation of key and random key, and cryptography methods are the three major parts in the entire algorithm. At the beginning stage, the data that is obtained from the use is encrypted and send it into the next level. In Second level, the generation of random keys for example, P_k, is random number used for next level encryption. Finally, get the original data it as to perform decryption process. Here, the plain text is converted into ASCII form by considering the text as a sequence of character or each letter as a character. The binary form is obtained from ASCII character. The encryption procedure of DNA is demonstrated in Figure-4. In this process of encryption, an input message M and transmitted to the receiver.

3.1 Encryption Process

The subsequent steps demonstrate the encryption procedure:

Step-1: Transform the original text into ASCII value i.e., numerical form

Step-2: Consider every the ASCII values as blocks

Step-3: Convert ASCII values into binary form (0's and 1's)

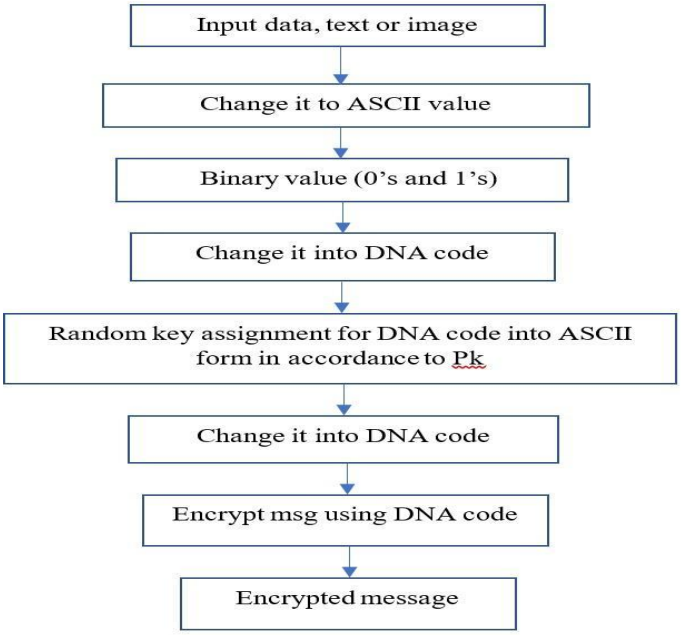

Figure-4.EDNA Based Data Encryption in Green Cloud

A mathematical illustration can be used to demonstrate the encryption procedure. Let as consider as a instance: the data INDIA as the input. Then the procedure as follows:

Step 1: ASCII value of "INDIA" is taken from ASCII table given in Table-2.
I = 73

N = 78

D = 68

I = 73

A = 65

Step -2: The equivalent binary data for each ASCII code is given as

I = 73 = 00011001 = 00 | 01 | 10 | 01 = ATGT
N = 78 = 00011110 = 00 | 01 | 11 | 10 = ATCG
D = 68 = 00010100 = 00 | 01| 01 | 00 = ATTA
I = 73 = 00011001 = 00 | 01 | 10 | 01 = ATGT
A = 65 = 00010001 = 00 | 01 | 00 | 01 = ATAT

Table-2. ASCII – Values

Char	ASCII	Decimal	Bits	Char	ASCII	Decimal	Bits	Char	ASCII	Decimal	Bits
0	48	0	000000	F	70	22	010110	d	100	44	101100
1	49	1	000001	G	71	23	010111	e	101	45	101101
2	50	2	000010	H	72	24	011000	f	102	46	101110
3	51	3	000011	I	73	25	011001	g	103	47	101111
4	52	4	000100	J	74	26	011010	h	104	48	110000
5	53	5	000101	K	75	27	011011	i	105	49	110001
6	54	6	000110	L	76	28	011100	j	106	50	110010
7	55	7	000111	M	77	29	011101	k	107	51	110011
8	56	8	001000	N	78	30	011110	l	108	52	110100
9	57	9	001001	O	79	31	011111	m	109	53	110101
:	58	10	001010	P	80	32	100000	n	110	54	110110
;	59	11	001011	Q	81	33	100001	o	111	55	110111
<	60	12	001100	R	82	34	100010	p	112	56	111000
=	61	13	001101	S	83	35	100011	q	113	57	111001
>	62	14	001110	T	84	36	100100	r	114	58	111010
?	63	15	001111	U	85	37	100101	s	115	59	111011
@	64	16	010000	V	86	38	100110	t	116	60	111100
A	65	17	010001	W	87	39	100111	u	117	61	111101
B	66	18	010010	'	96	40	101000	v	118	62	111110
C	67	19	010011	a	97	41	101001	w	119	63	111111
D	68	20	010100	b	98	42	101010				
E	69	21	010101	c	99	43	101011				

Table-3. DNA – Binary Code

DNA Code	Binary Code
A	00
T	01
G	10
C	11

Adenine (A), Cytosine (C), Guanine (G) and Thymine (T)

Thus, the input data INDIA is transformed into ATGT - ATCG - ATTA - ATGT - ATAT

Step-3: DNA code pattern is used to replace each character INDIA. Now a random key is generated and allocated to each pattern as 156, 151, 157, 156, 148 along with DNA code that illustrated in Table-4.
Step 4: Hence the code 156-151-157-156-148 is the password that is encrypted. Banking sectors use this type of password generation.

3.2 Random Key Generation

The generation of random key is the next step of DNA cryptography process selected the range of 1 to 256 which is allocated as Pk for encoding. In observing, the Pk codes are allocated as an index that are related to aggregate A, T, G and C. For instance, as in Table-4 the DNA code in AAAA for Pk=1. Similarly, using the technique of permutation, the four characters such as A, T, G and C give the 256-index value. If value of Pk changed, then it also leads to the changes in the index table. As the outcome of the encryption process, the given input INDIA is encrypted into ATGT - ATCG - ATTA - ATGT – ATAT.

3.3 Decryption Process

Conversion of encrypted data into its indigenous data back is called decryption process. The decryption process can be processed only by the user who has authentication and who is the holder of the data. Decryption can be done only by the owners who had the secret key. In the beginning, the message which is encrypted is considered as input in the decryption process. Then the block generates P_k. It is then converted into code of DNA and to corresponding values in binary. Later, the set of binary values 00, 01, 10, 11 is replaced in the place of 1, T, G, and G respectively. After that, the block is organized into a block of binary values which is then converted into ASCII values. At last, the earliest data or decrypted message is obtained from the ASCII values. This whole operation is specified as the following stages and is shown in the Figure-6.

Decryption Process
Step 1: Consider 156-151-157-156-148
Step 2: Substitute random generated key at an instance

156 -ATGT	- 00 | 01 | 10 | 01	- 00011001	- 73	- I
151 -ATCG	- 00 | 01 | 11 | 10	- 00011110	- 78	- N
157 -ATTA	- 00 | 01| 01 | 00 - 00010100	- 68	- D	
156 -ATGT	- 00 | 01 | 10 | 01	- 00011001	- 73	- I
148 -ATAT	- 00 | 01 | 00 | 01	- 00010001	- 65	- A

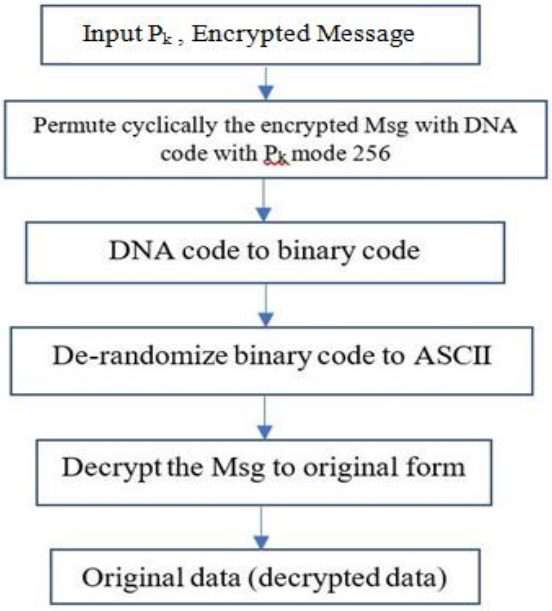

Figure-5. DNA Based Data Decryption in Green Cloud

The algorithm for generating key (as a password) which is only for the user having authentication is DNA cryptographic. The authorised user is the one those who can access any application or able to exchange the message with another authenticated user. For instance, if end user enters their username and password in the application, the password entered is considered as the input and with the help of DNA cryptographic method it is encrypted. Figure-6 demonstrate the operation of user registration, password is given by the user and DENA encryption is working in the system then the crypt password gets stored in the server or DB for further uses. Here, encryption is done automatically after entering of data by the user and authenticate the user without any knowledge which provides various application with high security.

Table-4. Random Key Generation for DNA code

1	AAAA	33	CAAA	65	GAAA	97	TAAA	129	AGAA	161	CGAA	193	GGAA	225	TGAA
2	AAAC	34	CAAC	66	GAAC	98	TAAC	130	AGAC	162	CGAC	194	GGAC	226	TGAC
3	AAAG	35	CAAG	67	GAAG	99	TAAG	131	AGAG	163	CGAG	195	GGAG	227	TGAG
4	AAAT	36	CAAT	68	GAAT	100	TAAT	132	AGAT	164	CGAT	196	GGAT	228	TGAT
5	AACA	37	CACA	69	GACA	101	TACA	133	AGCA	165	CGCA	197	GGCA	229	TGCA
6	AACC	38	CACC	70	GACC	102	TACC	134	AGCC	166	CGCC	198	GGCC	230	TGCC
7	AACG	39	CACG	71	GACG	103	TACG	135	AGCG	167	CGCG	199	GGCG	231	TGCG
8	AACT	40	CACT	72	GACT	104	TACT	136	AGCT	168	CGCT	200	GGCT	232	TGCT
9	AAGA	41	CAGA	73	GAGA	105	TAGA	137	AGGA	169	CGGA	201	GGGA	233	TGGA
10	AAGC	42	CAGC	74	GAGC	106	TAGC	138	AGGC	170	CGGC	202	GGGC	234	TGGC
11	AAGG	43	CAGG	75	GAGG	107	TAGG	139	AGGG	171	CGGG	203	GGGG	235	TGGG
12	AAGT	44	CAGT	76	GAGT	108	TAGT	140	AGGT	172	CGGT	204	GGGT	236	TGGT
13	AATA	45	CATA	77	GATA	109	TATA	141	AGTA	173	CGTA	205	GGTA	237	TGTA
14	AATC	46	CATC	78	GATC	110	TATC	142	AGTC	174	CGTC	206	GGTC	238	TGTC
15	AATG	47	CATG	79	GATG	111	TATG	143	AGTG	175	CGTG	207	GGTG	239	TGTG
16	AATT	48	CATT	80	GATT	112	TATT	144	AGTT	176	CGTT	208	GGTT	240	TGTT
17	ACAA	49	CCAA	81	GCAA	113	TCAA	145	ATAA	177	CTAA	209	GTAA	241	TTAA
18	ACAC	50	CCAC	82	GCAC	114	TCAC	146	ATAC	178	CTAC	210	GTAC	242	TTAC
19	ACAG	51	CCAG	83	GCAG	115	TCAG	147	ATAG	179	CTAG	211	GTAG	243	TTAG
20	ACAT	52	CCAT	84	GCAT	116	TCAT	148	ATAT	180	CTAT	212	GTAT	244	TTAT
21	ACCA	53	CCCA	85	GCCA	117	TCCA	149	ATCA	181	CTCA	213	GTCA	245	TTCA
22	ACCC	54	CCCC	86	GCCC	118	TCCC	150	ATCC	182	CTCC	214	GTCC	246	TTCC
23	ACCG	55	CCCG	87	GCCG	119	TCCG	151	ATCG	183	CTCG	215	GTCG	247	TTCG
24	ACCT	56	CCCT	88	GCCT	120	TCCT	152	ATCT	184	CTCT	216	GTCT	248	TTCT
25	ACGA	57	CCGA	89	GCGA	121	TCGA	153	ATGA	185	CTGA	217	GTGA	249	TTGA
26	ACGC	58	CCGC	90	GCGC	122	TCGC	154	ATGC	186	CTGC	218	GTGC	250	TTGC
27	ACGG	59	CCGG	91	GCGG	123	TCGG	155	ATGG	187	CTGG	219	GTGG	251	TTGG
28	ACGT	60	CCGT	92	GCGT	124	TCGT	156	ATGT	188	CTGT	220	GTGT	252	TTGT
29	ACTA	61	CCTA	93	GCTA	125	TCTA	157	ATTA	189	CTTA	221	GTTA	253	TTTA
30	ACTC	62	CCTC	94	GCTC	126	TCTC	158	ATTC	190	CTTC	222	GTTC	254	TTTC
31	ACTG	63	CCTG	95	GCTG	127	TCTG	159	ATTG	191	CTTG	223	GTTG	255	TTTG
32	ACTT	64	CCTT	96	GCTT	128	TCTT	160	ATTT	192	CTTT	224	GTTT	256	TTTT

Many numbers of organisations share their information in web using an interface with huge number of customers who must need to be authenticated. This can be done based on this proposed method by verifying with their respective DNA keys. For instance, there are users A and B as they need to exchange their message, they do using DNA cryptographic that gives the password by encryption then it is gets verified with the help of Database by checking the availability of encrypted password. If the password is present for the respective username which make the users both A and B is provided with the accessibility of application or official information's can be shared. Figure-7 illustrates the functionality of the model.

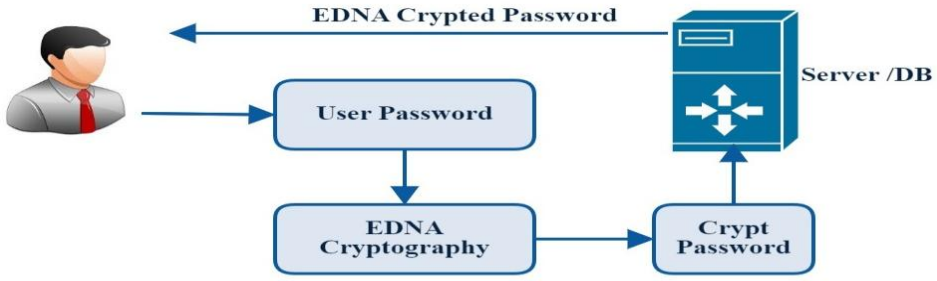

Figure-6 EDNA Password generation

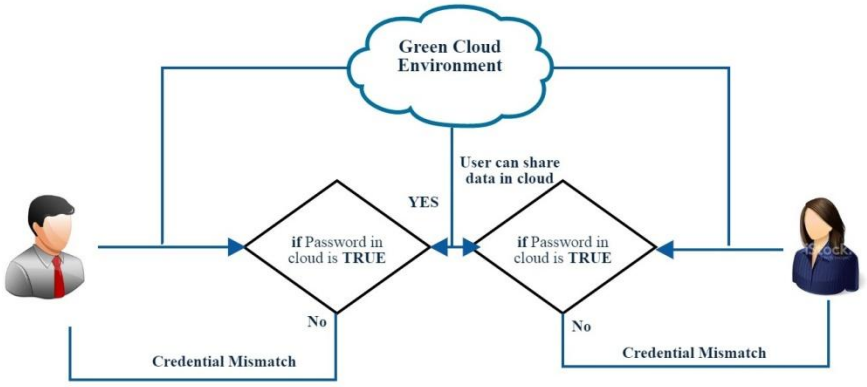

Figure-7. Two Users Can Share Their Data After DNA Encrypted PWD Based Authentication

This process can be used for authenticating the users in applications of web and cloud. In some instance, for encrypting the data encryption key is used or for transmitting the message between two users over the network. For encrypting both the size of data files such as large size and small size DNA cryptography can be used. This type of cryptography does not influence either the memory or time acquired for the process of encryption and decryption. DNA is quick, effective and processes it easily when compared with other cryptographic methods. In case of computational processes, it does not make more complexity. Also, it is language independent. Therefore, the implementation can be made with any coding languages. The complete process of proposed DNA cryptography is made with a pseudo code which is used to

code the program directly in any language along with the confirmation of efficiency. Here, the python is used for implementing the proposed DNA cryptographic algorithm based on web and the attainment is differentiated with the other existing approaches.

ALGORITHM EDNA_Encryption(msg)

```
//Encrypt the message using DNA code
//Input: An array msg[0....n-1] of n characters representing a data
//Output: An encrypted data
Dec_value← {empty}
Initialize i← 0
Dec_value← Ascii(msg[i])
While Dec_value> 0
    Reminder ←Dec_val modulo 2
    Binary[i] ← Reminder
    Dec_value←Dec_value divide 2
    Increment i value by 1
Assign j ← i-1
While j>=0
    If (j mod 2 = = 0 and  j ! = 0) then
            Code ← Concatenation (binary[j],binary[j+1])
            If Code = = 00   then
                    DNAcode← 'A'
            Else if Code = = 01 then
                    DNAcode←  'T'
            Else if Code = = 10 then
                    DNAcode← 'G'
            Else
                    DNAcode← 'C'
            FinalDNAcode← {Empty}
        FinalDNAcode← Concatenation(FinalDNAcode,DNAcode)
    Decrement j value by 1

Pk← Choose number from 1 to 256
FinalDNAcode←Pk
Encrypteddata← encrypt(msg,FinalDNAcode)
Return Encrypteddata;
```

ALGORITHM EDNA_Decryption(Encrypteddata,DNAcode,Pk)

```
//Decrypt an encrypted data using DNA code
//Input: An encrypted data, DNAcode and Pk
//Output: The decrypted data
Data ← Permutate(Encrypteddata,DNAcode,Pk mod 256)
Initialize i← 0
While Data[i] != '\0'
    If  Data[i] = = 'A' then
            Code ←  '00'
    Else if Data[i] = = 'T' then
            Code ←  '01'
    Else if Data[i] = = 'G' then
            Code ←  '10'
    Else
            Code ←  '11'
    Binarycode← {Empty}
        Binarycode← Concatenation(Binarycode,Code)
    Increment i value by 1
Assign Dec_value←0 and temp ←0
WhileBinarycode!=0
        Remainder ←Binarycode modulo 10
        Binarycode←Binarycode divide 10
        Dec_value←Dec_value+ Remainder * pow(2,temp)
        Increment temp value by 1
Decrypteddata←Char(Dec_value)
Return Decrypteddata
```

4 Experimental Results and Discussion

The green cloud environment was constructed using Xen Hypervisor with OpenStack cloud environment. OpenStack is using theXenAPI with python module for communicate with other cloud users . Here, the python language is used to implementation of the recommended EDNA cryptographic algorithm. For encrypting each character of data, single key is used which is examines as encryption of symmetric algorithm.EDNA chromosome or EDNA sequence are not needed by the proposed model for the processing of data. The range is

selected from 1 to 256 by the private key P_k for an untroubled conversation to clarify the process. The data given as input and $P_k$are the two values tha tmust be passed on for acquiring the encryption of data. The time complexity of execution is computed then it is related to currently available algorithms for estimation of efficiency of the propounded EDNA cryptography method. The outcomes of the comparison are displayed Figure-8. By comparing the outcomes, it is implied that the performance in security is effective and acceptable . Also, it is inferred that, in terms of authentication, the proposed EDNA cryptography is best that fits for any network / cloud applications.

As we discussed about the Asymmetric DNA calculation in [13], here we contrast the time complexity with the current Asymmetric DNA calculation and finished up by saying that the asymmetric DNA is likewise contrasted and the DEX, TDES, Blowfish, and AES. To demonstrate the bitterness, this proposed EDNA is contrasted and EDNA because it has been uncovered and unrivalled than different methodologies. On contrasting and different methodologies, it is construed that our proposed EDNA maintain a strategic distance from additional time multifaceted nature and decreases the cost intricacy. The Time get for the generation of parameter/key is another operator which build up the exhibition of the proposed calculation.

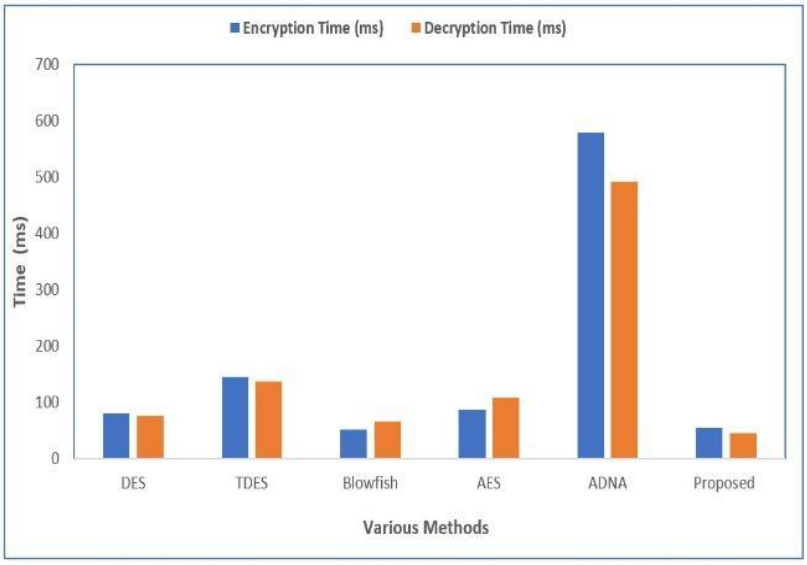

Figure-8. Time Complexity Comparison

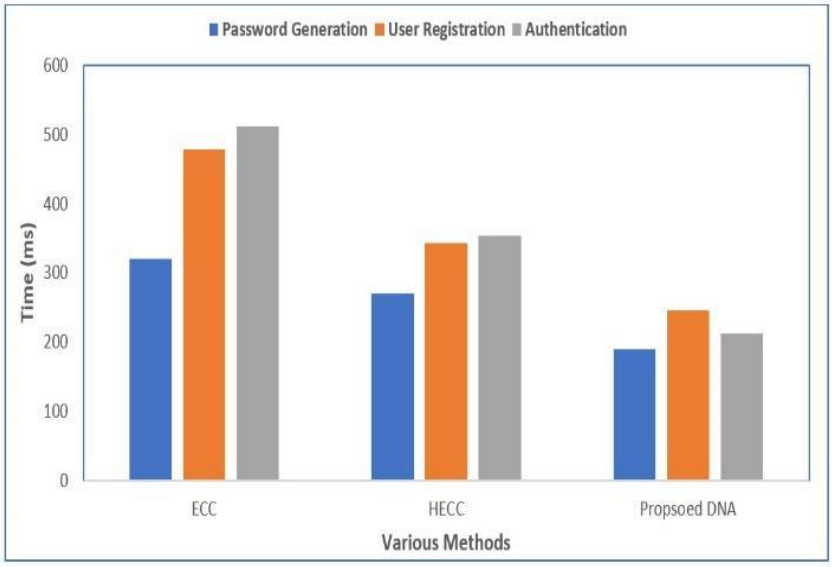

Figure-9. Time Complexity of Different Stages of the Framework

In this paper the essential stage and an essential procedure is key generation. Since, the time devoured for the generation procedure of key is registered and contrasted and the current methodology, for example, Electrical Curve Cryptographic (ECC) and Hyperelliptic Curve Cryptosystem(HECC) which has been portrayed in [21]. In Figure-9 it gives the correlation result and it shows that the propounded EDNA secure brief timeframe and computational complexity than contrasted with the other ECC and HECC strategies. Plus, the key size is changed to assess the presentation of DNA and it affirms the intricacy of time. The key size is indented as 32, 52, 64 and 128 bits in the show. All in all, for52 bits the results are looked at and appeared in Figure-9. From the results, it is built up that the intricacy of time is less in the proposed EDNA technique than the other existing ECC, HECC strategies where a similar sort of research work is finished. The generation of password, client enrolment and confirmation procedure of proposed EDNA got 189ms, 245ms, and 212ms individually and it is exceptionally little than the other existing methodologies as appeared in Figure-9.Thus, for cloud/arrange applications, the proficient model is the proposed EDNA model.

5 Conclusion

The indispensable motivation behind this examination work is to fix the client level security by planning and executing a novel security calculation.This is a confirmation model comprising of client validation process which can be utilized for any sort of system or cloud applications. Client verification process is one of the essential procedures and it is a compulsory procedure for a made sure about information transmission application.This procedure confirms the client as genuine or noxious client and strengthen that the predetermined client can get to the information or not. To carry out these responsibilities, the validation procedure is applied as the essential procedure and it is performed at a prior phase of the examination work. The EDNA cryptography based key generation provides the authentication for user validation, allocation, and confirmation. The benefits of the EDNA cryptographic technique were discussed completely and had been investigated. The outcomes were compared with the result of the existing model and it has been evidenced that the propounded technique called EDNA cryptography method is more effective than the other approaches in cryptography with respect to the complexity of time and computation. In succeeding level of the research work, membrane computing method is applied to provide security at infrastructure level, which will be suitable for green cloud and infrastructure security

References

[1] Enas Elgeldawi, Maha Mahrous, Awny Sayed, "A Comparative Analysis of Symmetric Algorithms in Cloud Computing: A Survey",International Journal of Computer Applications, vol.182, no.48, 2019.

[2] F. Mallouli, A. Hellal, N. Sharief Saeed and F. Abdulraheem Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms", 6th IEEE International Conference on Cyber Security and Cloud Computing,2019 .

[3] A.R.Pathak, S.Deshpande, M.Panchal, "A Secure Framework for File Encryption Using Base64 Encoding", Lecture Notes in Networks and Systems, Springer, vol. 75, 2019.

[4] K.Dhinakaran, R.Kirtana, K.Gayathri, R.Devisri," Enhance Hybrid Cloud Security Using Vulnerability Management", Advances in Intelligent Systems and Computing book series, Springer, vol. 614. 2017.

[5] P.Goyal, H.Makwana, N.Karankar, "MD5 and ECC Encryption based framework for Cloud Computing Services", Third International

Conference on Inventive Systems and Control (ICISC), pp.195-200, 2019.

[6] Esmael V. Maliberan, "Modified SHA1: A Hashing Solution to Secure Web Applications through Login Authentication", International Journal of Communication Networks and Information Security (IJCNIS),vol.11, No. 1, 2019.

[7] Mihir Bellare, , Ran Canetti and Hugo Krawczyk, , "Keying hash functions for message authentication ", Crypto 96 Proceedings, Lecture Notes in Computer Science , Springer-Verlag Vol. 1109, , 1996.

[8] "The Basics of Cryptography-Fisher College of Business". [Online] Available: https://fisher.osu.edu/~muhanna.1/pdf/crypto.pdf.

[9] J.Breier and X.Hou, "Introduction to Fault Analysis in Cryptography", Automated Methods in Cryptographic Fault Analysis, eBook , pp. 1-11,Springer,2019.

[10] Abhishek Majumdar, Arpita Biswas, Krishna Lal Baishnab and Sandeep K. Sood, "DNA Based Cloud Storage Security Framework Using Fuzzy Decision Making Technique", KSII Transactions on Internet and Information Systems, Vol. 13, No. 7, Jul 2019.

[11] A.Vikram, S.Kalaivani and G.Gopinath, "A Novel Encryption Algorithm based on DNA Cryptography", International Conference on Communication and Electronics Systems (ICCES), pp.1004-1009, 2019.

[12] A.Hazra , C.Lenka, A.Jha , M.Younus,"A Novel Two Layer Encryption Algorithm Using One-Time Pad and DNA Cryptography", Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, Springer, vol.103, pp 297-309,2020.

[13] W.Stallings, "Network security essentials", Prentice Hall, Fourth edition, 2011.

[14] Y.Niu, K.Zhao, X.Zhang, G.Cui, "Review on DNA Cryptography" ,Communications in Computer and Information Science, Lecture Notes in Networks and Systems, Springer, vol.1160, pp 134-148, 2020.

[15] A.M.Osman, A.Dafa-Allah, A.A.M.Elhag, "Proposed security model for web based applications and services", International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE), pp. 1-6, 2017.

[16] J. Sun, "Sequence splicing techniques and their applications for information encryption," The International Conference on Advanced Mechatronic Systems, pp. 310-313, 2012.

[17] Xiuli Chai et.al, "A novel image encryption algorithm based on the chaotic system and DNA computing",International Journal of Modern Physics C, Vol. 28, no. 5 , 2017.

[18] S Kumar, G Stecher, M Li, C Knyaz, K Tamura, "MEGA X: Molecular Evolutionary Genetics Analysis across Computing Platforms", Molecular Biology and Evolution, vol.35,No.6, pp.1547–1549, 2018.

[19] Xing Wang and Qiang Zhang, "DNA computing-based cryptography", IEEE proceeding of Fourth International Conference on Bio-Inspired Computing, pp.1 – 3, 2009.

[20] Barman Prokash and Saha Banani, "DNA Encoded Elliptic Curve Cryptography System for IoT Security" International Journal of Computational Intelligence & IoT, Vol. 2, No. 2, 2019.

[21] Radu Terec, Mircea-Florin Vaida, LenutaAlboaie, Ligia Chiorean, "DNA Security using Symmetric and Asymmetric Cryptography", International Journal on New Computer Architectures and Their Applications, vol.1, no.1, pp. 34-51, 2011.

Biographies

Dhinakaran K received his B.E Computer Science and Engineering from Anna University ,Chennai in 2011, Master of Engineering in Computer science and Engineering in 2013 from Sri Venkateswara college of Engineering and pursuing Ph. D in Anna University, Chennai, Tamilnadu, India from 2018. He is currently working as an Assistant Professor in the Department of Computer science and Engineering at Rajalakshmi Institute of Technology with total teaching experience of 7 years. He has been actively doing research in the area of cloud computing, Data analytics and data security.

R.Gnanavel is a Assistant Professor of the Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, based in Chennai, India. He holds Bachelor's and Master's degrees in Computer Science and Engineering from the Anna University affiliated institution at Tamilnadu. He has been with Rajalakshmi Institute of Technology since 2013, and has worked in several research areas, including Networking, Data Structures and Algorithms, Image Processing, and Data Analytics. His published works include more than 10 papers, blogs and standard contributions.

T.Rajasekaran received the B.Tech degree in Information Technology from Anna University, Tamilnadu, India in 2007, the M.E degree in Computer Science Engineering from Anna University, Tamilnadu, India in 2009. He is currently pursuing the Ph.D. degree in computer science with the Department of Computer Science and Engineering in Dr.M.G.R. Educational and Research Institute, Chennai, India. He is currently an Assistant Professor in the Department of Computer Science and Engineering in Sri Venkateswara College of Engineering, Tamilnadu, India. His primary research interest lies in the field of Cryptography, Cloud computing and Adhoc Networks.

Durgadevi S is an undergraduate in department of computer science and engineering at Rajalakshmi institute of technology. Completed the internship on the project "SAMVAAD (Middleware)" in Proconnect integrated logistics. Her research interest in data analytics, crowdsourcing and recommendation systems.