# IMPLEMENTATION OF DNA CRYPTOGRAPHY IN CLOUD COMPUTING AND USING SOCKET PROGRAMMING

# Priyanka agarwal<sup>1</sup>, sachin sharma<sup>2</sup>, Ritik sharma<sup>3</sup>

<sup>1</sup>Associate Professor, Dept. of ECE, Arya Institute of Engineering & Technology, Jaipur, Rajasthan, India <sup>2,3</sup>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 MainConversationandAESEncryptionAlgorithmtoEnh anceData Safety in Cloud Computing<sup>[1]</sup>.

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<sup>[2]</sup>.

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

permitgrantingticketandsessionkeyanditdirectedtotheuse rs. 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. INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY (IRJET)

Volume: 07 Issue: 02 | Feb 2020

WWW.IRJET.NET

### **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	А
01	Т
10	G
11	С

# **KEY COMBINATION**

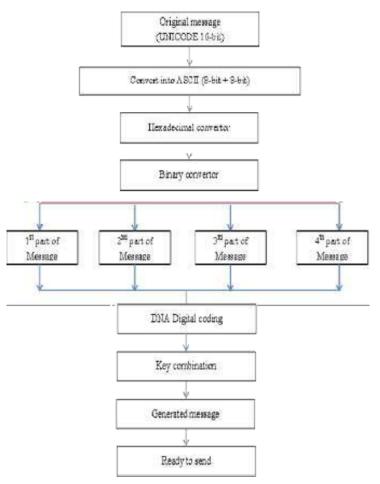
Now in this exertion, we are consuming ATGCasakey. Each bit have 2 bits like A=00, T=01, G=10, and C=11 and by consuming ATGC, key mixtures is produced and give numbering

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

<b>KEY COMBINATION</b>	PATTERNS	VALUES
AA	0101	5
АТ	0011	3
AG	0001	1
AC	0010	2
ТА	0110	6
TT	1111	15
TG	0111	7
ТС	1001	9
GA	1010	10
GT	0100	4
GG	1000	8
GC	1100	12
CA	1110	14
СТ	1011	11
CG	0000	0
CC	1101	13





**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:

આશિષ

### ASCII:

\u0e0\u0aa\u02020\u0e0\u0aa\u0b6\u0e0\u0aa\u0bf\u 0e0\u0a a\u0b7

### **Hexadecimal value:**

5c753065305c753061615c7530323032305c753065305 c

753061615c753062365c753065305c753061615c75306 2

665c753065305c753061615c7530623

INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY (IRJET)

TRIET VOLUME: 07 ISSUE: 02 | FEB 2020

### **Binary value:**

# **DNA Digital coding:**

### From Table 1 we can write

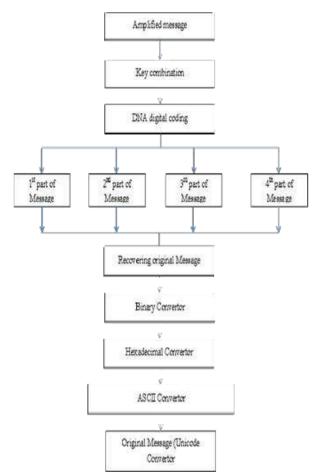
# Now from table 2, the amplified message is generated, Amplified Message

111110010010111111010011111001001010101110011011

0100101011100010010100

# **B. DECRYPTIONPROCESS**

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



**Fig: 2: Decryption process** 

### **Amplified Message**

VOLUME: 07 ISSUE: 02 | FEB 2020 WWW.IRJET.NET

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

110101001100000110001000110111

### **Hexadecimal value:**

5c753065305c753061615c7530323032305c753065305c75

3061615c753062365c753065305c753061615c753062665c

753065305c753061615c75306237

### ASCII:

IRIET

\u0e0\u0aa\u02020\u0e0\u0aa\u0b6\u0e0\u0aa\u0bf\u 0e0\u0a a\u0b7

### Unicode:

આશિષ

#### **Plaintext:**

Hello Technocrat

### 4.SNAPS OF PROPOSED WORK(ENCRYPTION)



Fig. 3: Encryption operation

ĥ	Preschell # strendendati a
ŝ	
	Taxet Mile Semante
4	Service of the two structures that the structure of the s
u	Name of a sector of the sector
	have been supported and the second
	IR Table lakes
	The second se
	Transactions and an anti-international contraction and an international contraction of the second statement
	435 3 (2 × 1) PU
	WHAT ADMALE, AT 100 DESCRIPTION AND ADDRESS AND ADDRESS TO THE PARTY OF THE ADDRESS AT TAXABLE ADDRESS AT TA
	The law value with The bay value with the law value with The bay value used
	The two value and it the law value shall. The law value and it the two value and it the two value and
	The last value and the second second second and the second second second second
	The feet value and the law value lawd. The law value and the law value and the law value and
	The My water and The My water and The My water and The My water Left The My water Left
	The lag minim mells. The lag value next: The lag value next: The lag value next: The lag value next:
	The two mains and? The two value and it has no value and it has no value and it has value and
	The activitie peak the optimizer per the entropy period peak period be optimized peak.
	The lay state setting water before the second setting water setting water setting value before
	The large state sheld. The large state sheld, The large state and T. The large state sheld.
	The same said the second the same said the same said the same said the said the said the said the said the said
	. Se les suite selle. Se les numerals deux de las results de les numerals de la service selle.
	The leg value lieft
	The sey wile weld. The say wile next: So bey wile next? The lay wile held: The bay wile herdi.
	the leg while self. The leg value selfs the leg value self. The leg value self. The leg value self.
	The test mine 1940, The lay mine 1940. The lay mine 1941. The set mine 1940. The test mine 1947.
	The key value and 1 the key value lands. The key value lands in the key value lands.
	<ul> <li>The key state sets. The key value sets? The key value sets? The key value sets?</li> </ul>
	The second party of the party of the second se
	The way walke areas a few and result. The least new? The least refull The least news?
	the lag salar sett the by take (JPD) the bit rates sett. The lag take sett the bit take set
	The lay value limits the lay value limit. The lay value of T. The lay value of T. The lay value limits
	The lay wine cost: The lay wine cost: The lay wine cost: The lay wine cost of the lay wine cost: The we wine cost: The lay wine cost: The lay wine cost: The lay wine cost: The term wine cost:
	The set of the local of the local of the local of the local test of the set of the local

### Fig.4: Encryption flow

### 5. SNAPS OF PROPOSED WORK(DECRYPTION)

RECEIVER.	C 2 3
	Receive
Encrypted Message	11111001001001001001001001001111111101001111
	Decrypt
Ptain Text	Helio Technoarete



here beed in them b	with a				
De ley suite pri- De ley suite pri-		Do no vice ordi. No ini vice ordi.	the second a cell the termine cells	De esplosite serie: De les volue serie:	
The lag raise and		The log value large	The let raise unit.	The last value torial	
Do inc mice and		To set up a pro-	Do ber man and	The face value (and)	
	the standard of	De les vale arts	fie ley nue tell.	The large value larves	
The bay value ( and		The lot value lottle	The lay tuble Leff."	De lay mile certit.	
The tax value last		The loss value last:	The lay value 1002	The task makes in the	
The last tailor (set		Tel alle inter	The last value larfs?	De ter mile (#0).	
The law rokes and		The lost value and the	The ter value hef?	Die less müller Laviel	
The bay rolling 1946		The let value Levill	The loty value loth?	the bay make setting	
The left tailor ( and		the set value party	The bay table 1977	The peri value Lawel	
The last value task		fig to use soft	The lay value lott?	The long value spectrum	
The lag value just		De ber balan 1972	The larg raise safety	The last indust (2002)	
The live raise (set	6. The net value limit	The net value up the	The last value last?	The last value (and)	
Its or playing	D . the net value law G	fin by sile left	the last value i.e.T.	Dia lang malan tanali	
The bay retrain lard	a the log rate limit	The last value law?	The lag racke Left	De wy mile left!	
the log failer last	t. Salas hala jota	the lot value lott	the bey lister sett	This beginned an address	
The log value lord	E for any take lot of	3m baj vaim 1002	The bag value left	the lag mains (setti-	
The log ratio and	7 The lett have seen	To be take (HT	The top value lateful	De les tobe series	
Do by sile (14)	6 Selected and	Do bet with Lordi	Do by rolat let?	Die beginnlass sieht.	
The leg tailed Lord	E - Da ing talin total.	the register and	Dating value and?	The long today served	
De lay islae Levi	<ol> <li>The log value unit;</li> </ol>	To be take 1972	The bey value upon	The lead value Levilli	
The left follow land	t beite telle lerth	To be blie into	The lay hile set?	The last value Levill	
The log raise and	6. This was a lot	To be not off	The say raise is will	the key value toritt	
The inty value and	5 Senencia la G	The last value land?	Deterministell.	The topy tracked service	
The lay rulas law	<ol> <li>To be relatively</li> </ol>		The ingradue settle	the leg rular (HG)	
The log tailor (eff	<ol> <li>An ing table lottli</li> </ol>	The left skille light	The leg industrieff	The test inclusion to the	
		"Bu bej talin jott	The bag router Levic'	The bay taken of TT - 200 Digitical ending	

#### Fig.6: Decryption flow

TRIET VOLUME: 07 ISSUE: 02 | FEB 2020

WWW.IRJET.NET

# WORKING ON AMAZON WEB SERVICE

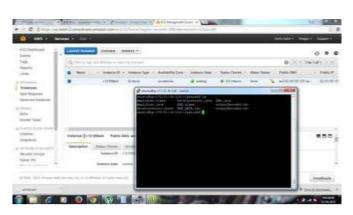


Fig.8: Encryption inAWS

				Con. Mail: Indiana, 147801	
	The Mill manual office		THE BE LEADED LATER		
	The big many press	the stores of the second	The level of period		
	The big more in-	The late in the latest	The last stand party	The second level	
the second second	the set mains three		the second course	The second second	
	The statement is the			And the local data	
		the set of the sector	the second second	The second second	
a state of the second	the last mine term	the states and		The sea waited in the	
	the set minuted		the second second	the state of the state	
	The sets major lands	The set of a last		the set within presi-	
and second in some	the sea heave that	the star teach worth	The set have not	OA DE DENG LATER	
	the set while terms	The set patter period		OA SHI NEED LATER	
NO TRADE LAND			The sec result server	OF NO 16HO HILL	
	The sea made uses	The bell heads town	The second upon	124 TO 10040 1PMD	
BC 14114 14190	12 IN 11 IN 123	the set owing lower		Two they wellow 147401	
		The second second	the second second	The second second second	
	the set of the later		The second second second	the set of the set	
	the state of the local	the set of a set	the second second	the said willing through	
	the state many service	the set makes upon		The second second	
and the second second	the set only in-	the set of lat later.	the part of the literature	the set that is not	
the second particular	the set mailer ( +-10)	the sky real at least	Der per belle under	the second second	
and which had the	The Real Prints Lands	The second parts	The Rep research party		
		the ball being torth		the stal manage letter time of	

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 AESEncryptionAlgorithmtoEnhanceDataSeftyinC loudComputing"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.