Ensure Data Security and Privacy using DNA Symmetric Encryption Method in Cloud

Dr. R. Sugumar, L. Leelavathy
Professor & Director,
ChristhuRaj College, Panjapoor, Tiruchirappalli, Tamil Nadu India
Research Scholar,
ChristhuRaj College, Panjapoor, Tiruchirappalli, Tamil Nadu India
rsugusakthi1974@gmail.com, leelakarthikeyen@gmail.com

Abstract
Cloud computing has changed the way mankind uses its technical expertise. Broadly speaking, it marks a transition in the use of computers as utility tools with extreme applications. An emerging technology, cloud computing is rapidly changing the texture of the technology landscape and now is focus of increased attention. Cloud storage is a young industry that shows great promise for growth. Large organizations have started showing interest in using it and are moving their data to the cloud. The unique architecture of the cloud not only offers unlimited storage capacity but also says the ground work for eliminating the need for periodic backup. The security is playing the major role in the cloud environment; the data users often store significant information with cloud. The providers may be unsafe. So the end users are speculating about attacks on the integrity and the availability of their data in the cloud from malicious insiders and outsiders, and from any indemnity damage of cloud services. These matters are tremendously significant but there is still ample area for security research in cloud computing environment. This paper is to propose a DNA based encryption algorithm it crops the data security in cloud storage.

Keywords: DNA, Security, cloud, Security, data center, Encryption algorithm.

1. Introduction
Cloud computing [1] has the current generations utility computing. It is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service [2] provider interaction. The National Institute of Standards and Technology (NIST) [3] [4] defines cloud computing by five essential characteristics, three service models, and four deployment models. The essential characteristics are on-demand self-service, location-independent resource pooling, broad network access, rapid resource elasticity, and measured service.
The foremost three service models are software as a service, platform as a service, and infrastructure as a service. The deployment models include private cloud, public cloud, community cloud, and hybrid cloud. Nowadays, cloud-computing paradigm can offer any conceivable form of services, such as computational resources for high performance computing applications, web services, social networking, and telecommunications services. In addition, cloud storage in data centers can be useful for users to store and access their data remotely anywhere anytime without any additional burden. However, the major problem of cloud data storage is security. Therefore, cloud data centers should have some mechanisms able to specify storage correctness and integrity of data stored on cloud. With the extensive application of cloud computing, more and more sensitive information and private data are stored in the cloud by users. Cloud data storage security is one of the important security issues in cloud computing. In order to protect the privacy of end users data, cloud data should be stored in the form of ciphertext. But encryption adds computational cost. It is expected that the confidentiality of the data will be assured at the lowest likely cost. Since cloud service providers are unreliable third parties, how to keep data confidential to cloud service providers and allow cloud service providers to complete many operations on data, it is problematic for traditional encryption methods to solve the above problems.

So information security becomes necessity for modern computing systems. There are some sectors like government, banks, military who can’t afford any leaks to their secret data. From our past to till date the secret writing techniques are used to protect the data from the adversaries and the techniques such as cryptography and steganography are most common and widely used methods. Cryptography performs the encryption of the data whereas steganography hides the data from the hacker. In cryptography the encryption and decryption of data (plaintext) is done with the help of key. The maximum secure and presently used technique is the modern approaches of cryptography which involves abundant mathematical computations and two types of keys, the public and private keys. Nowadays, there is additional newly emerging cryptographic technique in the field of cryptography called DNA cryptography. The main impartial of this method is to encrypt the plaintext and hide it in the DNA digital form. DNA cryptography enables the confidentiality of data further high then the modern methods with the use of one time pad keys and its size. Also it is believed that in DNA cryptography the key can be made for the huge length of data compared to the recent methods in which key are generated only for smaller length of the data. Also with the breaking up of modern cryptographic algorithm like DES and MD5 the new methods of information security are needed to protect our data. The concept of DNA computing plays an imperative role in the field of computer security which is expected to be a extra influential and strong cryptographic algorithm now a days. The DNA encryption technology supports the management of ciphertext data under privacy protection.

1.1 DNA
DNA stands for Deoxyribonucleic acid which store genetic information of the entire living organism ranging from human being to small viruses. It is also called as an
information carrier and consists of long polymer of small units called nucleotides. Further nucleotides consist of three components: Nitrogenous base, five Carbon sugar and Phosphate group. Nitrogenous base consists of four bases: Adenine, Thymine, Cytosine and Guanine (A, T, C, G), all the complex information about organism are stored with the combination of these bases. Adenine and Guanine are called purines, whereas Thymine and Cytosine are called pyrimidines. DNA is a double helix structure as shown in the Figure below.

2. Related Work

In this paper the author proposes a technique for DNA cryptography based on dynamic mechanisms and ‘dynamic DNA encoding’. To form dynamic sequence table: initially, DNA base sequences are assigned to 256 ASCII characters randomly. Where to attain dynamism, positions of DNA base sequences are reorganized iteratively following a mathematical series. Also, to form dynamic DNA encoding: the use of NCBI bank genome sequence with a mathematical series dynamically settles the number of DNA bases required to merge the ciphertext of every two chunks. Here, the way of encryption is to transform the plaintext into DNA bases. ASCII characters using dynamic sequence table, to divide these data into a finite number of chunks, to encrypt them by an asymmetric cryptosystem, and finally to merge the ciphertext of chunks through dynamic DNA encoding. Therefore, the usage of dynamic mechanisms along with an asymmetric cryptosystem obviously improves the secrecy level of data. Lastly, the outcome of the proposed technique, a comparative study with existing methods, the security analyses, and a statistical test according to the National Institute of Standards and Technology to analyze the randomness of the generated ciphertext are presented.[10]

Data safety in IoTcloud is a daunting task. Since IoTdevices are all stored in the cloud, therefore IoTcloud requires data protection. In the approach provides 2-level security for data and insists on using Huff-man coding algorithm for main group and using DNA cryptography for data protection. The approach uses symmetric key cryptography. Upcoming effort will focus on using asymmetric key cryptography for cryptanalysis. Data security is the main challenge for cloud service. RSA, Diffie-Hellman, DNA encryption etc. are available to provide data protection for data stored on the cloud such as cloud, digital signature. The Extensible Authentication Protocol is used for authentication. It get 2-layer protection for the ASCII character set. The system focuses on expanding the BDEA algorithm used with the UDICode character set. This can help cloud users reach a wider community. [11]

The author grouping of symmetric-key and asymmetric-key encryption technique for securing data in IoTCloud. Symmetric-key algorithm require low RAM for making in this way it stretches fast. When compared with symmetric-key algorithm, Asymmetric key encryption does not having any issue to skill the key. For settling key transport issue in symmetric-key encryption and to get the choice, proposed strategy and RSA
calculation are consolidated together. Hybrid encryption is achieved finished information exchange utilizing special session keys alongside symmetrical encryption. One promising position is that association channel is built up between two clients' arrangements of gear. Clients at that point can interface through hybrid encryption. Uneven encryption can back off the encryption procedure, however with the concurrent utilization of symmetric encryption, the two types of encryption are used. The outcome is the additional security of the transmittal procedure alongside generally enhanced system performance. In a usage, the Asymmetric key calculation that is RSA is utilized just to encode the symmetric key, for this it requires lesser computational cost. The strategy utilizing DNA cryptography and Huffman coding for encoding and decrypting data.[12]

Many groups are indifferent to use cloud services due to data security issues as the data resides on the cloud services provider’s servers. To talk this issue, there have been several approaches applied by various investigators worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm 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 work focuses on enhancing the BDEA to use with theUnicode characters. 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, in this achieve 2-layer security for ASCII character sets. This can help reach to the wider community of the cloud users. [13]

The idea of huge parallelism and great information density inherent in DNA molecule are exploited for cryptographic drives. Now, the main difficulties of DNA cryptography are the requirement of high tech bimolecular laboratory and computational complexity. In this paper, a new parallel cryptography technique is proposed using DNA molecular structure, one-time-pad scheme and DNA hybridization method which certainly minimizes the time complexity. An original DNA cryptography technique by using DNA digital coding technique and DNA hybridization. It can be concluded from the analysis of the method that the DNA cryptography method promises to be a better solution for implementation in secure network.[14]

Cloud computing, distributed resources are shared among users by incomes of networks. The data is available to the users from anywhere. In meanness of various benefits of cloud storage, there are still lots of interferences concerning security and privacy of the data that need to be set. Though, the cloud simplifies elastic and easy to access data storage and organization, there are still possibilities of illegal attacks and malicious activities. The cloud server may store confidential and sensitive data. So, the security of the data is of major concern. Cryptography methods offer a secure for private
data storage at the third party by incomes of encryption and grant its corresponding key to the authorized user only. In this work, a novel symmetric key cryptographic technique has been planned which is inspired by DNA cryptography. In this scheme uses dynamic encoding tables that are random in nature which leads to higher security. [15]

This work improvises the randomization for key generation, encryption, and decryption from the ElGamal cryptosystem, and this algorithm, key generation is a time-consuming one, since it will be done periodically, it is tolerable. And also it proves the user authentication of the Data Owner and the Data User thereby resulting in secure transfer of the key file between the Data Owner and the Data User. EEC security trusts on the effort of randomness and the separate problem. The author says the DNA cryptosystem provides data confidentiality for the data transferred between the Data Owner and the Data User in a cloud computing environment. The DNA nucleotides are recycled to completely hide the original data for a secure communication. The dynamic group of encoding table and intron sequence decreases the option of cryptanalysis and also enhances the security of data. The biological properties of DNA make the system yet more randomized and a prudent system as well as becomes the efficient system in practice while most of the DNA cryptosystems are theoretical. The possibility for an attack on the cloud environment for cryptanalysis is hard due to the dynamicity of cryptosystem. [16].

Cloud computing has transformed the way the data is stored, processed and made available. It has changed in numerous forms of utility computing through sharing resources, infrastructures and data storage facilities and got wide acceptance because of its services and storage capacities. But security issues are a major concern in the cloud which is restricting its use among organizations which deals with sensitive data such as health care, Pharmaceuticals etc. and remain one of the greatest inhibitors for the adoption of Cloud computing if the security issues continue. For data defense, various techniques evolved through years for Ciphers, Cryptography, Steganography and recently DNA based encryption for security is the trend. DNA cryptography was a breakthrough in the field of security which uses bio-molecular ideas and gives us new hope of unbreakable algorithms but the concepts need to be exploited more particularly in the cloud computing. This paper discusses cloud computing features, service models, and security issues and proposes a DNA based encryption algorithm for securing data in cloud environment which will be cost effective and secure by using bio-computational techniques. The suggested algorithm uses indexing and DNA steganography techniques along with binary coding rules which make algorithm secure as it is an additional layer of bio-security than conventional cryptographic techniques. [17]

DNA Cryptography is the division of computing. One gram of DNA covers 700 terabytes of data. So it is a actual compact way to store the huge amount of data. DNA
Computers are very wanton as compared to electronic computers. DNA computer wants very few power requirements as compared to contemporary automatic machines. Hybridization of DNA, DNA synthesis technology, DNA –chip-based technology, the Central view of molecular biology, PCR amplification technology, and OTP are used in DNA cryptography to make it secure then old-style cryptographic schemes which are indestructible by the attackers, due to molecular calculation inherent in it. Symmetric and asymmetric keys are used to deliver security to the application. DNA cryptography has an extensive range of applications and can be implemented in various arenas like mobile networks, cloud computing, IoT devices, Real-time applications, Internet, multicast applications to secure plain-text messages, videos, servers, images, etc. There are some limitations of DNA cryptography depend upon the technology used, keys used, and size of data.[18]

The current cloud technologies have altered the perspective of architecture, development and delivery models by providing on-demand services via the internet. It has become extra difficult to secure significant information from unwanted users. DNA cryptography shows a vital role in transforming important information into an encrypted form. In this paper, a new hybrid flower pollination algorithm with DNA cryptography, it is a nature-inspired algorithm that assists to find the optimal solution whereas DNA cryptography helps to encrypt a large number of data in few grams of DNA. So this is an extended version. The work extends the level of security by implementing optimization including random key values. The work is entirely based on the random and optimized numbers so that no users can predict the level of randomization. The time complexity of the work demonstrates the feasible nature of the algorithm. [19]

The dependency on computers for secure communication from machine to machine connected virtually has been grown. Cryptography supports to lessen such data security issues and change information into an unreadable form based on the key. This paper is based on the new technique based on the DNA cryptography along with Genetic Algorithm. Keys are generated using Genetic Algorithms that is measured as one of the most optimization technique. Each letter and the numerical value is encoded and converted into DNA sequence of nucleotides bases (As, Cs, Gs, Ts). In this work, a method is presented for generating a key using Genetic Algorithm and implementation of Encryption and Decryption using DNA cryptography. The Algorithm is completely based on the new cryptosystem where a key is generated using an optimized technique and applied to the text using DNA cryptography. Every individual has unique DNA and the transmission of genes from one generation to another and DNA founded algorithms are measured as a revolutionary system. [20].

3. PROPOSED ALGORITHM

The projected way to progress the classical encryption techniques by integrating substitution & transposition cipher. This two substitution and transposition techniques
have used alphabet for cipher text. In this proposed algorithm, 1st stage the plain text is converted into corresponding ASCII code (Hexa) value of each alphabet. In classical encryption technique, the key value ranges between 1 to 26 and key may be string (combination alphabets). But our proposed algorithm, key value range between 1 to 256. The next stage DNA procedure is used for this algorithm in order to encrypt the data of the user in the cloud environment. The end users can store data on demand or for the applications without keeping any local copy of the data on there machine. Since the user has no control over the data after his period is logged out, the encryption key play the very important part and its primary authentication for the user. The proposed DNA base algorithm is described below.

The given steps are the encryption algorithm steps.

Algorithm: 1 Encryption

Step 1: Count the No. of characters (N) in the plain text Without space.
Step 2: Convert the plain text into equivalent ASCII code. And form a matrix.
Step 3: Apply the converted HEXA code value form the Matrix.
Step 4: Take the even column (2, 4) vales Rewrite and odd column values (1,3) values rewrite to form the following order wise
Step 5: Take the key values (DNAC) 44,4E, 41, 43 and Ex-Or with the each row of the matrix.
Step 6: Convert the HEXA code into encrypted DNA code and the value into the matrix in the same order.
Step 7: Read the message by column by column. Using the key values (key values 3,1,4, 2)
Step 8: The Converted DNA value as the Cipher Text.

The followings are the detailed step in the encryption algorithm.

Step1: Count No. of characters (N) in the message without space.
Plaintext – CLOUDSYSTEMSECURITYD
N= 20 (N = No. of Characters in the Message)
Step 2: Convert the plain text into equivalent ASCII code. And form a square matrix.
ASCII code value for the plaintext (Hexadecimal Code)
43,4C,4F,55,44,53,59,53,54,45,4D,53,45,43,55,52,49,54,59,44
To form a matrix Form a 4 X 5 matrix.

Matrix = A

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>4C</td>
<td>4F</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>53</td>
<td>59</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>45</td>
<td>4D</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>43</td>
<td>55</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>54</td>
<td>59</td>
<td>44</td>
<td></td>
</tr>
</tbody>
</table>


Step 4: Take the even column (2,4) values Rewrite and odd column values (1,3) values rewire to form the following order wise

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>4C</td>
<td>55</td>
<td>43</td>
<td>4F</td>
</tr>
<tr>
<td>53</td>
<td>53</td>
<td>44</td>
<td>59</td>
</tr>
<tr>
<td>45</td>
<td>53</td>
<td>54</td>
<td>4D</td>
</tr>
<tr>
<td>43</td>
<td>52</td>
<td>45</td>
<td>55</td>
</tr>
<tr>
<td>54</td>
<td>44</td>
<td>49</td>
<td>59</td>
</tr>
</tbody>
</table>

Step 5: Take the key values (DNAC) 44, 4E, 41, 43 and Ex-Or with the each row of the matrix.

4C = 4 C
0100 1100

Key 44 = 0100 0100
0000(AA) 1000(GA)

Step 6: The above result encrypted by the DNA code and value into the matrix in the same order
Step 7: Read the message by column by column. Using the key values (key values 3, 1, 4, 2)

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>4</th>
<th>1</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>AA</td>
<td>TA</td>
<td>AA</td>
<td>AT</td>
</tr>
<tr>
<td></td>
<td>GA</td>
<td>CA</td>
<td>CA</td>
<td>GC</td>
</tr>
<tr>
<td>4</td>
<td>AA</td>
<td>AT</td>
<td>TA</td>
<td>AT</td>
</tr>
<tr>
<td></td>
<td>TT</td>
<td>TC</td>
<td>CA</td>
<td>CG</td>
</tr>
<tr>
<td>1</td>
<td>AT</td>
<td>AA</td>
<td>GC</td>
<td>AT</td>
</tr>
<tr>
<td></td>
<td>TT</td>
<td>AT</td>
<td>GG</td>
<td>CG</td>
</tr>
<tr>
<td>3</td>
<td>AA</td>
<td>TA</td>
<td>AT</td>
<td>CA</td>
</tr>
<tr>
<td></td>
<td>TA</td>
<td>TA</td>
<td>GG</td>
<td>AA</td>
</tr>
<tr>
<td>2</td>
<td>AA</td>
<td>AT</td>
<td>AT</td>
<td>AA</td>
</tr>
<tr>
<td></td>
<td>GA</td>
<td>AA</td>
<td>GG</td>
<td>GG</td>
</tr>
</tbody>
</table>

Encrypted Text:

ATGCAACATACAAAAAGATCGATGGATTCAATTATGGGAACGAAATATTTAATA
ATTGTATAAATAAAGAATGGATAAAAGA

The encrypted data is stored in the cloud storage. To retrieve the data from cloud, the decryption process is essential to get the actual data in the cloud storage area. Decryption is possible only with key values which are used for encryption algorithm. So the key plays the major and main role in the encryption and decryption algorithm.

The given steps are the decryption algorithm steps.

Algorithm: 2 Decryption
Step 1: The encrypted DNA text is to form the matrix column by column. Using the key values (key values 3,1, 4, 2)

Step 2: the same matrix again to form by use the key (2,4,1,1)

Step 3: Take the key values (DNA( 44, 4E, 41, 43 and Ex-Or with the each row of the matrix.

Step 4: Take the even column (2,4) values Rewrite and odd column values (1,3)values rewire to form the following order wise and arrange the data in proper matrix order (1,2,3,4)

Step5: Apply the converted DNA code to HEXA code and form the Matrix

Step 6: Convert the ASCII code into equivalent character value. Then, Decrypted result is, CLOUDSYSTEMSECURITY

The followings are the detailed description of each step in the decryption algorithm.

Step1: The encrypted DNA text is to form the matrix column by column. Using the key values (key values 3,1, 4, 2)

EncryptedText:
ATGCAACATACAAAAGATCGATGGATTCAATTATGGAACGAAATATTTAATAATTGTATAAATAAAGAATGGATAAAAGA

Step2: the same matrix again to form by use the key (2,4,1,3)

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>AA</td>
<td>TA</td>
<td>AA</td>
<td>AT</td>
</tr>
<tr>
<td>AG</td>
<td>CA</td>
<td>CA</td>
<td>GC</td>
</tr>
<tr>
<td>AA</td>
<td>AT</td>
<td>AT</td>
<td>AT</td>
</tr>
<tr>
<td>TT</td>
<td>TC</td>
<td>GG</td>
<td>CG</td>
</tr>
<tr>
<td>AT</td>
<td>AA</td>
<td>AA</td>
<td>AT</td>
</tr>
<tr>
<td>TT</td>
<td>AT</td>
<td>CG</td>
<td>GG</td>
</tr>
<tr>
<td>AA</td>
<td>TA</td>
<td>TA</td>
<td>AT</td>
</tr>
<tr>
<td>TA</td>
<td>AA</td>
<td>TG</td>
<td>CA</td>
</tr>
<tr>
<td>AA</td>
<td>AT</td>
<td>AT</td>
<td>AA</td>
</tr>
<tr>
<td>GA</td>
<td>AA</td>
<td>GG</td>
<td>GG</td>
</tr>
</tbody>
</table>
Step 3: Take the key values (DNAC) 44,4E, 41, 43 and Ex-Or with the each row of the matrix.

\[
\begin{align*}
4C &= \quad 4 \quad \text{C} \\
&= \quad 0100 \quad 1100
\end{align*}
\]

Key 44= 
\[
\begin{align*}
0100 &\quad 0100 \\
0000(\text{AA}) &\quad 1000(\text{GA})
\end{align*}
\]

Step 4: Take the even column (2,4) vales Rewrite and odd column values (1,3) values rewire to form the following order wise .

\[
\begin{array}{cccc}
2 & 4 & 1 & 3 \\
4C & 55 & 43 & 4F \\
53 & 53 & 44 & 59 \\
45 & 53 & 54 & 4D \\
43 & 52 & 45 & 55 \\
54 & 44 & 49 & 59 \\
\end{array}
\]


\[
\begin{array}{cccc}
1 & 2 & 3 & 4 \\
43 & 4C & 4F & 55 \\
44 & 53 & 59 & 53 \\
54 & 45 & 4D & 53 \\
45 & 43 & 55 & 52 \\
49 & 54 & 59 & 44 \\
\end{array}
\]

Now the message is,
43,4C,4F,55,44,53,59,53,54,45,4D,53,45,43,55,52,49,54,59,44

Convert the ASCII code into equivalent character value. Then, Decrypted result is,

plain Text: CLOUDSYSTEMSECURITYD
By end of all these steps in the decryption algorithm the original text is retrieved by
the user.

4. CONCLUSION
The cloud computing environment Security and Privacy are significant part in storing of
data in that location. So abundant researchers are work in that area. Cryptographic
techniques are used to provide secure communication between the end user and the
cloud. This paper proposed an encryption algorithm for secure data storage in cloud
storage. The proposed DNA cryptographic technique introduces dynamic mechanisms to
enhance the secrecy level of data. Though encryption, originally the exploitation of
dynamic sequence that holds the characteristics of substitution cipher ensures level of
secrecy. Currently to increase its privacy, finally, its security the usage of dynamic DNA
encoding that maintains the properties of product the iterations, the DNA base
sequences, are also associated with its secrecy. A upcoming idea is to apply the proposed

References

and Traceable Group Data Sharing in Cloud Computing”, IEEE Transactions On
Information Forensics And Security, Vol. 13, No. 4, April 2018.

data sharing for resource-limited users in cloud computing”, Available online at
www.sciencedirect.com journal homepage: www.elsevier.com/locate/cosecomputers & s
ecurity 72, 2018.

Research in Computer Science, Engineering and Information Technology, IJSRCSEIT

Recent Advances in Cloud Computing Security”, Journal of Next Generation
Information Technology(JNIT), Volume9, Number1, Mar. 2018.

Bose, Kaushik Basu, Saunak Chaudhury, Pritika Sarkar “Cloud Computing Security
Challenges & Solutions-A Survey”, IEEE, DOI: 10.1109/CCWC.2018.8301700 2018,
Conference Paper • January 2018.


