International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 4007–4014

Hybridization of Cryptography for Security of Cloud Data

Jaydip Kumar[1*], Prof. Vipin Saxena[2]

Department of Computer Science,
Babasaheb Bhimrao Ambedkar University (A Central University),Lucknow, India
Itsme.jay92@gmail.com[1], profvipinsaxena@gmail.com[2]

Abstract

Due to evolution of distributed computing, many of the on line system related to banks, financial organizations, etc are transferring the importent information from administrator to the users through the cloud server provided by the various internet providing componies. The basic question is that whether the transformation is highly secure or not. The main propose of this paper is to indroduce a hybrid approach in the form of algorithm for securing the information with high integrity, less time consuming and more confidentiality . The presented algorithm has been implemented by taking an example, object oriented Python Programming language is used for implemented of example and results are displayed in the form of table and figures.

Keywords: *AES Cryptography, Cloud Data Security, DNA-genetic algorithm, Hybridization, Public key cryptography.*

1. Introduction

In the current era of computer technology, “Cloud Computing” is a rapidly growing technology for the development of information in text, audio, and video for the use of industries. Many industries have shifted the old databases to the cloud and day by day, data is increasing. Cloud Computing was initially proposed by the National Institute of Standards and Technology (NIST) in the year 2006 for storing the local computer data storage into centralized data storage. Many industries are having a fear of the leakage of data from the cloud. Recently, the Paytm database in India has been leaked, which is related to the creditors and accounts' details. Therefore, storing cryptographical encryption is necessary at the time of retrieving the data from the cloud.

The cryptographical techniques are used to encrypt or decrypt the cloud information according to authorized security. It is a mathematical study of information security like confidentiality, authentication and data integrity, it may be of two forms one is symmetrical cryptography and the other is asymmetrical cryptography. The symmetric security algorithm has a generic key shared between the sender and receiver, while asymmetric key algorithms are used with different keys for encryption and decryption [2][24]. The public key encryption is based on computationally extensive mathematical functions such as Rivest-Shamir-Adleman (RSA). The three main functions in RSA are key generation, encryption and decryption and the best example of symmetric cryptography is Advanced Encryption Standard (AES), which uses various bits length keys such as 128, 192 and 256. It is a combination of Exclusive-OR operation, octet substitution with S_box, row and column rotations and a mixed column in the flow of algorithm [12]. The transmission of a secret message by hiding and avoiding a malicious attack on data and fulfilling safe transmission has become more powerful. From recent research, DNA has a few inherent properties that can be used in the encryption technique [7]. The DNA technology is used for ciphering, deciphering cloud data with high security and less predictable [2].

ISN: 2233-7857 IJFGCN

To enhance the cloud data storage security, a multilevel encryption technique can be used. In the present work, the proposed model has the ability to fulfill both efficiency and security factors with the highest secrecy value. The combination of different layers of encryption provides higher secrecy values are compared to single-layer encryption.

2. RELATED WORK

Many different evaluation approaches for AES, RSA and Genetic techniques have been proposed in the literature. Let us describe some of the important research work related to the present work. In a review paper, the author provided some previous information about hybrid encryption and related techniques and compared some techniques to keep information secure and redundant. By using techniques, the user can secure and protect their personal information from the hackers[3].In cloud computing, kuswaha et al. presented the different cryptographic algorithms using RSA and AES algorithms to enhance the secure data transmission over the network[1]. The single algorithm is not efficient for high-level information security requirements. Therefore, hybrid encryption using AES, ECC, and RSA methods to improve security in terms of encryption and authentication by using proposed combinations, the information is converted into ciphertext using AES and ECC[4]. In the cloud computing hybrid encryption, the technique is used to improve the integrity of data in between the sender and receiver, the advantages of the asymmetric algorithm like RSA which depends on the crucial process of factorization of a large prime number and the key generation DSA is combined with proposed algorithm and symmetric encryption is faster than the asymmetric encryption so that AES S-Box is used to hash the ciphertext obtained [12]. For providing more confidentiality of secure data, kumar et al. implemented a highly secure cloud security model with the combination of RSA and AES[13]. The key expansion techniques are used to enhance the security operations in AES key expansion because of the huge difference between the Mixcolumns and Inverse Mixcolumns[14]. In the cloud computing, transferring and storing passwords in plaintext is a risk from the raider, snoop, and spyware and bypassing this type of exposure. The strongest encryption or validation uses distinct techniques to minimize the probability of unencrypted information. The author's proposed a technique to protect data transmission using three different security techniques like AES, RSA and HMAC is used to encrypt data and password for transferring between client and server or client to client and verification from client to server and design it more secure to exposed from the attacker[15]. The art of designing ciphers, stream ciphers and block ciphers and hash function is called cryptographic technique that enables the cloud security services such as confidentiality, integrity, authority, availability, and non-repudiation to ascertain all these services, Abdelnapi et al. proposed an effective method to improve the security of data and proposed hybrid encryption with a hash function that uses RSA and AES with secure hashing (SHA 256) algorithm [6].

In cloud computing, the DNA encryption technique makes cloud computing high security less predictable. Using this technique, binaries or any type of digital signals are converted into DNA sequencing, reshaping, encryption, crossover, and mutate and then reshape and the main advantages of D-GET[2]. Information security is a significant concern for the individual or any organization for securing information. One of the authors proposed encryption and decryption of a three-layered technique that can encrypt or decrypt any characters or symbols using Genetic Algorithm (GA) or other implicit properties of Residue Number System (RNS). The presented technique result can encrypt a message with enhanced throughput that encrypts small and large messages [5]. To provide the secrecy of the relevant information, DNA cryptography plays a significant job on the data encryption model based on DNA technology has offered to transmit. Cloud information security pursuance the given model a message encrypted to a DNA sequence by using a

ISN: 2233-7857 IJFGCN

single mapping rule table and further canceled in DNA plasmid by recombination of DNA sequence[7].

In cloud computing One-Time Pad(OTP) is a base technology for the key generation used for stream ciphering and provides information with privacy. The OTP encryption has been proved nonbreakable in theory, but in the practical application, it is difficult to realize and the DNA cryptography is recent and trustable for information security [8]. A new model has been proposed for access control for Big data to store large files[9]. The first and second DNA proposed algorithm was implemented in java and Bio Java, MATLAB. Presented a comparison study of first and second DNA algorithms and implemented a new step to improve the security method using a DNA security algorithm through asymmetric key generation [16]. The DNA sequence has a few unique properties, namely, insertion, complementary pair and substitution method, complementary pair method and substitution method which can be utilized to hide the

information due to using these methods and DNA sequence S is selected and message M is combined with it so that S' is obtained and robustness and the tightly embedded capacity analysis of these methods are manifested [11]. Sindhuja and Devi presented a

genetic algorithm (GA) using a symmetric key that is used for encryption or decryption of plaintext text are changed over into text matrix and key are into the key matrix and adding both matrices by using additive matrix and for getting ciphertext from the additive matrix used by linear substitution function and forgetting the final cipher used by GA functions (crossover and mutation) [17]. The changeability in the data is called entropy. The entropy of the data is directly proportional to the security of the corresponding data. Cloud security is the most compatible and mandatory feature of cloud data transfer and storage based on different services. According to the above detailed genetic algorithm, users need to give plaintext and key and these datasets. The algorithm will provide ciphertext and encryption has been achieved [18]. It is dangerous and can turn into a threat if it falls into the wrong hands. To protect data, encryption is one of the most widely used technologies and proposed Genetic Algorithm (GA) operation with pseudorandom function are used to encryption and decryption of information and encryption process applied over the binary information so that this algorithm can encrypt any type of information over the internet[19].

3. CONFIDENTIALITY OF CRYPTOGRAPHIC TECHNIQUES

3.1. DNA-Genetic Algorithm

The DNA technique is implemented for information ciphering and deciphering in the advanced digital world but not at the molecular level[10]. The DNA contains nucleic acid, which contains genetic information and the DNA has the four nucleotide bases, $\sum$ = (A, C, T, G), Adenine (A), cytosine (C), Thymine (T) and guanine (G). The gene is used in the DNA sequence that contains the genetic data of all the alive things and three approaches to transform information from any binary information to the DNA sequence to an amino acid. It is a DNA based bio-molecular security technique that is based on DNA and carbon nanotube messages, which are used for transferring data between DNA and binary storage [2].

The nucleotides in DNA sequence has been used as given in table 1.

ISN: 2233-7857 IJFGCN

Table 1: DNA Sequence table

DNA	Bits
A	00
C	01
G	10
T	11

From the above table B is generated as CGAG and in the binary form it is 01100010. The DNA algorithm is represented below [10].

Step 1. Define a genetic evaluation of issues;

Step 2. First, create the leading population $Q(0) = a_{1,}^{0} a_{2,}^{0} a_{3}^{0} \ldots\ldots\ldots\ldots a_{N,}^{0}. Set\ t = 0$;

Step 3. To calculate the average fitness value $\int t = \sum_{i}^{N} \int (a_i)/N$ and provide to every particular, the normalized fitness value is $\int (a_i) / \int (t)$

Step 4. Select every a_i possibility $q(a_i, t)$ is proportional to its normalized fitness value. By using the distribution, choose N vectors from the $Q(t)$. By using this get the group of selective parents.

Step 5. Forming $N/2$ pairs from every parent at random and set up a new population $Q(t+1)$ by applying crossover and mutation.

Step 6. After Setting $t = (t+1)$, return to step 2.

The steps of above algorithm are represented in the following flow diagram.

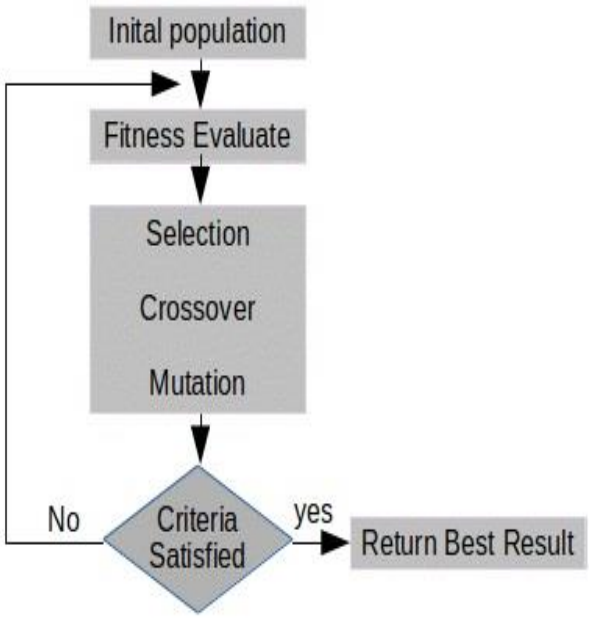

Figure 1. Flow Diagram for DNA Algorithm

3.2 Rivest-Shamir-Adleman (RSA)

RSA is asymmetric cryptography that uses the public and private key to encrypt plain text and decryption of ciphertext, which are integer formate between 0 to n-1 for some n

ISN: 2233-7857 IJFGCN

[19]. It is a combination of three steps, such as key generation, encryption, and decryption. It is mostly used in electronic commerce protocol because its security level depends on the decomposition of large numbers [4]. RSA is used for small or large scale of information or used for key exchange digital signature it uses variables key size and encryption block size and the key pairs come from large prime numbers [15]. The steps of the RSA algorithm are given below.

A: key generation (public & private keys)

Step 1. choose two distinct prime number pr1, pr2 with equal size.

Step 2. n= (pr1 * pr2)
Step 3. ∅(n)= (pr1 -1) * (pr2 -1)
Step 4. generate encryption key e which must be co-prime of ∅(n)
Step 5. calculate $d= e^{-1} mod \varnothing(n)$
Step 6. RSA pub_Key (e, n)
Step 7. RSA priv_key (d, n)

B: Encryption

Step 1. Message for encryption m, m < n
Step 2. the ciphertext of a message $c = m^e \pmod n$

C: Decryption

Step 1. Cipher Text at receiver end c
Step 2. Message $m = c^d \pmod n$

The RSA algorithm has also been represented in the following flow diagram.

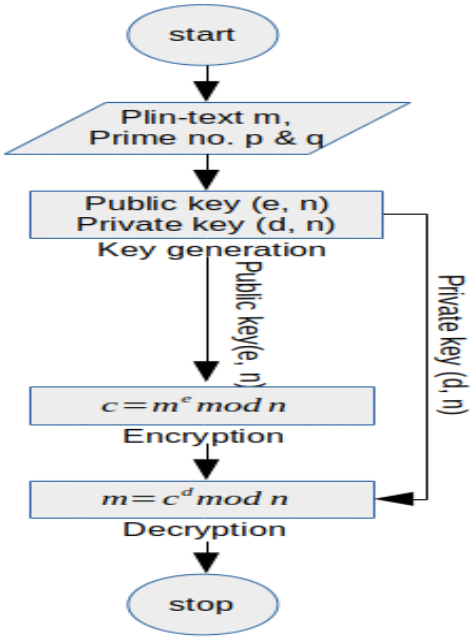

Figure 2. Flow Diagram for RSA Algorithm

ISN: 2233-7857 IJFGCN

3.3 Advanced Encryption Standard (AES)

AES is a symmetric cryptography, which is replaced by DES. In comparing public-key algorithms such as RSA, the structure of AES is more complicated than any other cryptographic technique. The cipher-text takes plain-text block size of 128, 192 and 256 bits and the algorithm referred to as AES-128 bits, AES-192 bits and AES-256 bits these are depending on the key length. The AES block cipher consists of N rounds, which depends on the AES key length AES-128, AES-192 and AES-256, respectively (10, 12 and 14 rounds). The N-1 AES rounds consist of different transformation techniques like SubBytes, ShiftRows, MixColumns and AddRoundKey and the last round contains only three transformation techniques like ByteSub, ShiftRow and AddRoundKey [19]. The following are the steps of AES.

A: SubBytes Transformation

SubBytes is a simply 16x16 matrix of byte values called as s-box that is combination of all possible combination of 8 bit sequence ($2^8 = 16 x 16 = 256$) [21].

B: ShiftRow Transformation

The ShiftRow is simple permutation and nothing more.

- The first row of State is not altered.
- The second, thrid and fourth row shifted left 1byte, 2 byte and 3byte in a circular manner [21].

C: MixColumn Transformation

This step is basically a substitution but it makes use entries in GF(2^8) and each column operated individually and the transformation is determined by the multiplication of the states [21].

D: AddRoundKey

In AddRoundKey transformations, the 128 bits which arranged in a 4x4 matrix consisting of bytes XORed with the output of the MixColumn step[20].

The above steps are represented in the following diagram:

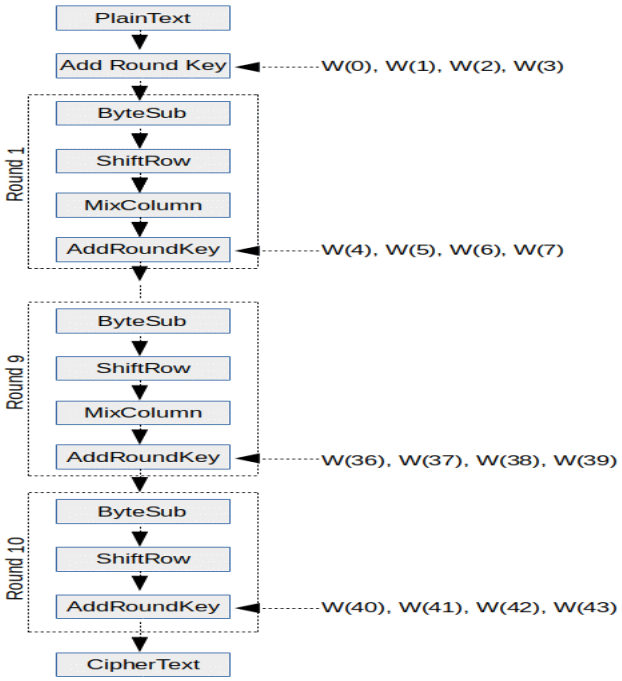

Figure 3. Flow Diagram for AES Encryption

ISSN: 2233-7857 IJFGCN

3.4 One-Time Password (OTP)

Password-based authentication is still secure for online services, One-Time-Password, which is a two-factor authentication scheme and an enhancement of the conventional username-and-password scheme. One-Time-Password is authenticated by users by agreeing on a pre-shared value's authority, which is the most secure factor in Two Factor Authentication (TFA) [22].

In the recent era, SMS-OTP is mostly used for authentication and authorization for different online services that provide a higher-level of authentication assurance, that is more secure for online payment services and One-Time-Password SMS, the user can use in the transaction only at one time any other user cannot use this password in the different transaction or same user at the second time. For using the security system the generated OTP is hard to guess or retrieve or trace by the hacker. There are different factors for OTP algorithms to generate difficult to guess.

- **IMEI number:** stands for International Mobile Equipment Identity, which is a unique number of each mobile devices that cannot be changed anymore
- **IMSI number:** International Mobile Subscriber Identity, which is a unique number provided by all network providers which store in-network provider's database.
- **Hour:** Details about OTP generated in each hour.
- **Minute:** This makes the OTP generated in each minute.
- **Session:** This makes the details about how many OTP generated in each session-id and after the session expires, all the OTP generated in a particular session will not work [23].

4. Proposed Algorithm

A hybrid cryptographic algorithm is the combination of different symmetric, asymmetric and DNA genetic algorithms. The benefits of the combination of different algorithms to provide the secure transportation of information between the user and cloud. The combination of both symmetric and asymmetric techniques provide authentication, integrity, and confidentiality. AES key is encrypted by the RSA algorithm to make secure data transmission and provides more efficiency. The steps of the proposed algorithm are given below.

Step 1: Key Generation (By RSA algorithm)

- choose two distinct prime number pr1, pr2 with equal size;
- n= (pr1 * pr2);
- ∅(n)= (pr1 -1) * (pr2 -1);
- generate encryption key e which must be co-prime of ∅(n);
- calculate $d = e^{-1} \bmod \emptyset(n)$;
- RSA pub_key (e, n);
  RSA priv_key (d, n);

Step 2: Encryption

Level 1: $AESCipher = ENC_{AES,\,pubkey}(message)$

Level 2: $DNACipher = ENC_{DNA,OTP}(AESCipher)$

Step 3: Decryption

Level 1. $AESCipher = DEC_{DNA,OTP}(DNACipher)$

Level 2. $message = DEC_{AES,\,prikey}(AESCipher)$

ISN: 2233-7857 IJFGCN

In the proposed algorithm, private and public keys are generated through the RSA algorithm by taking two large distinct prime numbers, public and private keys are represented by e and d, respectively, which are also a prime number. In the next step, and at the level of one, the information in the form of text is transmitted from sender to receiver through the cloud and then converted into ciphertext by the use of a public key (e) of RSA, AES is used for conversion of ciphertext. In the hybrid encryption method, another level two is used by the One Time Password technique in which DNA Genetic algorithm is used for getting ciphertext (second level) by OTP method. For the authentication purpose, further two levels are used for decryption of the ciphertext into the plain text and at level one, DNA genetic algorithms are used for getting AES cipher by OTP technique and further private key of RSA is used for getting the plain text.

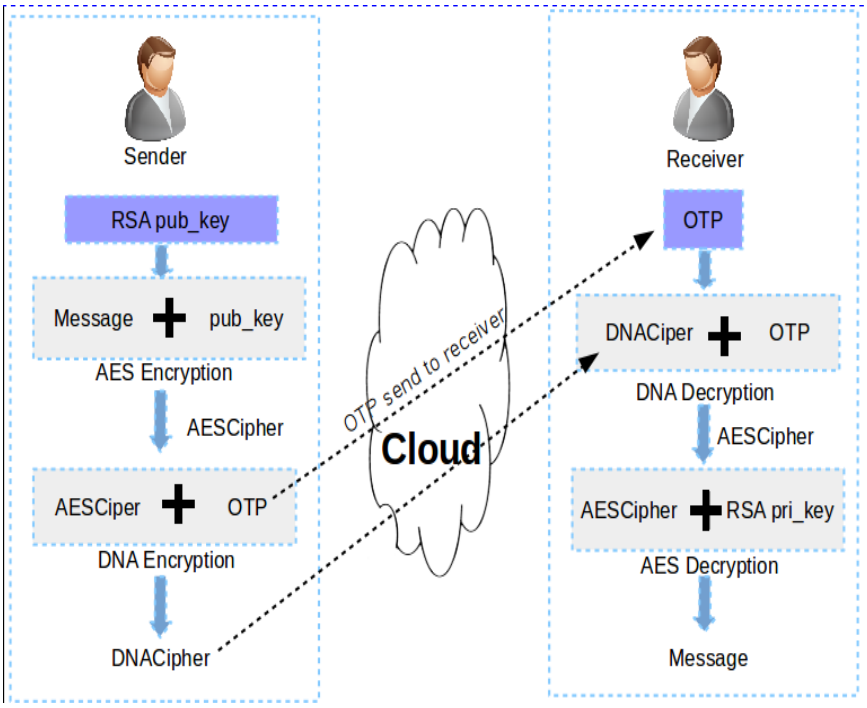

Figure 4: Proposed Hybrid model

5. Experimental Evaluation

The primary purpose of the proposed hybrid algorithm is to enhance data security in cloud computing. The proposed algorithm works on combining different cryptographic algorithms such as RSA, AES and DNA-Genetic using One Time Password to perform better security features for the user. The results are computed in Python 2.7.17. Let's take an example, input a text message like “Welcome To BBAU” and at the key generation RSA algorithm generates public and private key and the next first level encryption AES algorithm encrypts a message using RSA public key and at the second level encryption, the output of AES ciphertext is encrypted using a DNA-Genetic algorithm with One-time password that is randomly generated, after the final DNA sequence the OTP sent to the receiver directly using different medium and the receiver performs decryption in reverse order. It takes total computation time (milliseconds) “279.0”. as per the comparison from the previous simple encryption algorithms. The proposed algorithm provides better performance and fast execution time with high authentication, integrity and confidentiality. This is shown below table 2 and in following figure 5.

ISN: 2233-7857 IJFGCN

Figure 5. Hybrid Algorithm Result

ISN: 2233-7857 IJFGCN

Table 2: Level wise Encryption of Proposed Algorithm

Message	**First Level Encryption**	**Second Level Encryption**	**Decryption**	**Total computation time (milli second)**
Welcome To BBAU	pKiW8cC4jm0xZUixRN17CqKxcXGm22KGwEmeKLry66SdBNhD35KEqmk9JBFEgqdy7D6dnFjGoNqVfd3dDoYBMrAhQnEZHsWQCl5Nmz+cnlNwHErGwUTINbTfVblCh+hVCV7cWpNgMjWaZ4R4rJ4nvwB02i2Bgm4Q6rVYjMNp1iWbO8wJbBMOYeIE31x4ugbLXOy2Z8c8MGqGjVsXQAbeU4ZTvghk/ivQXlcA+xAQMzDxkDN/vjptBH9kQGEk/yQ7YP9j9LdVtLhMZ3VuCMBG3e2mhA9uw2FhfnEUpTGPBon/HWCdkx+2o0xNQqOZ9FXFECX/dT2ls89QVM/jb/4Ug==	AAACATCCCTCACCGGAGTGACAGGATACG AGGAGGGAAAACTAATTTTGTTGCGCCGCG CAGGATCGAGATAATCACCTCCTGAGACGC ATTGATGTAGTGCGACATCTCCACTGCTTGC AAGAACGCCGCCATCGCTCTGCGGGAAACT CAAAAAGAACAACTTCTAACGGGATATGTT CGGCCTGCATTTTTTGGCTTTACGGCGCTTA GTGTGTTTTTGGTGCGCTCTAGTGGCCACTA ATTATAGAGGCAGCATTACGTTTGAGGTTC GTTTCAAGGTAGGGAGAAACGGAAAAAGG GATTACCCGTATAATCATCGCACAGACGTT GTTAACTCGTACCTGAGGTCGGGATTGAAA GCACCTACTCAATTCGTCTGTATCGCAAAA GGAGCGCCTGTATTGTACCTCAAAAAGACA AGCGTACCCGCTTTTGGTCTACTACCAGGA CGTTTCAATCTATTAAGCCGGGACCGGCCC TGAGGGTCTAATGACGGAAACAATTGCGCA ATGGTATGATACCCCCGATGCTGAATCCCT CCCCGGGCGCCCAGACGCCTCGGTTAAGTA ATCAGCCTAGGCGTGAGTTTCGACCTTGGC ATTCTGTGTGAGCCTCAACCCAGCGTCCGG GCGCCCCATATGGCGCGAATATCCTAATTC TCATTACACCGGCGCGTGCACGTGGACGGG CGCCTGATTGCCGGATGGTGCCGAATGCTG ATTTTCTTACTCTTGCTGTCTCATGAAGGAT GAACGGATGCGGGATCCATGTACGAGGGTA GCAGATTAATAGAGGTAAGCGCAATGTCGA TCGACATCCGGAACATGTGTTAGTAACTCG CGTAAGGAATAGAAATGAGTGTCACACAGC AAGCTGCAACGTTTCATGAAAGCTTTCATA TCTTAGATAGGAGAACACGATAACCGCGAC GCATTAGCACTAAGAGACTTTACGTTGAAG ATTCCAACATAACGGAGACCTACTTATGTA CTTACGTTGGTTATTATATCACCGTAAACAC GTAAACAACAGGCCTATCTCTCAGGGGTTT ATAAGGTGAGCTCCCCTTCGGTCACCTTCA GGTCTCTTTTTGCAGTTTACACCAGGAGATA TCAGGCACCGTAGTGCAAACTACGCGTGAG CTAAATACTGGTAAGGGTATACTCTACTTG GATTAAGGGGGCCCGGCGCTGAACTTGGAC TGGCATCCCATTTCTTCTTGATGATGGTCGC AAGAGAAGACCGACCCCACTGCAGTGTCGC ACCATAATGAGGCGGTTCCACTTTTCTGCTG ACTTAAATTCTCGGGTACTTCCCATAGCGTC CAGGCCCACGATCAACCTTTAGTGGGTCTA CTGTAGTTGAGTGCGAAC	Welcome To BBAU	279.0

ISN: 2233-7857 IJFGCN

6. Conclusions & Future Scope

Customer requires to be set up to manage security issues in Cloud Computing. Subsequently, clients have given a hybrid encryption plan that can be used to guarantee customer's data in the cloud. Hybrid encryption allows only the affirm customers to get to it Combination of cryptography and symmetric cryptography is known as the hybrid technique. The hybrid technique provides higher steps of security and the efficiency stage is better than either of the technique used separately. The best technique to secure data, certificates and digital signature are needed. In this paper, It is observed that the hybrid approach of encryption and decryption of information from the sender to receiver through the cloud service is more reliable in comparison to the normal symmetric or asymmetric encryption and decryption of information. The information may be in the form of text or data and can be implemented for a large amount of data. The encrypted time in the object-oriented Python Programming language is only 279.0 milliseconds. The proposed approach can be implemented to transfer information related to banking services or any financial organization. In the future perspective of the research article, we will try to minimize the execution time to using GPU scheduling approach for encryption as well as decryption process.

References

[1] Kuswaha, S., Waghmare, S. and Choudhary, P.,Data Transmission using AES-RSA Based Hybrid Security Algorithms. *International Journal on Recent and Innovation Trends in Computing and Communication*, 2015,vol. 3, no. 4, pp.1964-1969.
[2] Mousa, H.,DNA-Genetic Encryption Technique, *I. J. Computer Network and Information Security* 2016, vol. 8, no.7 pp.1-9.
[3] Kumar L. and Badal N., A Review On Hybrid Encryption in Encrypted form of Text 2019, *2019 4th Int. Conf. Internet Things Smart Innov. Usages*, pp. 1–6.
[4] Saeed, Z.R., Improved Cloud Storage Security of Using Three Layers Cryptography Algorithms, Int. J. Comput. Sci. Inf. Secur. 2018, vol. 16, no. 10, pp. 34–39.
[5] Agbedemnab P. A., Baagyere E. Y., and Daabo M. I., A Novel Text Encryption and Decryption Scheme using the Genetic Algorithm and Residual Numbers, *Proc. 4th Int. Conf. Internet, Cyber Secur. Inf. Syst. 2019*, vol. 12, pp. 20–31.
[6] AbdElnapi, N. M., Omara, F. A., & Omran, N. F., A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing, *Int. J. Comput. Sci. Inf. Secur*. 2016, vol. 14, no. 4, pp. 175–181.
[7] Wang, Y., Han, Q., Cui, G. and Sun, J.., Hiding Messages based on DNA Sequence and Recombinant DNA Technique, *IEEE Trans. Nanotechnol*. 2019, vol.18, pp.299-307.
[8] Zhang Y., Liu X., and Sun M., DNA based Random Key Generation Management for OTP Encryption, *BioSystems* 2017, pp. 51-63.
[9] Namasudra, S. et al., Time Efficient Secure DNA Based Access Control Model for Cloud Computing Environment, *Futur. Gener. Comput. Syst.* 2017, vol. 73, pp. 90–105.
[10] Kalsi, S., Kaur, H., & Chang, V. , DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation, *Journal of Medical Systems* 2018, vol.42,no-1,pp 17.
[11] Shiu H. J. et al., Data Hiding Methods Based Upon DNA Sequences, *Information Sciences* 2010, vol. 180, no. 11, pp. 2196–2208.
[12] Rivera L. B. et al. Hybrid Cryptosystem Using RSA , DSA , Elgamal , And AES, *Int. J. Sci. Technol. Res.* 2019, vol. 8, no.10, pp 1777-1781,.
[13] Kumar B., Boaddh J., and Mahawar L., A Hybrid Security Approach Based on AES and RSA for Cloud Data, *Int. J. Adv. Technol. Eng. Explor.* 2016, vol. 3, no. 17, pp. 43-49,.
[14] Liu, Jia, et al. Optimization of AES and RSA Algorithm and its Mixed Encryption System. *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Springer, Cham. 2017, pp. 393-403.

ISN: 2233-7857 IJFGCN

[15] Salim E. and Harba I., Secure Data Encryption Through a Combination of AES, RSA and HMAC, *Engineering, Technology & Applied Science Research*. 2017, vol. 7, no. 4, pp. 1781–1785.
[16] Terec, R., Vaida, M. F., Alboaie, L., & Chiorean, L., DNA Security using Symmetric and Asymmetric Cryptography, *Int. J. New Comput. Archit. Their Appl.* 2011, vol. 1, no. 1, pp. 34–51.
[17] Sindhuja, K., & Devi, S. P., A Symmetric Key Encryption Technique Using Genetic Algorithm, *international journal of computer science and information technologies*.2014, vol. 5, no. 1, pp. 414–416.
[18] Dubey, S., et al., Encryption and Decryption of Data by Genetic Algorithm, *International Journal of Scientific Research in Computer Science and Engineering* 2017, vol. 5, no. 3, pp. 42–46.
[19] Stallings, W. Cryptography and Network Security, *published by Pearson india education services.,* 2018
[20] Trappe W. and Washington L.C.,Introduction to Cryptography with Coding Theory*, published by pearson Educatio,India.,* 2014.
[21] C. Hall and N. Ferguson, Chapter 7 The Advanced Encryption Standard (AES), November, pp. 58–73, 2001.
[22] Erdem, E. and Sandıkkaya, M.T., OTPaaS—One time password as a service. *IEEE Transactions on Information Forensics and Security*.2018,Vol.14, no. 3,pp.743-756.
[23] Gerami, M. and Ghiasvand, S., One-time passwords via SMS. *Bulletin de la Societe Royale des Sciences de Liege.* 2016, Vol. 85, pp. 106 – 113.
[24] Kumar N, Kumar S. Virtual Machine Placement Using Statistical Mechanism in Cloud Computing Environment. International Journal of Applied Evolutionary Computation (IJAEC). 2018 Jul 1,Vol. 9, No.3, pp.23-31.

ISN: 2233-7857 IJFGCN