International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/211630 Volume 9, Issue 1, January – February (2022)

RESEARCH ARTICLE

A Novel Algorithm for Secured Data Sharing in Cloud using GWOA-DNA Cryptography

Mercy Joseph
Department of Computer Science, Chikkanna Government Arts College, Tirupur, Tamil Nadu, India
elsinchakkala@gmail.com

Gobi Mohan
Department of Computer Science, Chikkanna Government Arts College, Tirupur, Tamil Nadu, India
mgobimail@yahoo.com

Received: 19 December 2021 / Revised: 30 January 2022 / Accepted: 04 February 2022 / Published: 28 February 2022

Abstract – Cloud is a recent technology that enables wide access and storage on the internet. Moreover, the cloud computing environment allows storing and sharing plenty of digital data including text, image, video, audio, etc. through the internet. Although it is cost-effective and has numerous advantages, cloud technology still faces a lot of challenges like data loss, quality issues, and data security. In this paper, an effective algorithm is introduced using deoxyribonucleic acid (DNA)-based cryptography to enhance data security while sharing the data over the internet. For this process, an optimized encryption model is implemented using Grey Wolf Optimization (GWO) Algorithm to generate optimal encrypted data while sharing. Various datasets have been implemented to verify the efficiency of the proposed GWO Assisted-DNA (GWOA-DNA) cryptography in terms of accuracy and execution time.

Index Terms – Data Security, DNA-Based Cryptography, User Access, Cloud Computing, Key Generation, Encryption, User Verification, User Access.

1. INTRODUCTION

In recent days, the number of users using the internet grows enormously. For this reason, a wide access and storage system is required to face the needs of the users [1]. Cloud technology enables the users to store and share over the internet more effectively. Cloud system allows users to access and share digital data among various users globally [2]. In addition to this, cloud technology permits the users to import and export data over the web object storage which may contain sensitive data such as personnel profiles [3], business data, and so on. Moreover, data sharing enables the selected things or objects in a database also data sharing is the capability for sharing the same data source my multiple users or application [4]. The data become stored in single or more servers in the network but contain few hacking mechanisms which avoid the same kinds of data from the two people [5]. The data-sharing system is detailed in Figure 1. The data sharing of the cloud contains three main objects that are mainly involving data owner who shares original data with another person [6].

The Cloud Service Provider (CSP) can offer computational facilities and storage related to data. To enhance the security of data sharing in the cloud, the data owner needs to send or share the data into encrypted at the next store the encrypted data in the cloud [7]. While the data owner sends the encrypted key means sharing the data or information to the user. With the help of the encrypted key share the decrypted data through the owner [8]. Consequently, sharing this way of data is more confidential because of the third and communicating parties. Though the cloud provides several services and huge storage facilities, the security of the data shared over the internet is still vulnerable to several attacks such as brute force attacks, occlusion attacks, etc. [9]. Moreover, hacking is also another threat that leads to data loss or data corruption may while data transferring and storing [10].

To overcome the issues in cloud computing, numerous researches have been implemented to enhance secure data sharing via key generation processes [11]. However, it suffers authentication and trust issues between the sender and receiver of the data [12]. Occasionally, the key cryptosystem is time-consuming and might cause computational errors [13]. Later, DNA-based encryption is introduced for secured data sharing over the cloud [14]. Nevertheless, the issues in efficacy continue in terms of computational complexity and high execution time. To overcome the issues, researchers developed various optimization algorithms, to optimize the DNA coding while generation and transmission [15]. Generally, DNA codes are developed with unique structures which can solve several issues simultaneously [16].

This paper introduces a novel GWOA-DNA cryptosystem that is proposed to generate optimal keys for both encryption and decryption processes. The proposed model includes

RESEARCH ARTICLE

optimal key generation, DNA encryption, and decryption process.

The main contribution of the paper is given below.

- Generally, cloud system lacks security for data sharing over the internet. To enhance the security with effective computational capacity, a novel algorithm is proposed named GWO cryptosystem.
- Initially, an optimal key is generated to reduce the computational time and enhance security.
- Moreover, the accuracy of data shared among the data must be ensured to assure reliability.
- A real DNA sequence dataset has been implemented and compared with various encryption algorithms.

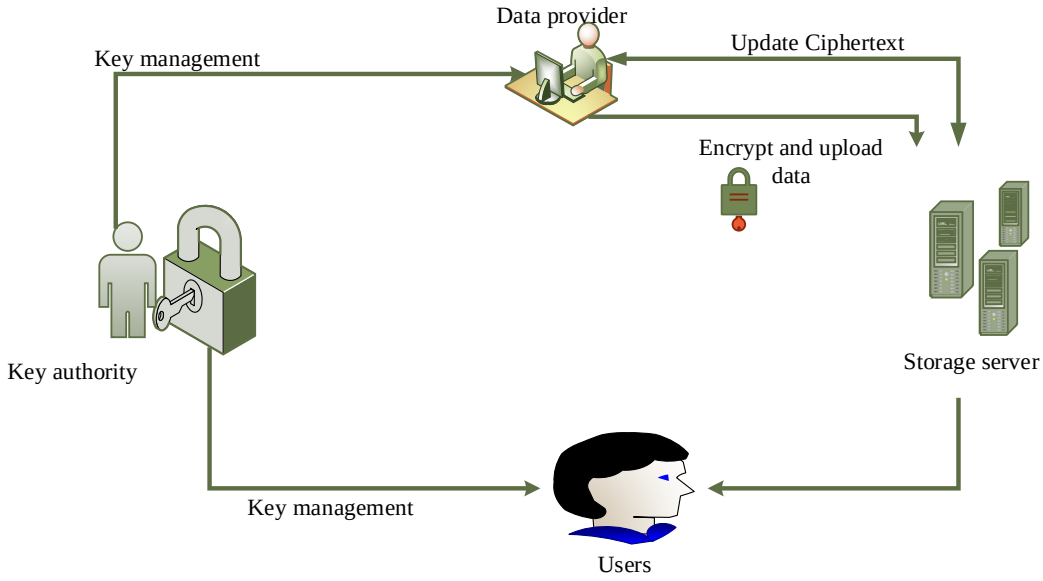

Figure1 Data Sharing System

The arrangement of this article is structured as follows: The related work based on DNA encryption and decryption is detailed in section 2 and the basic problem statement is elaborated in section 3. Also, the process of the proposed methodology is described in section 4. Finally, the achieved outcomes are mentioned in section 5 and the conclusion about the developed model is detained in section 6.

2. LITERATURE REVIEW

In 2020, Majumdar *et al.* [17] have developed a system that used a DNA–based encryption along with a fuzzy-based Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) and Multi-Criteria Decision-making (MCDM) methods. In this method, the shared data can decide the storage servers based on the fuzzy inference system. The experimental results deliberate the efficiency of the proposed model in terms of accuracy, sensitivity, and execution time.

In 2019, Elhadad [18] have proposed a model that used a framework named DNA-proxy re-encryption. In this method, initially, 3 keys were introduced for owner, proxy, and end-user. At first, the owner encrypts his data using the first key, and then the proxy re-encrypts the data using the second key, and finally, the end-user decrypts the data using the third key. The experimental outcomes proved their efficiency via execution time.

In 2017, Thangavel and Varalakshmi [19] have implemented a system that used DNA-based encryption and an enhanced ElGamal cryptosystem including three parts namely key management, data owner, and data user. This method was proposed for enhancing data security using both symmetric and asymmetric cryptosystems. The investigational results demonstrated the efficacy through security and enhanced performance.

In 2019, Nithya Chidambaram *et al.* [20] have developed a method that was used to ensure the security of the images shared over the cloud using a three-layer image cryptosystem via DNA algorithm with confusion and diffusion methods. The efficiency of the proposed method was proved through Amazon S3 web services in terms of suitability and strength over various attacks and computational and complexity evaluation.

In 2021, G. K. Sandhia and S. V. K. Raja [21] have implemented a system that used Multi-Authority Cipher-text Policy Attribute-Based Encryption with Elliptic Curve Cryptography (MA-CPABE-ECC). In this model, the keys were generated based on the requirements of the user, and the

RESEARCH ARTICLE

keys were pointed as elliptical curves so that the proposed model achieved enhanced security. The efficacy of the proposed model was measured in terms of performance and security evaluation.

In 2020, Muhammad Tahir, *et al.* [22] have proposed a system that used a Genetic Algorithm (GA) named CryptoGA to ensure a secured data sharing and reliability model among users. Here, GA was implemented to generate keys to enhance the encryption and decryption process and ten various datasets have been implemented to verify the efficiency via key size, computational time, and the avalanche effect. The summary of the literature review is presented in Table 1.

Authors	Methods	Features	Challenges	Achievements
Majumdar *et al.* [17]	The TOPSIS and MCDM Methods	● Achieved considerable security over attacks ● Minimized computational time	● The performance is limited since the sensitivity was minimized after applied the avalanche effect	Accuracy sensitivity, and execution time.
Elhadad [18]	The DNA-proxy re-encryption Method	● Guaranteed better performance via better computational performance	● However, the accuracy of the shared data was meagre	Minimized execution time
Thangavel and Varalakshmi [19]	The DNA-based and ElGamal cryptosystems Methods	● Accomplished effective execution time	● For larger datasets, it was bounded by computational complexity	Enhanced security and performance
Nithya Chidambaram *et al.* [20]	The three-layer-based DNA cryptosystem Method	● Attained suitability over web storage services ● Remarkable computational efficiency	● While sharing larger data, it failed to provide robustness	Suitability and strength over various attacks and requires low computational time
G. K. Sandhia and S. V. K. Raja [21]	The MA-CPABE-ECC Method	● Attained improved security ● Enhanced accuracy	● Revealed highly complicated expressions and computation	Robust to several vulnerabilities and enhanced security
Muhammad Tahir, *et al.* [22]	The CryptoGA Method	● Ensured better security ● Exposed minimized computational overhead	● Easily susceptible to attacks	Minimized key size, and computational time.

Table 1 Summary of Literature Review

3. PROBLEM STATEMENT

The TOPSIS and MCDM [17] models achieved enhanced security and computational time, yet it lacks due to the minimal sensitivity after applying the avalanche effect. The DNA-proxy re-encryption [18] method ensured better performance via better computational performance, but it needs to prove the accuracy of the shared data. The DNA-based and ElGamal cryptosystems [19] method attained effective execution time. However, for larger datasets, it suffers computational complexity. The three-layer-based DNA cryptosystem [20] obtained suitability over web storage services and computational efficiency. However, it lacks robustness over larger datasets. Though MA-CPABE-ECC [21] model attained improved security, it was limited by the computational complexity. The CryptoGA [22] method ensured better security and reliability, yet the performance was limited by the vulnerability over attacks. For this reason, the limitations in the conventional models tend to introduce a novel effective methodology for secure data sharing in cloud systems with improved performance.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/211630 Volume 9, Issue 1, January – February (2022)

RESEARCH ARTICLE

4. PROPOSED METHODOLOGY

The proposed secured data sharing model over the cloud is presented in Figure 2. This model consists of three major processes including secret DNA sequence S selection, message to be encrypted$M$, and a transformed sequenceS'. Initially, a secret S is chosen from the openly available DNA sequence. This secret S is only knowledgeable to the sender and receiver of the sensitive data$M$. Besides, the secret $S$is embedded into the data M which becomesS'. Now, the sender A_1 sends the transformed sequence S' to the receiver B_1 with a group of several DNA codes. The receiver B_1 receives all the DNA codes together with S' and analyses all the codes. Once, B_1 recognizes the exact S', it decrypts the S' and attain M. Moreover, the DNA cryptosystem is developed with three major phases such as key generation, encryption on owner data and decryption on user data similar to conventional systems. Nevertheless, the key generated for encryption and decryption are optimized using GWO algorithm. Here, the data owner uploads the data through the proposed data-sharing framework. In addition to that, the uploaded data are encrypted using the proposed GWOA-DNA cryptosystem in a secured manner through an optimal key. Furthermore, the message transformed in to S' is encrypted using the optimal key generated by the proposed GWOA-DNA cryptosystem. The optimal key generated via the GWO algorithm efficiently encrypts the data at the security level. When the end-user requests the data for retrieval, the framework authenticates the user by verifying the S' from the owner level. Then, the data-sharing framework retrieves the respective data in the cloud and allows the user to decrypt the secret DNA code S' using his optimal key. From this decrypted data, the user can access the original data M. The major three phases are given below.

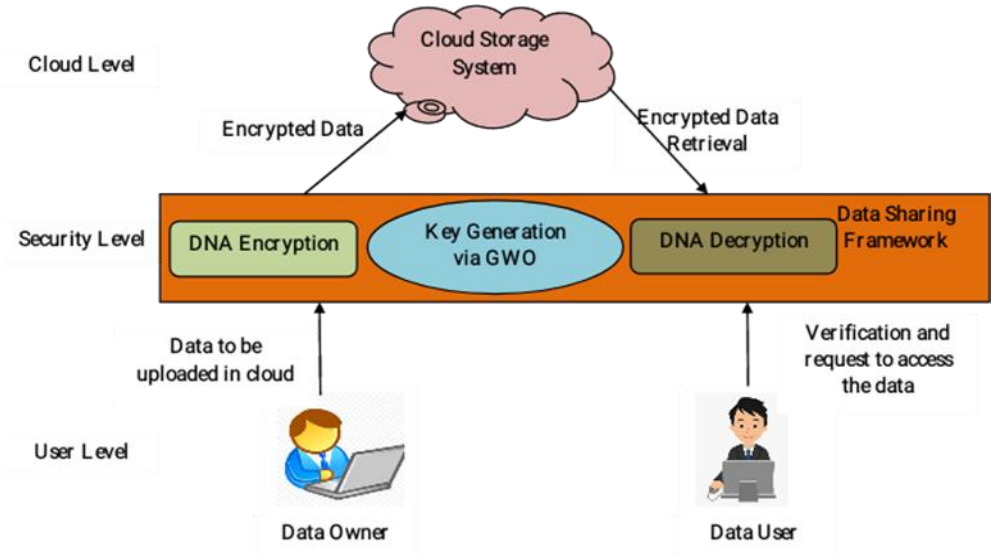

Figure 2 Proposed GWOA-DNA Cryptosystem

- User level: Initially, this level includes a data owner and a user. Later, the number of data users can be extended based on the requirement of the data from the owner. All the end-users are verified with the security keys generated by the GWO model.
- Security level: Here, the data sharing process takes place that includes data uploading, data encryption, data downloading, data decryption, and security authentication using an optimized key.
- Cloud level: At this level, the cloud system provides storage and access to the users which attain the major concern, since data uploading and downloading takes place here. The data uploaded to the cloud is encrypted and the downloading data is decrypted at this level. Moreover, all these processes are implemented in a secured manner using the optimized security keys.

4.1. Design of Proposed GWOA-DNA Cryptosystem

4.1.1. GWO Algorithm

The proposed secured data sharing model over the cloud is implemented using GWO [23] model for generating an optimized key. The mathematical model of GWO is presented here. Generally, it includes four types of wolves namely the most powerful one as alpha (fitness solution) α_1, second as beta β_1, third as delta δ_1 and the rests are omega ω_1. The encircling prey process of grey wolves is given in Eq. (1) and (2).

$$D = \left| C \cdot X_I(\mathrm{T}) - X(\mathrm{T}) \right| \quad (1)$$

$$X(\mathrm{T}+1) = X_I(\mathrm{T}) - A \cdot D \quad (2)$$

RESEARCH ARTICLE

Here, T denotes present iteration, A and C indicates coefficient vectors, X_I presents the location of prey vector, and X denotes location vector of grey wolves. Eq. (3) and (4) show the evaluation of vectors A and C, which, a represents linearly minimized values in the range of 2 to 0 during the iterations and $r1$, and $r2$ states arbitrary numbers from $(0-1)$.

$$\mathrm{A} = 2a \cdot r1 - a \tag{3}$$

$$C = 2 \cdot r2 \tag{4}$$

The solution update process is evaluated as given in Eq. (5), (6) and (7).

$$\begin{aligned} D^{\alpha} &= \left| C1 \cdot X^{\alpha} - X \right|, \\ D^{\beta} &= \left| C2 \cdot X^{\beta} - X \right|, \\ D^{\delta} &= \left| C3 \cdot X^{\delta} - X \right| \end{aligned} \tag{5}$$

$$\begin{aligned} X1 &= X^{\alpha} - \mathrm{A1} \cdot \left(D^{\alpha} \right), \\ X2 &= X^{\beta} - \mathrm{A2} \cdot \left(D^{\beta} \right), \\ X3 &= X^{\delta} - \mathrm{A3} \cdot \left(D^{\delta} \right) \end{aligned} \tag{6}$$

$$K = \frac{X1 + X2 + X3}{3} \tag{7}$$

Here, K indicates the optimal key generated by GWO in Eq. (7). Initially, the owner data enters the security level while uploading the data. At this level, a secret key is generated for this data using the GWO algorithm and performs encryption using the DNA encryption model.

4.1.2. Proposed DNA Encryption Model

The proposed DNA encryption is discussed in this section. Here, a client-side encryption model is implemented, in which the data to be uploaded in the cloud is encrypted by the data owner. Moreover, the cloud service provider cannot access the owner's data in its original form which ensures the security of the original data. Since cloud storage is easily vulnerable to attacks, if any malicious user enters into the cloud cannot access the original file as the file is already in an encrypted format. The proposed DNA encryption model is implemented as follows. Initially, an arbitrary number X (solution to GWO) is given as input and the owner data is shuffled based on the value.

Moreover, the plaintext is changed as a sequence of values through the shuffled values and an optimized key value is developed depending on the GWO algorithm. Based on the optimized key value, the plaintext sequence is extracted. For example, if the key's first bit is 1, then the bits in odd locations are taken for encryption. Conversely, if the initial bit is 0, the even location bits are taken for encryption. Here, binary coding involves a transformation of alphabets such as A, C, G and, T into binary codes and contrary wise. Let A be 00, C be 01, G be 10, and T 11 and it can be specified with more digits. Moreover, if a message M ATACG is represented as 0011000110 it can be denoted as the secret DNA sequence S AATCACTGT. This message can be decoded as follows. Initially, the secret DNA sequence S is transformed into binary code as 000011010001111011.

The attained bits are then partitioned as a sequence of bits based on the optimal key-value, in which the substitution method is applied. Furthermore, the locations of every sequence are changed by the bit sequence. Partition the sequence S according to the random number generated by the GWO. An optimized key sequence K is attained which is the original key used to encrypt the data. For instance, if the key sequence K is 3, 2, 2, and 4, then the sequence S is partitioned accordingly. Now, 000, 01, 10, 1000, 111, 10, and 11 codes are partitioned to the key$K$. The digits apart from the key size are ignored. Augment the first two bits of original code at the beginning of the partitioned bits as given as follows: 00000, 1101, 0010, 011000, 10111, 10, and 11.

The digits without secret sequence are ignored Herein, partitioned codes are concatenated as follows 000001101001001100010111. The DNA sequence S is faked and is transformed into S' as AACGGCATACCT. Further, the bit sequence is partitioned into 2 parts, where the left part is implemented as the initial part whereas the right part is the next half. Later, the two parts are exchanged and the final optimized sequence is changed as cipher-text characters. At this point, the DNA sequence S and faked sequence S' are completely different. This faked sequence S' is now sending to the receiver. The proposed GWOA-DNA encryption model is given in Algorithm 1.

Input: Plain text

Output: Cipher text

Start

{

Read the plain-text

Update input dataset, X // X- arbitrary number which is given as input

Initialize X, a, A and C // X -grey wolf solution

While (R! =0) do

{

Shuffle the owner data to Eq. (7).

Decrease X

RESEARCH ARTICLE

}

end while

Generation of sequence of values // plain-text (ATACG)

Update optimal secret key, K // K- input of optimal secret key

if(bit=1001101)

{

Generate optimal key, K

}

End if

Apply substitution operation

Between K and S // K- key

// S- sequence of value

Partition $a_b \rightarrow S$ // a_b - attained bits

Get location

if(a_b = 1)

{

Encrypt odd location bits

}

Else if ($a_{b=0}$)

{

Encrypt even location bits

}

End if

Divide $a_b \rightarrow$ 2 equal parts

Arrange

$left\_part \rightarrow 1^{st} half$ and $right\_part \rightarrow 2^{nd} half$

Exchange two partitions

Partition a_b into optimal sequence

Output

Attained Cipher-text

End

Algorithm 1 Proposed GWOA-DNA Encryption Model

4.1.3. Proposed DNA Decryption Model

In this subsection, the proposed DNA decryption is presented which takes place on the user side at the security level. Initially, the user is needed to verify the identity of the storage to attain access rights. Then, he enters his data file to be accessed on the cloud. The cloud provides the encrypted data which is then subjected to decryption. In this process, the user acquires the decryption key and the X value to access the data. In contrast to the encryption process, the decryption model reverses the encrypted data to its original form. Initially, the cipher-text is accessed and later the optimal secret key is accessed which is then changed to optimal private key K based on the first bit of K. to X value, the data is shuffled and the cipher-text is changed as a bit sequence. Here, the cipher-text is partitioned as two parts, conversely, the right part is performed as the first shift, and the left part is performed as the second shift. Exchange the two parts and the attained bit sequence is grouped as the sequence of blocks. Apply substitution operation between the optimal key K and the attained bit sequence. The fake sequence S' AACGGCATACCT is transformed to the binary bits as 000001101001001100010111. As the receiver already knows the secret key K, the bits are now partitioned according to the key K(3, 2, 2, and 4). The partitioned bits are 00000, 1101, 0010, 011000, and 10111. Remove the key and extract the first two bits from each partition as 0011000110. Transform the binary codes to the alphabets as ATACG which is the original text send by the sender. Finally, the bit sequence is changed as plain text in the original form. The proposed decryption model is presented in Algorithm 2.

Input: cipher text

Output: plain text

Start

{

Access the cipher data and secret key

Get K // K- optimal key

// based on the initial bit

While (R! =0) do

{

Shuffle the cipher data to the X value

Decrease X

}

end while

Generation of sequence of bits // cipher data

Divider $a_b \rightarrow$ 2 equal parts

RESEARCH ARTICLE

Arrange $right\_part \rightarrow 1^{st} half$ and

$left\_part \rightarrow 2^{nd} half$

Exchange two partitions

Partition $a_b \rightarrow S$ // a_b - attained bits, S-sequence

Eliminate extra bit

Get location

if (a_b=1)

{

Decrypt odd location bits

}

Else if (a_b=0)

{

Decrypt even location bits

}

End if

Substitute K and S // K-optimal key

//S-sequence

Output

Attained Plain-text(ATACG)

End

Algorithm 2 Proposed GWOA-DNA Decryption Model

The threshold values are used for securing the cloud during data sharing, whether the threshold value is greater than the obtained optimal solution means normal user but the threshold value is lower than the optimal key results means attacks or unauthorized person. Based on the threshold value identifies the data user and attacks also enhance the securing in the cloud during data sharing. The optimal key values are denoted as the threshold of the developed framework which encrypts the pain text into some secret key using an optimized key solution.

5. SIMULATION RESULT

5.1. Simulation Setup

The proposed method was performed in MATLAB 2018a. The efficiency of the proposed method was observed via the simulation outcomes. The plain text for data transmission was arbitrarily chosen with different data sizes between 5kb to 30kb. Moreover, for each input plain-text, the size of cipher-text created was evaluated to compute the total execution time. The efficiency of the proposed model was measured in terms of accuracy, execution time, throughput, and various conventional symmetric key methods namely Re-Encryption based DNA (RE-DNA) [18], DNA and Cryptosystem (DNAC) [19], Cloud Compatible DNA (CCDNA) [20], Cryptosystem based Genetic framework (CG) [22], Advanced Encryption Standard (AES) [23], Blowfish [24], Data Encryption Standard (DES) [25], and DNA [26], models. Moreover, attained outcomes of developed technique stimulated parameters are detailed in table2.

Sl.no	Parameters
1	Accuracy
2	Execution Time
3	Encryption Time
4	Decryption Time
5	Throughput

Table 2 Stimulated Parameters

5.2. Algorithm Analysis

The efficiency of the proposed model can be evaluated in terms of throughput, execution time, and the efficiency over conventional encryption algorithms. Here, the computational time and throughput of the plain-text to be encrypted for the data in the size of 5, 10, 15, 20, 25, and 30 kb respectively. Moreover, efficiency of the proposed GWOA-DNA Cryptosystem is analyzed over traditional symmetric algorithms in terms of accuracy, execution time, encryption time, decryption time, throughput, and so on.

5.2.1. Accuracy

Accuracy is used to check the reliability of the developed framework which is the set of measurement that is closeness measurement of the exact values. Moreover, it is the state or quality of being precise or correct. The degree of the gained specification conforms to the standard value is called accuracy. The measurement of accuracy is obtained using Eq. (8)

$$Accuracy = \frac{C_p}{T_p} \quad (8)$$

Where, C_p is represented as the number of correct data transmission and T_p is denoted as the total quantity of the data transmission. Also, the gained accuracy of the developed technique is compared with other existing techniques which are shown in Figure 3.

RESEARCH ARTICLE

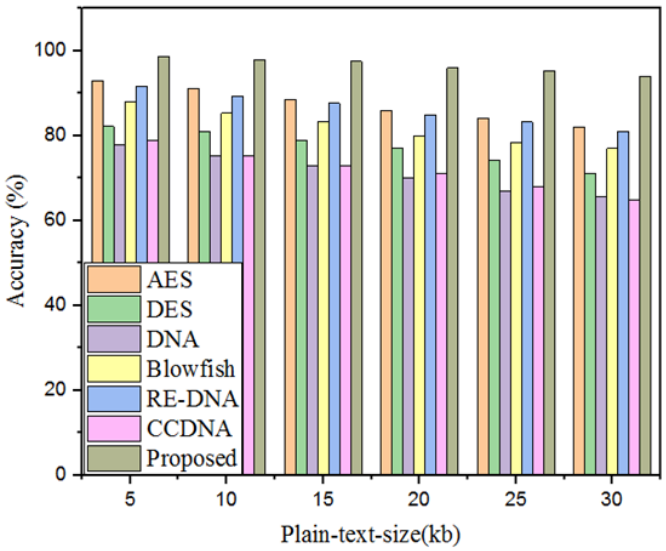

Figure 3 Analysis of Accuracy

The gained accuracy of the developed framework is compared with other existing techniques such as AES, DES, DNA, RE-DNA, CCDNA, and blowfish. Moreover, higher accuracy is 12.8% better than AES, 20.12% improved than DES, 23.65% better than DNA, 12.98% better than Blowfish model, 18.72% better than RE-DNA, 32.34% better than CCDNA model. It shows that the proposed model is more efficient than the other encryption algorithms.

5.2.2. Execution Time

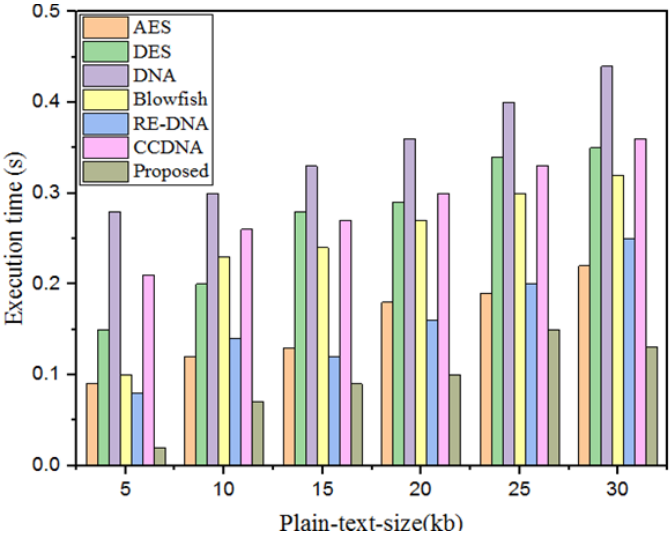

Figure 4 Analysis of Execution Time

Generally, execution time is the ratio of the amount of time essential or required for completing the task also it is calculated based on the overall processing time of data sharing in the cloud to the total time required for encrypting and decrypting the data in cloud computing. The comparison of execution time is shown in Figure 4.

Figure 4 demonstrates the execution time of the proposed GWOA-DNA which is 55.18%, 71.98%, 85.29%, 60.51%, 77.12%, and 54.72% better than AES, DES, DNA, Blowfish, RE-DNA, and CCDNA models respectively. It is proved that the performance of the proposed model is better than the conventional models through the low execution time.

5.2.3. Encryption Time

The encryption time is the required time for converting the data or information into the secret code which become hides the true meaning of the data or information. The time required for converting secretes code is called encryption time. Furthermore, encryption time helps calculate the throughput of any encryption process. The measurement of encryption time is the total plaintext encryption divided by encryption time. The comparison of the encryption time is detailed in Figure 5.

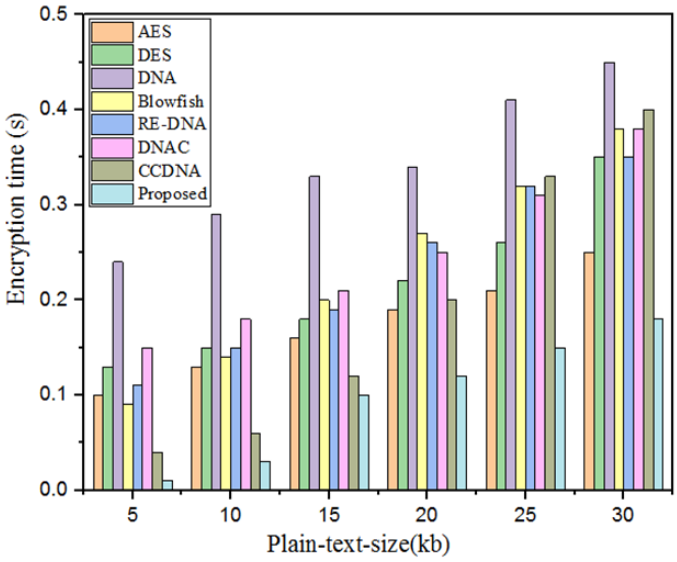

Figure 5 Analysis of Encryption Time

Figure 5 demonstrates the encryption time of proposed GWOA-DNA which is 54.20%, 70.82%, 86.34%, 66.12%, 44.2%, 73.54% and 61.48% better than AES, DES, DNA, RE-DNA, DNAC, CCDNA and Blowfish models respectively. It is proved that the performance of the proposed model is better than the conventional models through the low encryption time.

5.2.4. Decryption Time

The term decryption is the conversion of encrypted data into the original form that is mainly reverse proof of encryption. Moreover, decodes the encrypted data or information hence

RESEARCH ARTICLE

that only authorized the user decrypt the data since decryption need a password or secret key. Additionally, decryption time is the average time for decrypting files or information. The comparison of decryption time is shown in Figure 6.

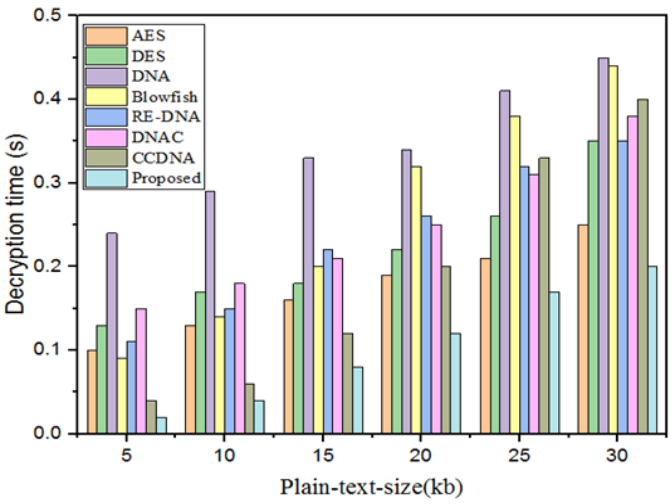

Figure 6 Analysis of Decryption Time

Figure 6 demonstrates the decryption time of proposed GWOA-DNA which is 54.20%, 71.82%, 86.94%, 56.12%, 40.2%, 73.54% and 61.48% better than AES, DES, DNA, RE-DNA, DNAC, CCDNA and Blowfish models respectively. It is proved that the performance of the proposed model is better than the conventional models through the low decryption time.

5.2.5. Encryption Time and Decryption Time of Cipher Text

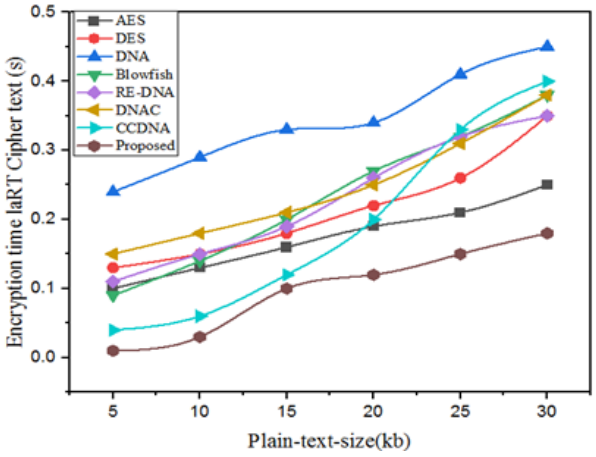

Figure 7 (a) Encryption Time of Cipher Text

Generally, the required time of encrypting plain text into ciphertext through the security key and the cipher key enhances the security of data sharing. It is the time required for converting plain text into ciphertext. The measurement of encryption time is the total ciphertext encryption divided by encryption time. The comparison of the ciphertext encryption time is detailed in Figure 7 (a). The term decryption is the conversion of cipher text encrypted data into the original form that is mainly reverse proof of encryption. Additionally, the decryption time of ciphertext is the average time for decrypting files or information from the secret code. The comparison of ciphertext decryption time is shown in Figure 7 (b).

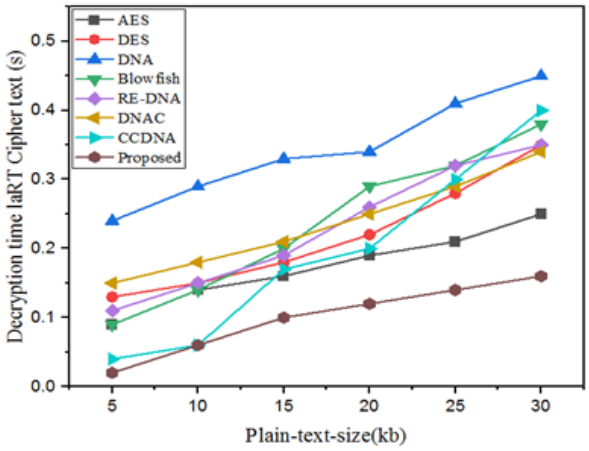

Figure7 (b) Decryption Time of Cipher Text

Figure 7 (a) demonstrates the encryption time of cipher text in proposed GWOA-DNA which is 45.67%, 71.65%, 81.23%, 54.23%, 61.98%, 77.12% and 63.27% better than AES, DES, DNA, RE-DNA, DNAC, CCDNA and Blowfish models respectively. Moreover, Figure 7 (b) demonstrates the decryption time of cipher text in proposed GWOA-DNA which is 40.98%, 67.12%, 78.80%, 81.2%, 73.6%, 81.02% and 61.45% better than AES, DES, DNA, RE-DNA, DNAC, CCDNA and Blowfish models respectively. It is proved that the performance of the proposed model is better than the conventional models through attaining low encryption and decryption time of cipher text.

5.2.6. Throughput

The efficacy of the proposed model is based on the greater throughput. The higher results of the throughput, enhance the performance. The throughput for the encryption model is evaluated based on the size of the plain text and the computation time as given below in Eq. (9).

$$\text{Throughput} = \frac{S(p) - t}{C_t} \quad (9)$$

Where, $S(p)$ is represented as six of plain, t is called as text and C_t is denoted as computation time. The efficiency of the

RESEARCH ARTICLE

proposed model is verified through the throughput over traditional models as given in Figure 8.

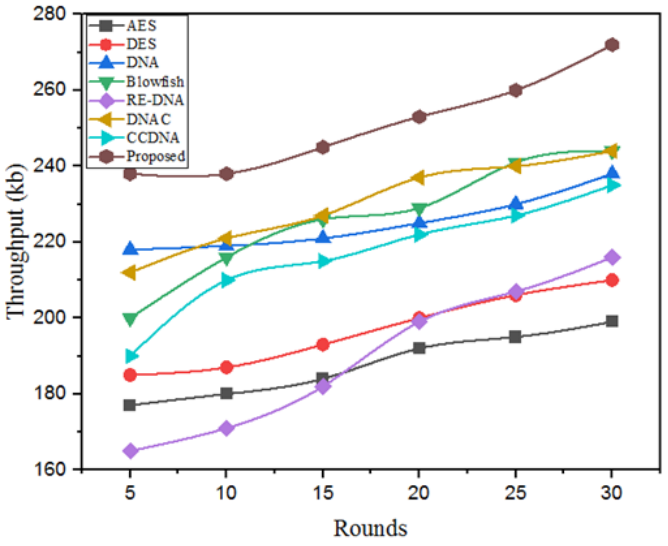

Figure 8 Analysis of Throughput

The proposed GWOA-DNA model attained higher throughput which is 24.8% better than AES, 19.53% improved than DES, 7.57% better than DNA, 13.81% better than Blowfish model, 26.72% better than RE-DNA, 8.12% better than DNAC, and 21.56% better than CCDNA model. It shows that the proposed model attained greater throughput over the other encryption algorithms.

6. CONCLUSION

Generally, cloud computing offers global access to the users via networks where the resources the distributed in an open environment. Although the cloud provides numerous services to the users, the issues in the cloud such as security breaches, data losses, etc. still need to be resolved. Furthermore, authentication problems, unauthorized access, and various attacks over the internet limit the performance and benefits of the cloud system to the users. For this reason, a lot of research has been implemented to resolve the cloud computing issues. In this paper, a novel DNA-based encryption algorithm was implemented to provide a secured data-sharing environment to the users. It includes three major phases such as optimal key generation, DNA encryption, and DNA decryption. The optimal key was generated through the efficient GWO algorithm, and then the data were encrypted at the owner side while uploading to the cloud and decrypted while downloading at the user side. The performance of the proposed model was verified using throughput and execution time and compares over conventional models. The efficiency of the proposed model is verified through the throughput over traditional models as given in Figure.8. The proposed GWOA-DNA model attained higher throughput which is 24.8% better than AES, 19.53% improved than DES, 7.57% better than DNA, 13.81% better than Blowfish model, 26.72% better than RE-DNA, 8.12% better than DNAC, and 21.56% better than CCDNA model. The experimental results show the efficiency of the proposed model and attained better throughput over other models.

REFERENCES

[1] Selvi, S., and M. Gobi. "Hyper Elliptic Curve Based Homomorphic Encryption Scheme for Cloud Data Security." International Conference on Intelligent Data Communication Technologies and Internet of Things. Springer, Cham, 2018.

[2] Gobi, M., and R. Sridevi. "An Approach for Secure Data Storage in Cloud Environment." International Journal of Computer and Communication Engineering 2.2 (2013): 206.

[3] Fu X, Liu B, Xie Y, Li W, Liu Y. (2018) 'Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos', IEEE Photonics Journal. Vol.10 NO.3, pp.1-15

[4] Selvi, S., and M. Gobi. "An Efficient Data Security Model using Hyper Elliptic Curve Cryptography and Steganography

[5] Liu X, Deng R. H, Choo K. -K. R, Yang Y, and Pang H. (2020) 'Privacy-Preserving Outsourced Calculation Toolkit in the Cloud', IEEE Transactions on Dependable and Secure Computing,vol. 17 NO.5, pp.898-911

[6] Wei X, Guo L, and Zhang Q.(2012), 'A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system', J. Syst. Softw. Vol.85 NO.2, pp.290-299

[7] Q. Alam S. U. R. Malik A. Akhunzada K. R. Choo S. Tabbasum and M. Alam,(2017) ' A cross tenant access control (CTAC) model for cloud computing: Formal specification and verification', IEEE Trans. Inf. Forensics Secur, vol.12 NO. 6 pp.1259-1268

[8] Gobi, M., R. Sridevi, and R. Rahini. "A comparative study on the performance and the security of RSA and ECC algorithm." International journal of advanced network and application (2015)

[9] Sridevi, R., and S. Selvi. "Progressing Biometric Security Concern with Blowfish Algorithm.", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8, Issue-9S2, 2019.

[10] Kumar B. M, Sri B. R. S, Katamaraju, G. M. S. A, Rani P, Harinadh N, and Saibabu C. (2020) 'File Encryption and Decryption Using DNA Technology', 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp.382-385

[11] Kumar, G. Kishore, and Dr M. Gobi. "Role of Cryptography & its Related Techniques in Cloud Computing Security." International Journal for Research in Applied Science and Engineering Technology, IJRASET 5 (2017).

[12] Selvi, S., et al. "Hyper elliptic curve cryptography in multi cloud-security using DNA (genetic) techniques." 2017 International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2017

[13] Pushpa B. R. (2017) 'A new technique for data encryption using DNA sequence', 2017 International Conference on Intelligent Computing and Control(I2C2), pp.1-4

[14] Ritu Gupta and Anchal Jain. (2014) 'A New Image Encryption Algorithm based on DNA Approach', International Journal of Computer Applications, Vol. 85 NO. 18

[15] Selvi, S., and R. Sridevi. "Efficient Scheduling Mechanisms for Secured Cloud Data Environment.", International Journal of Recent Technology and Engineering (IJRTE), Volume-8, Issue-2S11, 2019.

[16] Seyedali Mirjalili, Seyed Mohammad Mirjalili and Andrew Lewisa, (2014) 'Grey Wolf Optimizer, Advances in Engineering Software, Vol.69, pp.46-61

[17] Abhishek Majumdar, Arpita Biswas, Atanu Majumder, Sandeep Kumar Sood and Krishna Lal Baishnab, (2020) 'A novel DNA-

RESEARCH ARTICLE

inspired encryption strategy for concealing cloud storage', Frontiers of Computer Science,Vol. 15
[18] Ahmed Elhadad . (2019) ' Data sharing using proxy re-encryption based on DNA computing', Soft Computing,vol.24, pp. 2101–2108
[19] Thangavel,M Varalakshmi,,P. (2017) 'Enhanced DNA and ElGamal cryptosystem for secure data storage and retrieval in cloud', Cluster Computing, vol.21, pp.1411–1437
[20] Nithya Chidambaram, Pethuru Raj Thenmozhi,k Sundararaman Rajagopalan, Rengarajan Amirtharajan,(2019) ' A cloud compatible DNA coded security solution for multimedia file sharing & storage', Multimedia Tools and Applications,vol.78, pp.33837–33863
[21] Sandhia,G.K. Raja, S. V. K. (2021) 'Secure sharing of data in cloud using MA-CPABE with elliptic curve cryptography', Journal of Ambient Intelligence and Humanized Computing
[22] Muhammad Tahir, Muhammad Sardaraz, Zahid Mehmood and Shakoor Muhammad, (2020) CryptoGA: a cryptosystem based on genetic algorithm for cloud data security. Cluster Computing. Vol. 24, pp. 739–752
[23] Rashmi Ramesh Rachh, Ananda Mohan P.V,and Anami B.S. (2012) 'Efficient Implementations for AES Encryption and Decryption. Circuits, Systems, and Signal Processing', Vol.31, pp.1765-1785
[24] Ch. Usha Kumari, T. Pavani, A. Sampath Dakshina Murthy, B. Lakshmi Prasanna, and M. Pala Prasad Reddy, "Generating Cipher Text using BLOWFISH Algorithm for Secured Data Communications", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 9, No. 2, December 2019
[25] Indumathi Saikumar, (2017) 'DES- Data Encryption Standard', International Research Journal of Engineering and Technology,Vol. 4 NO.3,
[26] Khan J.S. (2020) et al., 'DNA and Plaintext Dependent Chaotic Visual Selective Image Encryption', IEEE Access. Vol.8, pp.159732-159744.

Authors

Mercy Joseph – Received MSc Computer Science Degree from Mahatma Gandhi University Kottayam, Kerala and received ME(CSE) from satyabama university Chennai. Currently, she is a research scholar at the Department of Computer Science, Chikkanna Government Arts College Tirupur, India. Her research interests include Cryptography and network security, Data Security in cloud computing and machine learning.

Dr. M.Gobi – Associate Professor in Department of Computer Science in Chikkanna Government Arts College, Tirupur, India. He has published original articles and the finest journals in the area of cryptography and security. His research interests include (but are not limited to) Cryptography, Java, Software Engineering and Information Systems Security.

How to cite this article:

Mercy Joseph, Gobi Mohan, "A Novel Algorithm for Secured Data Sharing in Cloud using GWOA-DNA Cryptography", International Journal of Computer Networks and Applications (IJCNA), 9(1), PP: 114-124, 2022, DOI: 10.22247/ijcna/2022/211630.