[1]S.Lakshmanan
[2]T. Kokilavani
[3]P. Joseph Charles

DNA Secured Edge Computing for Heterogeneous IoT

Journal of Electrical Systems

Abstract: - Edge computing (EC) effectively analyses and stores data near end users and Internet of Things (IoT) devices. IoT is an innovative concept that offers several applications essential to our daily lives. It is crucial to protect data safety because huge amounts of private information are transmitted between these devices. Due to the low computing power of IoT devices, standard cryptography methods are unsuitable. The objective of this paper is to improve a lightweight cipher procdure for heterogeneous smart devices. This paper proposes a three-stage data security (TSDS) algorithm for heterogeneous IoT in edge computing using DNA (Deoxyribonucleic Acid) encoding. DNA encoding is a cryptography technology that uses DNA sequences based on biological functions to encode and decode the original data. The level of security is selected depending on the IoT data confidentiality level. Through tests, the effectiveness of the suggested method is evaluated in terms of encryption and decryption times. The proposed algorithm uses simple, lightweight encoding methods with DNA operations. The suggested technique efficiently hides the data from unauthorized access with the help of DNA. It reduces encryption and decryption time. It is more reliable and lighter, which makes it appropriate for low-power IoT devices.

Keywords: IoT Devices, Edge Computing, Data Security, DNA Encoding.

I. INTRODUCTION

Edge computing technology makes services more stable and offers artificial intelligence services for terminal devices and data that are continually expanding. Edge computing is located near the data source, such as intelligent terminals. Data is handled and stored at the network's edge. It provides users with proximity and location awareness in addition to near-end services [1]. Faster, more secure, and processed data. Furthermore, addressing the issue of high energy consumption in cloud computing, it can reduce costs and alleviate strain on network bandwidth [2]. Manufacturing [3], energy[4], smart homes, healthcare[5], and transportation are some of the areas that can benefit from edge computing .

In an IoT setting, wireless signals link the devices or sensors. Such channels are frequently faulty and disclose users' private information to eavesdroppers [6]. Supervision and protecting the enormous amounts of information generated by diverse smart devices is a challenge in IoT applications. Implementing end-to-end encryption to safeguard insecure communication protects the privacy-sensitive data. Conventional asymmetric key-based cryptography techniques such as curve cipher [7], digital signature [8], and symmetric key encryption techniques [9] are not suitable for use in encrypting and protecting the privacy of data produced by smart devices. These gadgets are referred to be restricted devices since they have a finite amount of processing power and memory. Traditional encryption techniques, which require higher processing power and resource capacity, are unsuitable for smart devices. Therefore, a novel lightweight cipher model is required to guarantee strong data secrecy while having minimal needs efficiently.

To protect healthcare data in smart healthcare infrastructure, Das [10] introduce a novel cipher approach utilizing Serpent, curve based cipher, and Advanced cipher Standard (AES). Many lightweight encryption algorithms [11,12] are suggested for IoT. In these methods, DNA (Deoxyribonucleic Acid) based cryptography [13] is a novel development used in various cryptosystems. Hybrid encryption, which combines homogeneous and asymmetric-based encryption techniques, improves information related to healthcare security. Fadhil [14] suggest the lightweight AES technique to secure data from IoT devices. Cryptography(IECC) to secure the authentication and encryption of data from IoT-based medical sensors. The IECC is a curve-based system with a particular base

[1] *Corresponding author: Research Scholar, Department of Computer Science, St.Joseph's College(A), Affiliated to Bharathidasan university, Tiruchirappalli, lakshmansjc1@outlook.com

[2] Author 2 Affiliation: Assistant Professor, Department of Computer Science, Christ University , Bangalore, India

[3] Author 3 Affiliation: Assistant Professor, Department of Computer Science, St.Joseph's College(A), Affiliated to Bharathidasan university, Tiruchirappalli

point determined by a prime number's functions. This system combines user credentials and biometric criteria, enhancing network security.

Hameed [15] proposed a new security architecture that combines blockchain technology and the AES algorithm. Chen[16] created a new framework for securely storing and distributing encrypted data by integrating proxy re-encryption and blockchain technology. Al-Husainy[17] suggested a lightweight encryption approach with simple replacement and permutation operations to encode the secret data using DNA sequences. Namasudra [18] suggests a unique security system based on DNA cryptography and steganography. DNA-based multiple operations are used to encrypt the sensitive data. Khobzaoui [19] proposed a DNA-based symmetric cryptography approach. Using a symmetric key derived from a chromosome entails breaking the data into chunks of characters for cryptography or deciphering. Kh-Madhloom [20] use layered ASE and DNA for ECG encryption. This method reduces encryption time and well well-suited for IoT health systems.

Alshamrani [21] suggest simple DNA-GA (genetic algorithm) for blockchain encryption. It enhances data security and speeds up the encryption and decryption process. A new combined disordered DNA and AES cipher technology is proposed by Ettiyan [22]. To increase security against IoT assaults, it combines the effective attributes of Unorganised maps in three dimensions with DNA operations in an AES system. A unique DNA-based encryption method is proposed by Majumdar [23], driven by the biological properties of DNA and protein production. Table 1 provides the existing methods and algorithms with its limitations. A novel, lightweight cipher technique built on the DNA system is suggested by Qaid [24]. The DNA key encrypts the information using two straightforward and dependable techniques: substitution and transposition operations that satisfy IoT processing demands. The LZW [25] compression is used to compress the IoT data. LZW is a widely used and extremely effective lossless compression method that is excellent for repeated data types. It is easy to understand and does not rely on previous awareness of the data type. Table 1 shows the existing approaches and its limitations.

Table 1.Different Security Methods Comparison

Ref	Domain	Methods /	Limitations
[10]	IoT Healthcare	Hybrid Encryption Technique (ECC and AES)	Data security is improved; however, the computational burden has not decreased.
[14]	IoT	Lightweight AES	High power consumption
[15]	IoT Architecture	Blockchain with AES	Ineffective with respect to high computational power
[16]	IoT	Proxy re-encryption and blockchain	High network latency and Time consumption verification are needed to
[18]	IoT	Lightweight cryptography with DNA sequence	It lacks security
[19]	Cloud-based IoT	DNA cryptography and steganography	It does not provide data privacy and is vulnerable to
[23]	IoT Patient Monitoring	Hybrid logistic DNA encryption	Security and adversarial mode analyses are missing.

II. DNA CRYPTOGRAPHY

DNA cryptography is a method of data concealment based on DNA sequencing. In the cryptographic method, every character of the alphabet is changed into a unique combination of the four elements (A, C, G, and T) that make up a human's DNA. DNA cryptography is a rapidly evolving field of science based on DNA computing principles[26].

III. THREE STAGES OF DATA SECURITY

This research proposes a three-stage data security (TSDS) algorithm for heterogeneous IoT in edge computing using DNA encoding. DNA encoding is a cryptography technology that uses DNA sequences based on biological functions to encode and decode the original data. The level of security algorithm is selected depending on the data confidentiality of IoT devices. The proposed algorithm uses simple, lightweight encoding

methods with DNA operations. The proposed TSDS algorithm includes (i) simple, lightweight one-time encryption (OTE) with DNA XoR operation for low-level data confidentiality, (ii) for medium data privacy level, the OTE is combined with DNA Addition operation to form a two-stage encryption (TSE), and (iii) the compression algorithm is united with TSE for high-level data security. This paper consider the medical IoT sensors based sensitive data. The collected medical sensitive data is encrypted based on the data security level. Figure 1 shows the proposed work flow.

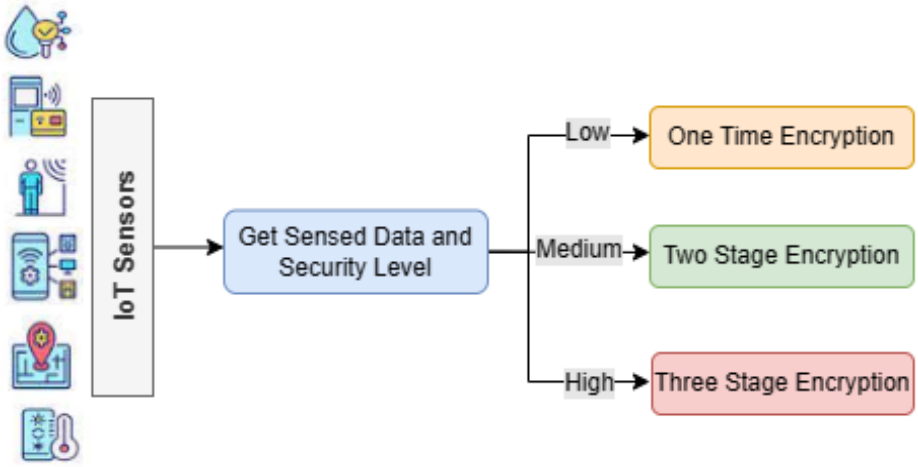

Figure 1. Proposed TSDS Work Flow

A. One Time Encryption

The one-time encryption is applied for low-level data security devices. It converts the data collected from the IoT device into ASCII (American Standard Code for Information Interchange) value. Convert ASCII code into binary value (8-bit) and reverse it. The reversed binary value is divided into four parts (2 bits per part). Each part is converted into DNA code using Table 1. The dynamic secret key is generated based on the sensed data. Generate DNA code for the corresponding secret key. Finally, the DNA XoR operation is used to encode the message".

B. Two Stage Encryption

The two-stage encryption is applied for medium-level data security devices. In stage 1, one time encryption is applied, and in stage 2, the DNA addition operation is used to generate the encrypted text. In this encryption, the first stage generates the encrypted text using a one-time encryption. In the second stage, the encrypted text is divided into several fragments of 4 bits. The DNA addition operation is applied for each fragment to get the second-stage encrypted text. DNA sequences are added to and subtracted from conventional addition and subtraction in the binary system. For example, adding G and C is T (10 + 01 = 11). The subtraction of G and C is C (10 - 01 = 01).

C. Three Stage Encryption

The three-stage encryption is applied for high-level data security devices. In the first stage, the DNA XoR operation encodes the text. The DNA addition operation is used in the second stage, and finally, the data compression technique is used in the third stage to secure the IoT data. The LZW [28] compression is used to compress the IoT data

Algorithm-1 IoT Data Encryption - TSDS
Input: Sensed Data (S), Key key, Data Security Level (SL) Output: Encrypted Data (EC) Step01: dnaKey = Generate DNA Code for key Step02: If SL = ='Low' then // One Time Encryption Step03: C = count (S) Step04: For each character in S Step05: Convert S(i) into ASCII value (AV) Step06: Convert AV into Binary value (BV)

Step07: RB = Reverse(BV)
Step08: Divide RB into four parts
Step09: dnaVal=Convert RB into DNA Code // (use Table 1)
Step10: OTE = OTE+(dnaVal XoR dnaKey) // (use Table 2)
Step11 EndFor
Step12: Else If SL = = 'Medium' then // Two stage Encryption
Step13: OTE = Execute Step03 to Step11
Step14: Divide OTE into a set of fragments with 4 bits (F_1, F_2, F_3, … F_k)
Step15: For each F_i in Fragment
Step16: v1= $F_i(1)$ + dnaKey(1) // DNA Addition Operation
Step17: v2= $F_i(2)$ + dnaKey(2)
Step18: v3= $F_i(3)$ + dnaKey(3)
Step19: v4= $F_i(4)$ + dnaKey(4)
Step20: TSE = TSE + (v1+v2+v3+v4)
Step21: EndFor
Step22: Else // Third stage Encryption
Step23: TSE = Execute Step13 to Step21
Step24: Initialize the dictionary (dict) with the DNA symbol
Step25: Initialize the compressedList to empty
Step26: initW = ''
Step27: For each character (ch) in TSE
Step28: uncomp= initW + ch
Step29: If dict contains uncomp
Step30: initW=uncomp
Step31: Else
Step32: Add compressedList(dict(initW))
Step33: Add dict to uncomp
Step34: initW = ch
Step35: EndIF
Step36: EndFor
Step37: EndIf

IV. RESULTS AND DISCUSSION

The proposed three-stage data security algorithm is evaluated using encryption and decryption time. This algorithm was implemented using Java (Version- Jdk-8). The cipher and decipher time of the suggested approach is compared with the LWC_DNA approach . In cryptography, the process of creating keys is called key generation. Using dynamic key creation, distinct keys are generated for every encryption operation. The dynamic key is stored in gateway server. Tables Table 6 and The times for encryption and decryption of single and multiple words are shown in Table 2and 3. Control restrictions and positive feedback coefficients might result from the intended position of the characteristic eigenvalues. As such, the stability, resilience to parameter changes, and system performance are seriously compromised.

Table 2. cipher and decipher Time for Single word

Approach (Single Word)	Encryption Time (Sec)	Decryption Time (Sec)
LWC_DNA [24]	0.0285	0.035
One Time Encryption	0.002	0.001
Two Stage Encryption	0.010	0.001
Three Stage Encryption	0.016	0.004

Table 3. Encryption and Decryption time for multiple-word

Approach (Multiple Words)	Encryption Time (Sec)	Decryption Time (Sec)
LWC_DNA [24]	0.0320	0.0476
One Time Encryption	0.006	0.001
Two Stage Encryption	0.017	0.001
Three Stage Encryption	0.021	0.007

Figure 2 illustrates the contrast in encryption time between single and multiple words.

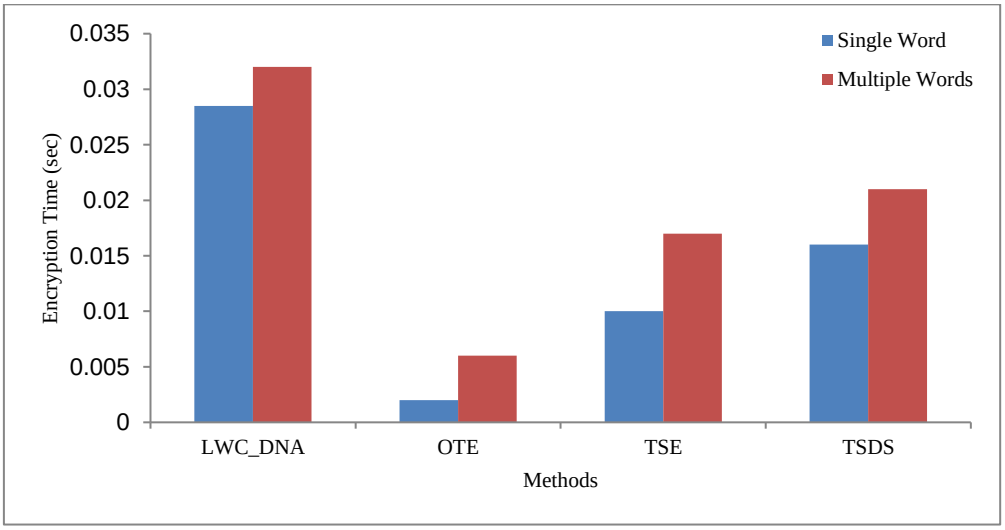

Figure 2. Encryption Time Comparison

Figure 3 depicts the performance comparison of decryption time for single and multiple words.

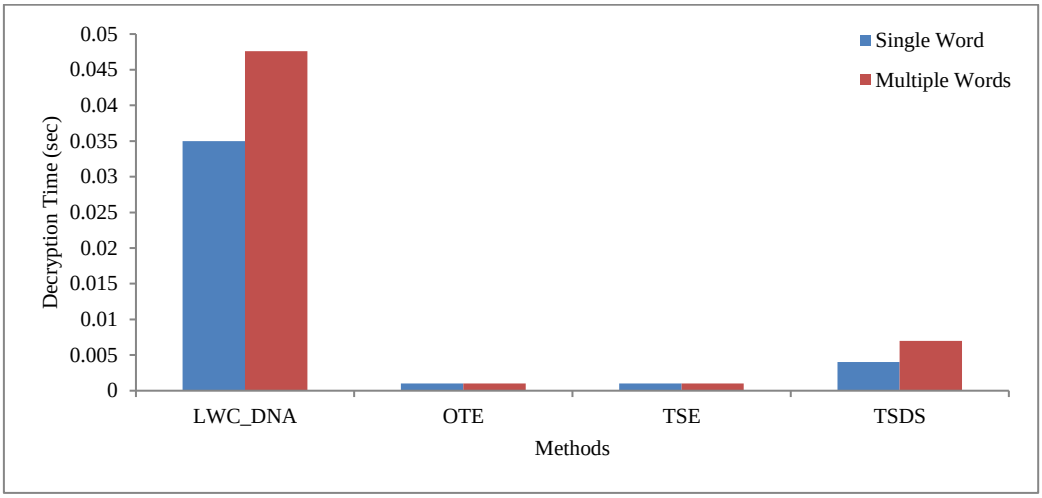

Figure 3. Decryption Time Comparison

A. Security Analysis

This three-step data security approach's high-level evaluation is carried out on security features such as minimizing unauthorized access, data interception, device spoofing, data tampering, and Denial of Service (DoS)

- Unauthorized access: The algorithm's encryption techniques and DNA encoding provide an additional layer of security, making it difficult for unauthorized entities to access and decipher sensitive data

- Data interception: By encrypting the data using DNA encoding, the algorithm ensures that intercepted data remains unreadable and protected from unauthorized access
- Device spoofing: The customizable security levels of the algorithm allow for different encryption techniques based on the security level of smart devices, ensuring it difficult for invaders to impersonate legitimate devices and gain unauthorized access .
- Data tampering: The algorithm's encryption methods and DNA encoding make it difficult for attackers to modify or tamper with the transmitted data without detection, ensuring data integrity.
- Denial of Service (DoS): While the specific mechanisms to mitigate DoS attacks are not mentioned, the algorithm's focus on data security can indirectly contribute to minimizing the impact of DoS attacks by ensuring the availability and integrity of data

With the preceding explanations, table-4 lists the various security risks on which the suggested DNA cryptography approach is focused.

Table-4 Comparison of Various Security Threats with Existing Approaches

Security Threats	Approaches			
	DNA Cryptosystem[19]	Light weight Cryptosystem[17	LWC DNA[24]	TSDS (Proposed)
Unauthorized access	Partially guaranteed	Not guaranteed	Guaranteed	Guaranteed
Data interception	Not Guaranteed	Guaranteed	Partially Guaranteed	Guaranteed
Device spoofing	Not Guaranteed	Not Guaranteed	Not Guaranteed	Guaranteed
Data tampering	Not Guaranteed	Not Supported	Not Guaranteed	Guaranteed
Denial of Service (DoS)	Guaranteed	Not Guaranteed	Partially Guaranteed	Guaranteed

V. CONCLUSION

The IoT network's devices are insignificant, low-energized, and resource-constrained. Battery life, processor speed, and memory size are all considered while assessing resource limitations. There will still be ways to develop original solutions and modify existing security measures. This is because it is necessary to balance the strength of security and the limitations of the smart devices. In this work, a constrained device approach is developed for IoT devices. This research study suggests a three-stage data security utilizing DNA Computing to safeguard data transit for IoT devices. The outcomes of the studies show that the proposed technique achieves a lower processing time than existing approaches while still offering a good level of security. The secret key and encrypted data are hard for attackers to decode.

ACKNOWLEDGMENT

Many thanks for the cooperation of my Ph.D. Research supervisor Prof. Thangavel Kokilavani that spent a valuable part of his time for the paper.

REFERENCES

[1] K.Cao, Y.Liu, G.Meng, Q. Sun,"An Overview on Edge Computing Research", IEEE access, Vol. 8, pp.85714-85728, May 2020.

[2] E. Fazeldehkordi, T.M. Grønli, "A Survey of Security Architectures for Edge Computing-Based IoT", IoT, Vol.3, No.3,pp. 332-365,Feb.2022.

[3] G.Nain, K.K. Pattanaik, G.K.Sharma, "Towards Edge Computing In Intelligent Manufacturing: Past, Present and Future". Journal of Manufacturing Systems,Vol. 62, pp.588-611, Jan.2022.

[4] Q.N. Minh, V.H.Nguyen, V.K. Quy, L.A. Ngoc, . A.Chehri, G.Jeon, "Edge Computing for IoT-Enabled Smart Grid: The Future of Energy. Energies", Vol.15, No.17,pp.1-16, Jul.2022

[5] H.Yar, A.S.Imran, Z.A.Khan, M.Sajjad, Z. Kastrati, “Towards Smart Home Automation Using IoT-enabled Edge-Computing Paradigm”,Sensors, Vol.21, No.14,pp.1-23, Jul.2021.

[6] R.Rajavel, S.K. Ravichandran, K.Harimoorthy, P.Nagappan, K.R. Gobichettipalayam, “IoT-Based Smart Healthcare Video Surveillance System Using Edge Computing”, Journal of Ambient Intelligence and Humanized Computing, Vol.13,pp.1-13, Mar.2021.

[7] A.Sachan, N. Kumar, "S-Edge: Heterogeneity-Aware, Lightweighted, and Edge Computing Integrated Adaptive Traffic Light Control Framework", The Journal of Supercomputing,Vol. 79,No. 13,pp 14923–14953,Sep 2023.

[8] X. Luo, l.Yin1, C.Li, C. Wang, F.Fang, C.Zhu, Z. Tian, “A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IOT Environment,” IEEE Access, vol. 8, pp. 67192–67204,Apr. 2020.

[9] A.D. Durai Sundararajan, R. Rajashree, “A Comprehensive Survey on Lightweight Asymmetric Key Cryptographic Algorithm for Resource Constrained Devices,” ECS Transactions, vol. 107, no. 1, pp. 7457–7468, Apr. 2022.

[10] H.L. Yin, Y.Fu, C.L. Li, C.X. Weng, B.H. Li, J.Gu, Y.S.Lu, S.Huang, Z.B.Chen, Experimental Quantum Secure Network with Digital Signatures And Encryption,” National Science Review, vol. 10, no. 4, Oct. 2022.

[11] W. Cai, H. Yao, “A Secure Transmission Method of Network Communication Data Based on Symmetric Key Encryption Algorithm,” Wireless Personal Communications, vol. 127, no. 1, pp. 341–352, Feb. 2021.

[12] S. Das,S. Namasudra, “A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure,” Computers and Electrical Engineering, vol. 101, p. 107991, Jul. 2022.

[13] S. Li, S. Zhao, G. Min, L. Qi, G. Liu, “Lightweight Privacy-Preserving Scheme Using Homomorphic Encryption in Industrial Internet Of Things,” IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14542–14550, Aug. 2022.

[14] M. Saad, “Designing A Secure Environment For IOT Networks Using Lightweight AES Algorithm,” Iraqi Journal of Science,Vol.16, No.8, pp. 2759–2770, Aug. 2021.

[15] S. S. Hameedi, O. Bayat, “Improving IOT Data Security and Integrity Using Lightweight Blockchain Dynamic Table,” Applied Sciences, vol. 12, no. 18, pp.1-18, Sep. 2022.

[16] Y. Chen, B. Hu, H. Yu, Z. Duan,,J. Huang, “A Threshold Proxy Re-Encryption Scheme for Secure IOT Data Sharing Based on Blockchain,” Electronics, vol. 10, no. 19, pp.1-18, Sep. 2021.

[17] M. A. Al-Husainy, B. Al-Shargabi, S. Aljawarneh, “Lightweight Cryptography System for IOT Devices using DNA,” Computers and Electrical Engineering, vol. 95, pp.1- 108, Oct. 2021.

[18] S. Namasudra, “A Secure Cryptosystem Using DNA Cryptography and DNA Steganography for the Cloud-Based IOT Infrastructure,” Computers and Electrical Engineering, vol. 104, p. 108426, Dec. 2022.

[19] A. Khobzaoui, K. Benyahia, B. Mansouri, S. Boukli-Hacene, “DNA-Based Cryptographic Method for the Internet of Things,” International Journal of Organizational and Collective Intelligence, vol. 12, no. 1, pp. 1–12, May 2022

[20] J. Kh-Madhloom, M. Khanapi Abd Ghani, M. Rizuan Baharon, “ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing,” Intelligent Automation & Soft Computing, vol. 28, no. 2, pp. 493–512, Apr.2021.

[21] [S. S. Alshamrani, A. F. Basha, “IOT Data Security with DNA-Genetic Algorithm Using Blockchain Technology,” International Journal of Computer Applications in Technology, vol. 65, no. 2, pp.1-15, May 2021.

[22] B. Al-Shargabi, M. A. F. Al-Husainy, “A New DNA Based Encryption Algorithm for Internet of Things,” Lecture Notes on Data Engineering and Communications Technologies,Vol.72,No.1, pp. 786–795, May 2021.

[23] A. Majumdar, A. Biswas, A. Majumder, S. K. Sood, K. L. Baishnab, “A novel DNA-inspired Encryption Strategy for Concealing Cloud Storage,” Frontiers of Computer Science, vol. 15, no. 3,pp.1-12, Dec. 2020.

[24] G. R. S. Qaid and N. S. Ebrahim, “A Lightweight Cryptographic Algorithm Based on DNA Computing for IoT Devices,” Security and Communication Networks, vol. 2023, pp. 1–12, May 2023.

[25] A.P.Sridhar, P.V.Lakshmi, "An Efficient Lossless Medical Data Compression Using Lzw Compression for Optimal Cloud Data Storage", Annals of the Romanian Society for Cell Biology, Vol.25,No.6,pp. 17144-17160, May 2021.

[26] [R. I. Abdelfatah, "Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations," in IEEE Access, vol. 8,No.1 pp. 69894-69907, Apr.2020