Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

Enhancing IoT Data Security through Multilayered Approach: Chaotic Map, DNA Sequencing, Blockchain Intergration

[1]Amanbir Singh, [2]Sonal Sood

[1]Research Scholar, Rayat Bahra University, Mohali
[2]Assistant professor, University of Engineering and Technology,
Rayat Bahra University, Mohali

Abstract: The rapid proliferation of the Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity, yet it also poses significant challenges in terms of data security and privacy. In this research, a robust and innovative approach is proposed to address these challenges by introducing a multi-layered security model integrating three powerful technologies: chaotic maps, DNA computing, and block chain technology to fortify IoT data protection. The key objective of proposed technique is to offer security to data at multiple levels while minimizing the Encryption Time (ET) and Decryption Time (DT). In the proposed work, two types of inputs i.e., textual data and medical image data is taken upon which proposed technique is implemented. The key innovation lies in the generation of binary keys from chaotic maps, making it different from traditional chaotic key methods, thereby establishing a unique and robust foundation for encryption. Furthermore, to enhance the encryption process, a dual layer of security is implemented through DNA sequencing and blockchain, ensuring an unprecedented level of data integrity and confidentiality. Notably, the blockchain phase utilizes SHA-256 for generating hash values, fortifying the blocks with an additional layer of cryptographic strength. This novel approach offers a comprehensive and sophisticated solution, effectively mitigating security concerns in IoT ecosystems. By combining the power of chaotic maps, DNA encoding, and blockchain technology, proposed model stands at the forefront of IoT data security, providing a resilient defence against contemporary and future threats.The performance of proposed approach is examined and validated in terms of ET and DT in MATLAB software. Simulating results revealed that proposed model is outperforming other similar models by attaining lowest ET and DT time for both text and image data.

Keywords: IoT, Data Security, Key Generation, Encryption, Blockchain etc.

1. Introduction

The Internet of Things (IoT) is considered as one of the rapidly expanding technologies that is transforming a number of industries, including farming, health care, and transportation. IoT devices may collect and exchange data instantaneously while they are connected to the internet. According to Markets and Markets, the global IoT industry is projected to rise from $235 billion in 2020 to $623 billion in 2025 at a CAGR of 21% [1]. IoT is now necessary due to the growing demand for real-time data and automation in a number of industries. Organizations can track their activities and gather information in real-time thanks to IoT gadgets. IoT sensors in agricultural activities, for instance, might offer data on the soil's moisture level, temperature, and dampness, allowing growers to maximize the yield of their crops. The identical scenario applies to healthcare industry, wherein IoT devices might be used for monitoring the well-being of patients to reduce the need for physical visits and enhance patient outcomes [2]. IoT does, however, present a number of difficulties, with security being the most important. It is difficult to guarantee whether every gadget linked to the internet is secured because there are trillions of them. IoT device vulnerabilities are frequently used by cyber criminals to carry out cyberattacks, jeopardizing the safety and confidentiality of people and organizations. According to Verizon research, IoT devices will be to blame for 17% of data breaches in 2020 [3]. Because of the absence of standardization in this equipment, it is difficult to implement security requirements across different IoT devices [4]. IoT gadgets are complex, and this makes it difficult to secure them. There are numerous entry points to numerous IoT devices, and every single one could have distinct security specifications. Moreover, because IoT devices have limited storage and computer power, it is challenging to deploy complex security mechanisms [5]. Hackers can readily hack IoT devices since they frequently lack essential security mechanisms.

In the last few years, a significant number of researchers have utilized different encryption algorithms for securing the data over IoT, however, its computational complexity is one of the significant issues that demands attention. The majority of the present-day encryption techniques, including RSA and ECC, are computationally complicated, consume a lot of computing power, and have other resource-intensive requirements [6]. More compact encryption methods that can deliver the required security without taxing the capabilities of the device are therefore required. Key management is another problem with existing encryption techniques. Symmetric encryption uses the same key for both encryption and decryption, which indicates that if a single key is made public, any data encrypted with that key will also be impacted. The maintenance of both public and private keys in asymmetric encryption can be difficult, especially when working with a lot of devices. It may become challenging to maintain system safety as a result of key management and distribution concerns [7]. An additional problem with contemporary encryption techniques is side-channel attacks. Attacks like this utilize some of the physical features of the equipment, such as the utilization of power or electromagnetic radiation, to get details on the password or text. Due to the fact that symmetric encryption methods use the same key for decryption as well as encryption, side-channel attacks can be especially effective against them. This renders it simpler for hackers to acquire data regarding the encryption key or text by analyzing the gadget's electrical usage or electromagnetic emissions. The adaptability of encryption techniques presents a last problem. As more IoT devices are introduced to the structure, it becomes more difficult to maintain the safety of the system. Hence, conventional encryption methods may not be appropriate for large-scale IoT deployments because these can be difficult to administer and might not be applicable to a significant number of gadgets [8].Consequently, stronger encryption techniques are required to overcome these issues and offer IoT devices greater security. For IoT devices with limited resources, academics are pushed to create new techniques for encrypting data which are effective and extensible. The forthcoming methods should take key management into account and offer tools for safe key transmission and storage.

1.1 Motivation

The endeavor to safeguard IoT devices is as crucial as keeping IoT equipment accessible for usage, considering the risk of exposing consumer data or gaining access to secret systems. In the field of information security, it is common knowledge that criminals are developing their skills daily and coming up with innovative methods for taking advantage of security flaws. In other instances, it's also getting less expensive to exploit security flaws. Companies are boosting IoT-related operation, which creates greater potential for exploitation as hackers get more adept. Numerous internet-connected gadgets are available today that link and share critical data but only have basic security measures like a single password authentication. however, a single password is currently not enough to authenticate users in the dangerous IoT world of today. To effectively reduce risk and stop breaches, many layers of identity verification spanning a user, device application, and data must be in existence. Keeping this in mind, an effective multi-layer security system is proposed in this paper that can overcome limitations of key management and data encryption.

The rest of the paper is categorized as: Section 2 reviews some of the recent publication for securing IoT systems, along with problem statement. Section 3 gives overview about proposed work along with its methodology. Results are discussed in section 4 and finally paper is concluded in Section 5.

2. Literature Review

In the ever-expanding realm of IoT, where devices communicate seamlessly and data flows relentlessly, ensuring the security of this vast network has become paramount. In this literature section, various techniques usedfor safeguarding data in IoT environments are discussed. Through the lens of cutting-edge techniques such as encryption, cryptography, and blockchain technology, different innovative approaches that researchers and experts are employing to protect sensitive information from cyber threats are reviewed.

Mona MElamir et al. [9]proposed an effective security system in which they used RSA and DNA for improving the security of medical images in IoT system. Their method successfully recreated photos with superior resolution. Results showcased that similarity index of 92% was achieved by suggested model in just 18s, between original and received data.

K Abdelkader, et al. [10], yet again offered a DNA based symmetric cryptography security technique in which texts were encrypted and decrypted in character blocks. Moreover, they utilized a symmetric key that was attained from chromosome for encrypting and decrypting data. The technique was implemented on Raspberry Pi system, upon which good results were obtained for complexity and attack resistance.

Kumar, Anuj in [11], two techniques i.e., DNA and AES were hybridized for ensuring safety of data in IoT platforms. By using the hybrid technique, the experts of this paper encrypted and decrypted data over the network. Results obtained showcased that their technique ideally improved the security in cloud systems.

El-Shafai, Walid, et al. [12], utilized the advantages of H.264/MVC compression technique along with Latin Square Cipher (LSC) with symmetric keys to create a hybrid approach for safeguarding data. They included three techniques i.e., Latin Square Whitening, Latin Square Substitution along with Permutation operations in the encryption method. The suggested approach provides strong defence, credibility, and safety performance for various broadcast video clips, according to simulation findings and analysis performed using MATLAB on various RGB video segments.

Bendaoud, Salma, et al. [13], proposed an improved ECC technique for encrypting images wherein they used DNA computing. They utilized ECC for encrypting the original image and mapping was done by using map table. Following this procedure, they were able to attain a DNA sequencing after encoding every point. An encoded picture using the DNA operations was finally retrieved, thereby providing two layers for security to data. Results showcased that suggested technique can withstand brute force, mathematical, and differential attacks effectively.

Patnala, B.D, et al. [14], utilized codons of DNA for proposing an effective data security mechanism. The replacement process used was based on a lookup database that lists the DNA codons and the associated alphabetic readings. After this, the table was put together arbitrary and was sent to receiver using secured medium. Long-term information storage was at the heart of DNA molecules. According to the study's findings, the method was more effective and dependable over the current systems.

A Musa et al. [15], developed and implemented a symmetric key encrypting method wherein files were encrypted at client end before uploading them to cloud database and then decrypted at receiving end by using the encrypted key. However, they utilized a different algorithm for determining the key value. As a consequence, their approach provides larger files with improved efficiency and safety. By doing so, they provided an additional degree of protection that will prevent unauthorised access to sensitive data and a shortage of standardisation.

S. Kumar, et al. [16], offered an effective multi-level cryptography technique especially for CC systems, wherein they combined symmetric and asymmetric key methodologies. DES and RSA were implemented for increasing the safety to cloud systems on various levels of encryption and decryption at both ends data transmission. For the purpose of minimise security risks, this security paradigm provides openness to both cloud users and cloud service providers. In comparison to the current framework, this approach speeds up text-based file upload and download processes while increasing security for information to the highest possible level.

Kifouche, A et al. [17], presented another lightweight cryptography based secure system for providing safety to data in IoT systems. Their model incorporated three modules, one was chaos-based generator, second was confusion and third was diffusion blocks. Results revealed that proposed model when implemented on Mbed Microcontroller NXP LPC1768 utilized low storage and energy and improved encrypting and decrypting speed respectively.

After reviewing the literatures, it is observed that a number oftechniques have been proposed by various researchers for securing data in IoT systems. These techniques were providing good results but we observed that there is still as cope of improvement. One of the major limitations of current system is that their key generation process is quite complex which affects the performance of these models. Also, it has been observed that majority of these techniques were either using symmetric or asymmetric encryption, however, an effective and strong encryption demand utilization of both symmetric and asymmetric techniques. Moreover, current encryption techniques take longer for encrypting or decrypting data, making them time consuming and intricate processes. Furthermore, not much work has been done on providing security at different levels in IoT communications, which can ensure data integrity.Considering this, an effective and efficient data securing method must be proposed to overcome these limitations.

3. Proposed Work

This section gives a detailed information about proposed model for securing data in IoT environment. As mentioned earlier, current security systems are not strong enough, when it comes to protecting data over IoT network. Because of this, attackers can easily invade and get access to confidential or sensitive information, creating a security barrier. This served as the motivation for proposed work, wherein, a multi-layered security approach is developed for overcoming the limitations of current encryption techniques and providing double security to IoT data.The key objective of proposed work is not only to protect data at multiple layers but to reduce the encryption time (ET) and Decryption Time (DT) also. To achieve this goal, three effective techniques i.e., Chaotic map, DNA sequencing and blockchain are usedin proposed model to offer security at different levels. Initially, a chaotic map is implemented for key generation then DNA based encryption technique is implemented for encoding and decoding data and finally, blockchain concept in introduced for recording and securing encryption activities to ensure data integrity and robust key management system.Moreover, the reason for selecting chaos based key generation technique in proposed work is that it offers high security, ensures quicker encryption and decryption process, and has low computational complexity than other techniques. Also, DNA has been used in proposed work because it has high computational speed with least power and storage. The DNA can store data of whole world in just few milligrams as DNA’s 1gram comprises of 1021 bases which is equal to 108TB. To further increase the robustness of proposed approach, blockchain is used, which has strong encryption strategy, making it perfect to be used in IoT systems. Blockchain's capacity for third-party verification of public keys enhances trust in the encryption process. Moreover, it provides a secure key management system, effectively mitigating key compromise risks. Thus, blockchain technology is chosen as the cornerstone of our multilayer encryption model, offering a comprehensive solution to the challenges presented by traditional encryption methods, and ensuring the highest standards of data security and reliability.

The proposed system is implemented on two types of data, one is textual data and other is medical image data taken from Kaggle.com. For securing a data, chaotic map is used for generating keysby employing logistic maps. The value of key is determined through two model parameters i.e., r and x.However, the chaotic map produces data in numeric form between 0 to 4, but DNA needs data in binary form for performing encoding. Therefore, T factor is used in proposed work, which serves as threshold value. By using this factor, any value above T value is taken as 1, otherwise 0. In the next step, DNA sequencing is used for encoding the data by creating pairsof four nucleotides i.e., A, T, C and G,using any one defined rule. After this, Blockchain is implemented on encoded data in which SHA-256 is used for creating the 32 bytes hash value of data. This output is unique for different inputs, thereby ensuring data integrity. Moreover, even a small change in the input data results in a significantly different hash, providing a high level of security against collisions. This final encrypted message or image is passed over the IoT network and is finally been decrypted at the receiving end, by following the reverse process. The step by step working of proposed model is explained in next section of this paper.

4. Methodology

The proposed model undergoes through three layers of security wherein chaotic maps are used for generating high security keys, DNA is used for encoding data and blockchain is used for key management and improving security further. Here, two inputs i.e., a textual data and medical image data is taken that needs to be encrypted for safeguarding the information over IoT network. Two main operations i.e., Encryption and Decryption are performed on given data, whose diagrams are shown in Fig 1 and Fig 2 respectively.

4.1 Input Data

In the first step of proposed work, an input data is taken upon which encryption needs to be applied. Here, data is taken in two forms (as shown in Fig 1), one is textual data of 100 characters and other is medical image taken from Kaggle.com. The given dataset comprises a total of 253 brain tumour MRI images, out of which 98 are normal and 155 are tumour images. In order to effectively understand the application of proposed model on both datasets, we have taken samples of textual data and image data. The original sample text data is given below, while as medical image is shown in Fig 3 (a) and its histogram image is shown in Fig 3 (b) respectively.

Sample of original text data= {The Internet of Things}

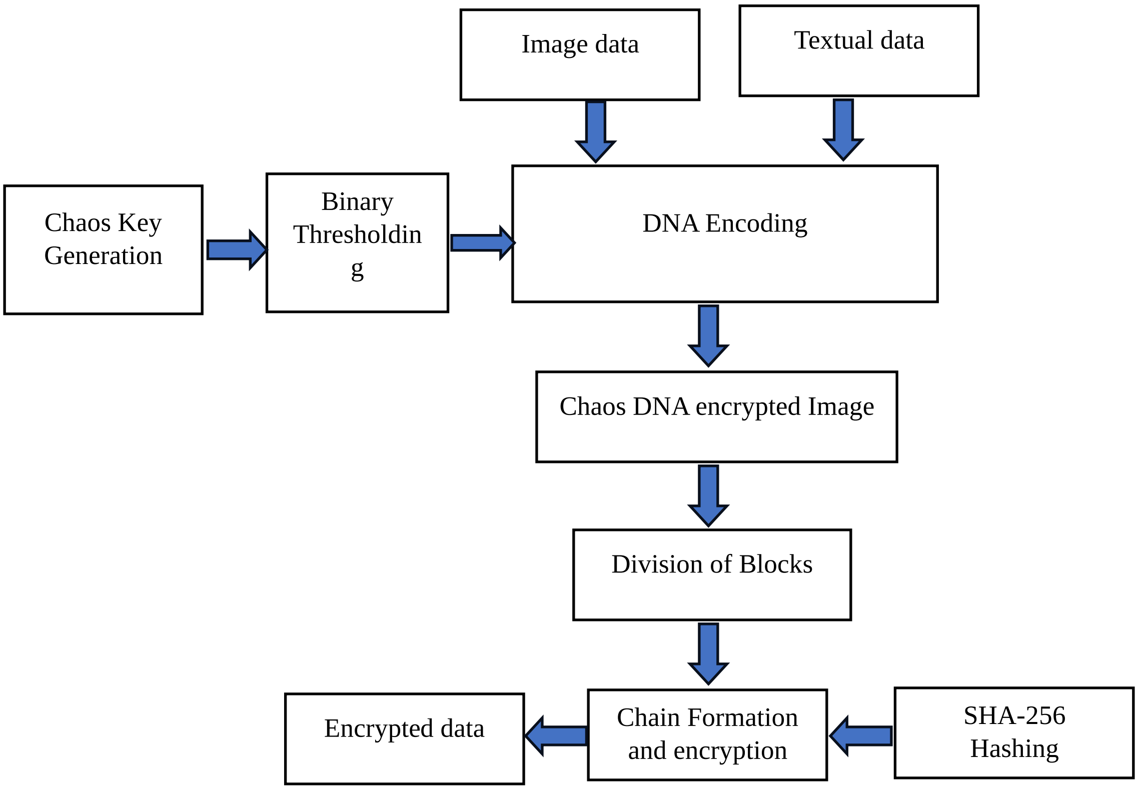


Fig 1: Encryption process in proposed Work

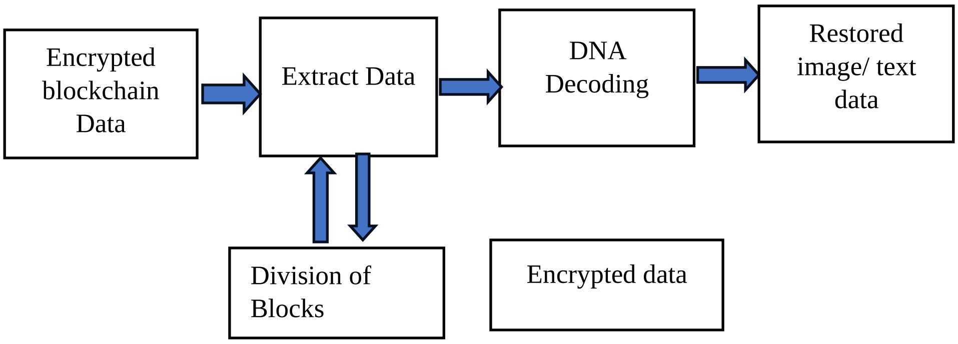
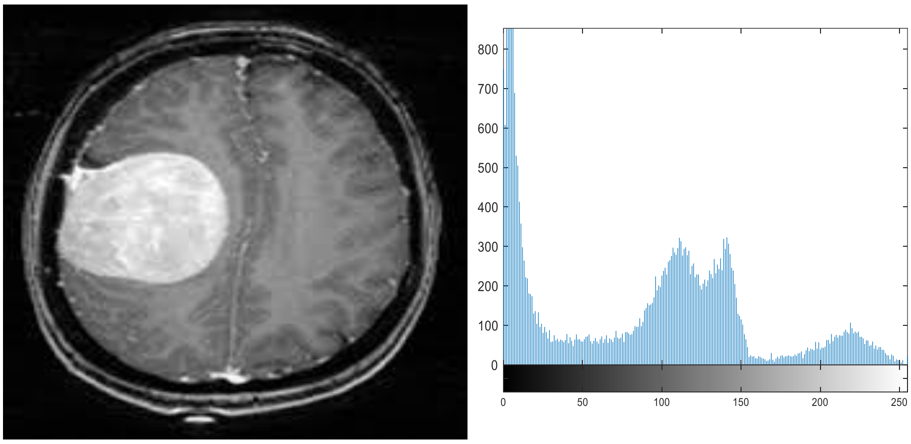


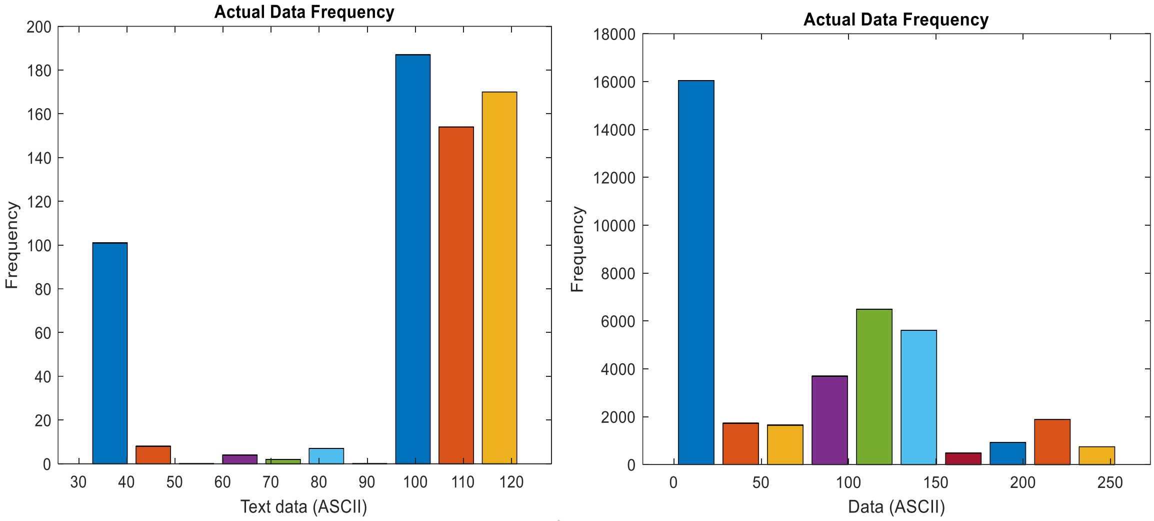
Fig 2: Decryption Process in proposed Work

After this, the frequency of words in actual data is observed that specifies how frequently words or data is repeating in the original data. However, the frequency of the characters is determined in terms of their ASCII codesto provide numerical representation of characters that can be easily counted, sorted and analysed. Fig 4 (a) and (b) shows the frequency of characters/data in textual and image data respectively.



(a) (b)

Fig 3: Brian tumour image and its histogram in (a) and (b)



(a) (b)

Fig 4: Actual data frequency of two inputs

4.2 Key Generation using Chaotic map

Generating key is the next step of proposed work wherein encryption is done by using public key and for decrypting this data, private or secret key is used at receiving end. Here, chaotic map is used for generating key because of the high security and less complexity they offer. Basically, chaotic map is 1D function which can be used in 2D applications as well, by doing some basic modifications. Here, chaotic logistic maps are used for generating the 2D key of for given data, by using equation 1.

$$X_{n+1} = rX_n(X_n - 1) \qquad (1)$$

Wherein, X_n depict the logistic function whose value ranges from 0 to 1, while as, value of r in given equation ranges rom 0 to 4. It must be noted here that value of “r” determines the behaviour of given logistic function. Particularly, the logistic function creates several output forms depending on the value of“r”. If the value of r falls between 0 and 1, then output obtained is considered as fixed and stable with values close to 0. On the other hand, if the value of “r” is above 1 and equal to 3, then output values is close to (r-1/r). Likewise, periodic attractors are present in output value if values range from 3 to 3.57 and in between 3.57 to 4, output obtained in chaotic. Furthermore, in order to determine the length of key, the value of N in proposed model is taken as 8 bits. However, keys are generated in numerical form but DNA encoding accepts data in binary form only, hence numeric data needs to be converted into binary form. To accomplish this task, a threshold factor “T” is introduced in the proposed work whose value if 0.65. Any key value above than T is considered as 1, while for other cases, key value if taken as 0. By doing so, we are able to generate secured keys in binary form using the concept of chaotic maps. The specific value of different parameters used during key generation process are given in Table 1.

Table 1: Values of different key generating parameters

Factors	Values
R (Control parameter)	3.9
X0	0.5
N (iterations)	8
T (threshold for bin key)	0.65
Data	8 Bit

Now, before applying the DNA encoding technique on this data, XOR operation is performed on input data and key generated to create ciphertext. This is done to because even a small change in input data or the key results in completely different output, enhancing security.

4.3 Data Encoding using DNA

In the next step, process of encoding is started in which DNA sequencing is applied to given ciphertext or cipher image. DNA comprises of polymers with billions of nucleotides and every nucleotide is made up of 4 bases i.e., A, T, C and G. By utilizing these four nucleotides, pairs are formed which are used for encoding the secret information. Moreover, DNA sequences are created in the proposed work for encoding secret message by using any one rule given in Table 2.

Table 2: Data Encoding rules of DNA

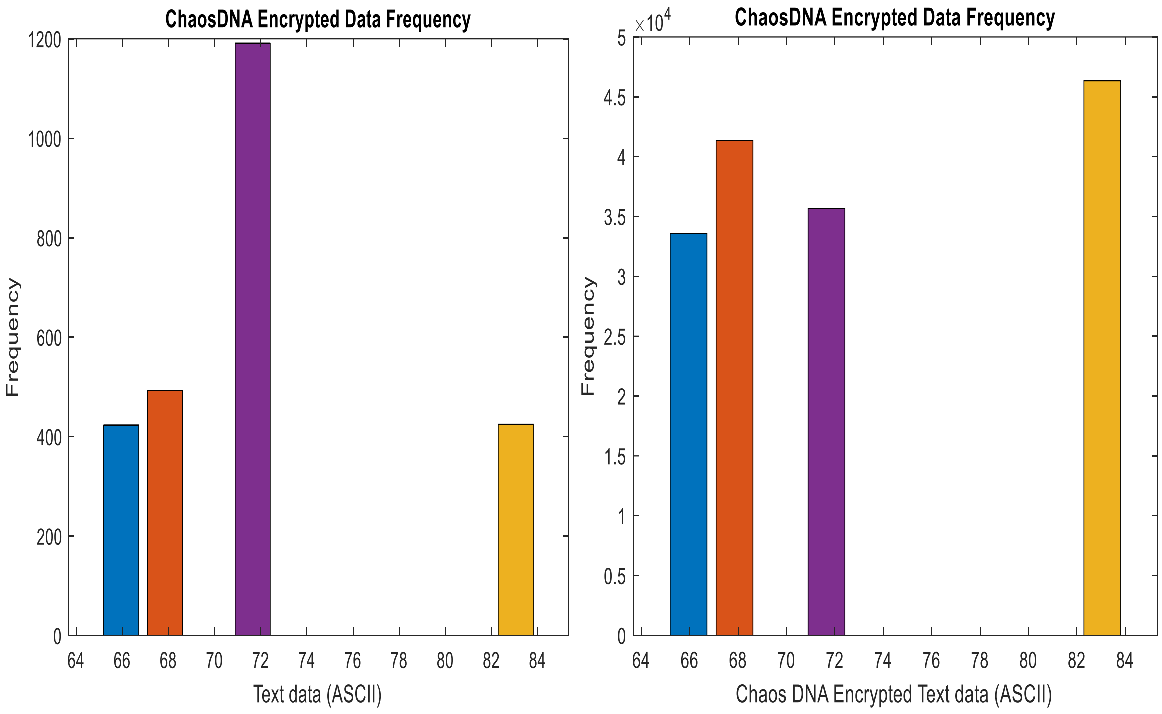
Base	A	C	T	G
Rule 1	00	10	01	11
Rule 2	00	01	10	11
Rule 3	01	11	00	10
Rule 4	01	00	11	10
Rule 5	10	11	00	01
Rule 6	10	00	11	01
Rule 7	11	10	01	00
Rule 8	11	01	10	00

In the proposed work, Rule 1 is followed for encoding the secret data (text and image). The encoded data obtained for given text is shown below.

ChaosDNA Encrypted input Data={GAAAGGGAGGATCGTAGTGTG}

At this stage, again the frequency of characters in encoded data for given text and imageis analysed and the figure obtained for the same is shown in Fig 5 (a) and (b) respectively. The x-axis andy-axis of the two graphs depicts the DNA encoded text and their frequency respectively.

Below figures show, that for textual data nucleotide G is showing highest frequency while as, for image data nucleotide T is showing highest frequency. Once the data is encoded, 32-bit blocks are created which will be used in the next phase of proposed model.



(a) (b)

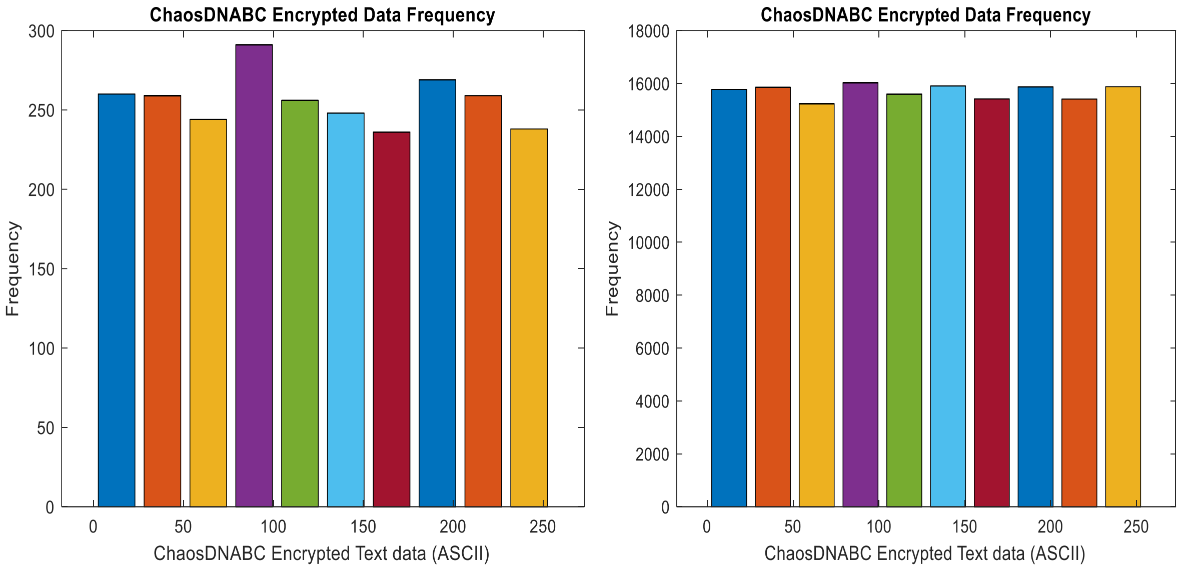
Fig 5: Encoded data generated by ChaosDNA technique

4.4 Encrypting Data using Blockchain

In the next phase, the blocks formed in the previous phase are used by blockchain technique for creating a chain and encrypting data.A blockchain can typically be defined as digital ledger which contains record of every transaction that has ever taken place in the network. As the name of the technique suggested, a number of blocks are linked together through a unique hash value. The very first block of the chain is refereed as Genesis block. Each block in the chain relates to previous block through a hashing address and includes all information. In case of proposed model, the first 32-bit block formed in previous step serves as the genesis block that contains all information in encoded form. After this, hash value of block is calculated. Here, SHA-256 hashing technique is used for calculating the hash value of encoded blocks. It produces a 256-bit (32-byte) hash value, making it computationally infeasible to generate the same hash from different data. Any small change of data inside block, will reflect changes in its hash value as well, demonstrating high level data security. Before adding a block to the blockchain, the data within the block, including transaction details, is hashed using SHA-256. This hash value uniquely represents the data within the block. Each block in the blockchain contains a header. The header includes several components, one of which is the hash of the previous block's header. This creates a chain of blocks, where each block's integrity is ensured by the hash of the previous block. In the next step, miners in blockchain compete to find a specific hash valuethat, when hashed with the block data, produces a hash that starts with a specific number of leading zeros. This process involves changing a nonce value in the block header and repeatedly hashing the block data using SHA-256 until the desired hash is found. Once a block is added to the blockchain, changing any data inside the block would require changing the hash of the block. Since SHA-256 is a cryptographic hash function with strong properties like collision resistance, it is computationally infeasible to reverse-engineer the original data from its hash. This immutability ensures the security and integrity of the blockchain data. Finally, at the end of this step, an encrypted message is received for given text, which is shown below.

Chaos DNA-Blockchain Encrypted data= {YOe” vÞkËJ¿ ðŽ í• HÇ• Ç¢Ó6'ÇY¸qx}

The frequency of finally encrypted data is again calculated for showing the effectiveness of proposed approach. Fig 6 (a) and (b) depicts the frequency of data for text and images respectively.



(a) (b)

Fig 6: Frequency of final encrypted data using proposed technique

Above two graphs clearly show the increased number of combinations formed after applying the blockchain on encoded data. This signifies that ample number of combinations can be formed for a single input data, which makes it difficult for any unauthorized person to access the confidential information. This encrypted data is then transmitted over the internet and is ready to be received at the receiving end.

4.5 Decryption Process

Once the data is received by the intended user, decryption process is started that is just the reverse process of encryption. During this process, data is extracted from the encrypted blockchain by using SHA-256 hasher. After this, DNA decoding method is implemented on the extracted data by using chaos keys. Finally, the original data is being restored by the authentic user.

4.6 Performance Analysis

In the last phase of proposed work, the efficacy of the proposed technique is validated by analysing its encryption time and decryption time. The results obtained for the time is explained in next sections of this paper.

4.7 Results Analysis

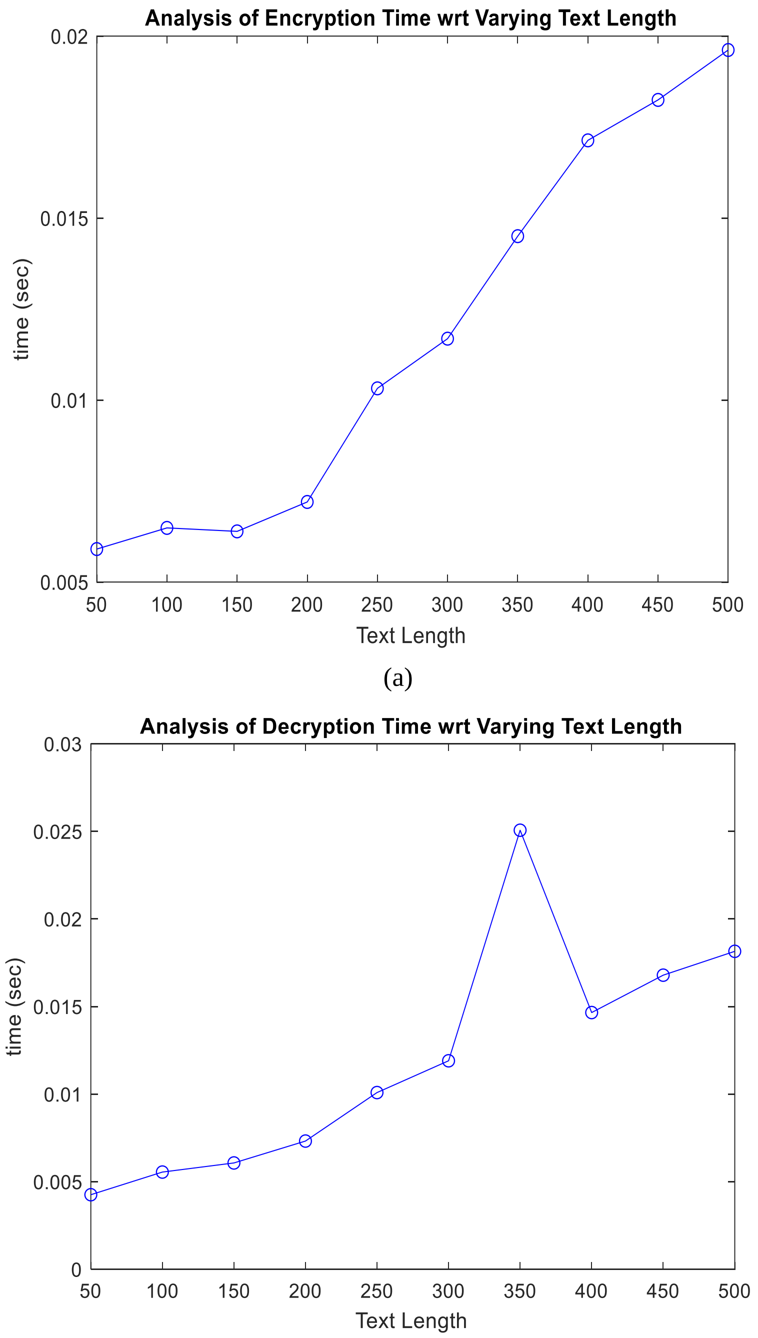
The efficacy of the proposed chaotic-DNA and blockchain (CIDNABC) based approach is tested and validated by using MATLAB 2018 softwareinstalled in a system with 8GB RAM and 500 GB hard disk. The simulating outcomes were obtained in terms of time taken by standard and proposed technique for encryption and decryption for standard text lengths. In addition to this, we have noted down the time for encrypting and decrypting data for varying text lengths. The detailed analysis of the results is explained in this section of paper.

4.8 Performance Evaluation

To begin with, initially performance of proposed CIDNABA method is endorsed by contrasting it with standard models like DVA, RSA, and hybrid RSA-DNA in context of their encryption and decryption time when text length is fixed at 100. The results obtained for the same are shown in Table 3. As per the data given in the table, it is observed that hyrbidRSA-DNA based technique is taking longer time of 0.228 seconds for encrypting data while as, its decryption time is also high at 0.202 seconds, making it the slowest technique in terms of processing time for the given operations. Moreover, RSA, a widely used asymmetric encryption method, takes 0.162 seconds for encryption and 0.128 seconds for decryption, again displaying slower performance due to its complex mathematical operations. In contrast, standard DNA encryption and decryption times are 0.08 and 0.054 seconds, respectively, showcasing its swift processing due to parallel computing inspired by biological systems. On the contrary, CIDNABC stands out as the fastest technique, taking merely 0.03039 seconds for encryption and 0.02579 seconds for decryption for 100 text length, due to its effective key management and blockchain concept.

Table 3: Analysis of different technique for ET and DTwith Fixed text length

Algorithm	Encrypting Time	Decrypting Time
DNA	0.08	0.054
RSA	0.162	0.128
BothRSADNA	0.228	0.202
CIDNABC	0.03039	0.02579



(a)

(b)

Fig 7: ET and DT of proposed model with varying text lengths

Furthermore, to prove the supremacy of proposed CIDNABC approach, its performance has been analysed and examined for varying text lengths (from 50 to 500) in terms of encrypting and decrypting times. The line graph obtained for the same is shown in Fig 7 (a) and (b) respectively. The horizontal line of the graph showcases different text lengths while as vertical line depicts time values. The given graphs reveal that as the data length increases, both encryption and decryption times also increase, indicating a clear linear pattern. It is observed that with a data length of 50, encryption takes only 0.005905sand decryption takes only 0.0042581s in proposed model. However, when the text length is maximum at 500, encryption time extended to 0.0196180s, and decryption time also increased to 0.01815s. The same pattern is followed for encryption process, but when decryption time is analysed closely, we see that when the text length reaches 350 and continues to increase up to 500, the decryption time decreases rather than following the expected trend of increasing processing time with longer data. This decrease in decryption time for data lengths of 350 or higher suggests a potential optimization of proposed model in the decryption algorithm used. The specific values of the ET and DT across different text lengths are given in Table 4.

Table 4: ET and DT in proposed model for varying text lengths

Data Length	**Encryption Time (sec)**	**Decryption Time (sec)**
50	0.005905	0.0042581
100	0.006487	0.0055515
150	0.006391	0.006072
200	0.007200	0.0073218
250	0.0103217	0.010090
300	0.0116864	0.01190
350	0.014503	0.02506
400	0.0171355	0.01465
450	0.0182465	0.0167
500	0.0196180	0.01815

Table 5: Analysis of different technique for ET and DT with varying text length

Algorithm	Encrypting Time	Decrypting Time
DNA	15.86	3.801
RSA	16.641	13.766
BothRSADNA	31.329	18.272
CIDNABC	1.6951	1.6551

In addition to this, when input data is changed from textual data to medical image data, the performance of proposed model is again tested across standard models with respect to time taken from encrypting and decrypting data. The resulting time values are recorded in Table 5. After carefully observing table data, it is observed that DNA stands out as the fastest among traditional models, taking only 15.86 seconds for encrypting image data, followed closely by RSA with 16.641 seconds and finally, BothRSADNAclocking in at 31.329 seconds, making it comparatively slower. However, CIDNABC shines as the most efficient encryption technique, taking merely 1.6951 seconds for encrypting given image data. Likewise, decryption process paints a similar picture, with DNA demonstrating impressive speed among other traditional models at 3.801s, while RSA and BothRSADNAtaking more time of 13.766s and 18.272 seconds for decryption, indicating their slower performance. On the contrary, proposed CIDNABC, again, proves to be the most efficient, taking only 1.6551 seconds for decrypting image data at another end. These results underline the diverse efficiency levels of these algorithms, with CIDNABC emerging as the optimal choice for both encryption and decryption, showcasing its potential for applications where swift data security processes are imperative.

Findings obtained from results reveal that proposed CIDNABC method is taking less time for encrypting and decrypting data across three cases i.e., with fixed text length, varying text length and image data. These results prove that by using chaotic map for key generation, DNA for encoding data and blockchain for encrypting it, an effective data security mechanism is established that can be implemented in real world scenarios.

5. Conclusion

This paper introduces a novel data security model namely as, CIDNABC, whose performance is rigorously evaluated using MATLAB across fixed text length, varying text length, and image data. The results obtained from our experiments present a compelling case for the efficiency and effectiveness of CIDNABC in securing data. In the context of fixed text length, CIDNABC outperforms other algorithms with encryption and decryption times as low as 0.03039s and 0.02579s, respectively, showcasing its remarkable speed. Moreover, when text length varies from 50 to 500, proposed CIDNABC technique continues to demonstrate its superiority by maintaining comparatively low encryption and decryption time even with increase in text lengths. The ET is only 0.005905s for 50 text lengths which increased to 0.0196180 when text length is extended to 500, which is not exceptionally high. Moreover, our model exhibits exceptional adaptability in handling image data which is encrypted in only 1.69s while as, traditional models like DNA, RSA and BothRSADNA took 15.8s, 16.6s and 31.32s respectively. These results show that proposed model is taking less time for both processes and hence is more effective than other similar methods.

References

[1] MarketsandMarkets. (2021). IoT market by component, application, vertical, and geography - global forecast to 2025. Retrieved from https://www.marketsandmarkets.com/Market-Reports/iot-market-573.html

[2] Pyingkodi, M., et al. "Sensor based smart agriculture with IoT technologies: a review." *2022 international conference on computer communication and informatics (ICCCI)*. IEEE, 2022.

[3] Xiong, H., Wang, C., Huang, Y., & Zhou, X. (2020). IoT security: Threats, challenges, and solutions. Journal of Cybersecurity, 6(1), tyaa004. https://doi.org/10.1093/cybsec/tyaa004

[4] Karie, Nickson M., et al. "A review of security standards and frameworks for IoT-based smart environments." *IEEE Access* 9 (2021): 121975-121995.

[5] Xu, Q., Xu, L., & Yin, X. (2019). Blockchain meets IoT: Challenges and opportunities. Journal of Industrial Information Integration, 15, 29-34. https://doi.org/10.1016/j.jii.2019.03.003

[6] Younas, M., Raza, B., & Muhammad, G. (2019). A comprehensive survey of security and privacy issues in internet of things. Journal of Network and Computer Applications, 126, 22-43. https://doi.org/10.1016/j.jnca.2018.10.020

[7] Cagliero, L., & Rebaudengo, M. (2018). Survey of IoT Security from the Data Encryption Perspective. IEEE Internet of Things Journal, 5(6), 4426-4446. doi: 10.1109/JIOT.2018.2843541

[8] Satamraju, Krishna Prasad. "Proof of concept of scalable integration of internet of things and blockchain in healthcare." *Sensors* 20.5 (2020): 1389.

[9] Elamir, Mona M., and May S. Mabrouk. "Secure framework for IoT technology based on RSA and DNA cryptography." *Egyptian Journal of Medical Human Genetics* 23.1 (2022): 1-7

[10] Khobzaoui, Abdelkader, et al. "DNA-based cryptographic method for the internet of things." *International Journal of Organizational and Collective Intelligence (IJOCI)* 12.1 (2022): 1-12.

[11] Kumar, Anuj. "Data Security and Privacy using DNA Cryptography and AES Method in Cloud Computing." *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2021.

[12] El-Shafai, Walid, et al. "An efficient multimedia compression-encryption scheme using latin squares for securing Internet-of-things networks." *Journal of Information Security and Applications* 64 (2022): 103039.

[13] Bendaoud, Salma, Fatima Amounas, and El Hassan El Kinani. "A new image encryption scheme based on enhanced elliptic curve cryptosystem using DNA computing." *Proceedings of the 2nd international conference on networking, information systems & security*. 2019.

[14] Patnala, B.D., Kiran Kumar, R. (2019). A Novel Level-Based DNA Security Algorithm Using DNA Codons. In: Computational Intelligence and Big Data Analytics. SpringerBriefs in Applied Sciences and Technology(). Springer, Singapore. https://doi.org/10.1007/978-981-13-0544-3_1

[15] A. Musa and A. Mahmood, "Client-side Cryptography Based Security for Cloud Computing System," 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 2021, pp. 594-600, doi: 10.1109/ICAIS50930.2021.9395890.

[16] S. Kumar, G. Karnani, M. S. Gaur and A. Mishra, "Cloud Security using Hybrid Cryptography Algorithms," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2021, pp. 599-604, doi: 10.1109/ICIEM51511.2021.9445377.

[17] Kifouche, A., Azzaz, M.S., Hamouche, R. et al. Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications. Int. J. Inf. Secur. 21, 1247–1262 (2022).