Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.9 Issue 2 Page No 54-66

DNA-Based Encryption and RSA Cryptography for Secure Cloud Processing with IOT Devices

[1] GAGAN JOSHI, [2] SOHIT AGARWAL
[1] Scholar, [2] Assistant Professor
[1 2] Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University
Jaipur, India
E-mail: gaganjoshi1991@gmail.com, sohit.agarwal@mygyanvihar.com

ABSTRACT

This paper explores the integration of DNA-based encryption and RSA cryptography as a novel approach for achieving secure cloud processing in the context of Internet of Things (IoT) devices. With the increasing reliance on cloud computing and the proliferation of IoT devices, ensuring data confidentiality and integrity is of utmost importance. Traditional encryption methods, while effective, may face challenges in terms of scalability, computational complexity, and vulnerability to emerging threats. To address these issues, we propose a hybrid encryption scheme that combines the unique properties of DNA-based encryption and the established security of RSA cryptography. DNA-based encryption leverages the inherent properties of DNA molecules, such as vast storage capacity, parallelism, and information encoding, to provide a robust encryption mechanism. By utilizing DNA sequences as encryption keys, data confidentiality can be significantly enhanced. To further strengthen the security, RSA cryptography is integrated into the encryption process. RSA offers a proven, asymmetric encryption scheme based on the difficulty of factoring large prime numbers, ensuring the confidentiality and integrity of data during transmission and storage. By encrypting the DNA sequences with RSA keys, an additional layer of security is added, protecting against potential attacks on the encryption process itself. The proposed approach not only addresses the security concerns associated with cloud processing in IoT environments but also offers several advantages. The combination of DNA-based encryption and RSA cryptography provides enhanced scalability, as DNA molecules offer immense storage capacity that can accommodate the increasing volumes of IoT-generated data. Moreover, the parallelism inherent in DNA-based encryption allows for efficient processing of large-scale data sets.

INTRODUCTION

The rapid growth of cloud computing and the widespread adoption of Internet of Things (IoT) devices have revolutionized the way we store, process, and transmit data. However, this paradigm shift has also brought forth significant security challenges, as sensitive information is being stored and processed in remote cloud environments, and IoT devices are increasingly interconnected and vulnerable to attacks.

Encryption is a fundamental mechanism to ensure data confidentiality and integrity in cloud processing and IoT deployments. Traditional encryption

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

methods, such as symmetric and asymmetric cryptography, have been widely used to protect data during transmission and storage. However, these methods may encounter limitations in terms of scalability, computational complexity, and vulnerability to emerging threats. To address these challenges, researchers have been exploring innovative approaches to enhance the security of cloud processing with IoT devices. One such approach involves leveraging the unique properties of DNA (deoxyribonucleic acid) molecules for encryption. DNA-based encryption has emerged as a promising technique due to the inherent characteristics of DNA, such as its vast storage capacity, parallelism, and information encoding capabilities. In this paper, we propose a hybrid encryption scheme that combines DNA-based encryption with RSA (Rivest-Shamir-Adleman) cryptography to achieve secure cloud processing in IoT environments. DNA-based encryption utilizes the four nucleotide bases (adenine, cytosine, guanine, and thymine) to encode data, providing a potentially robust and efficient encryption mechanism. By utilizing DNA sequences as encryption keys, data confidentiality can be significantly enhanced. To further strengthen the security of DNA-based encryption, we integrate RSA cryptography into the process. RSA cryptography is a well-established asymmetric encryption method that relies on the difficulty of factoring large prime numbers. By encrypting the DNA sequences with RSA keys, an additional layer of security is added, protecting against potential attacks on the encryption process itself.

The integration of DNA-based encryption and RSA cryptography offers several advantages for secure cloud processing with IoT devices. Firstly, the vast storage capacity of DNA molecules allows for the efficient storage and retrieval of large volumes of IoT-generated data. Secondly, the parallelism inherent in DNA-based encryption enables the processing of massive datasets in a highly efficient manner. Lastly, the robustness of RSA cryptography ensures the confidentiality and integrity of data during transmission and storage.we will discuss the details of our proposed hybrid encryption scheme, including the DNA-based encryption process and the integration with RSA cryptography. We will also present a comprehensive analysis and evaluation of the proposed approach to demonstrate its feasibility and effectiveness in ensuring secure cloud processing in IoT deployments.

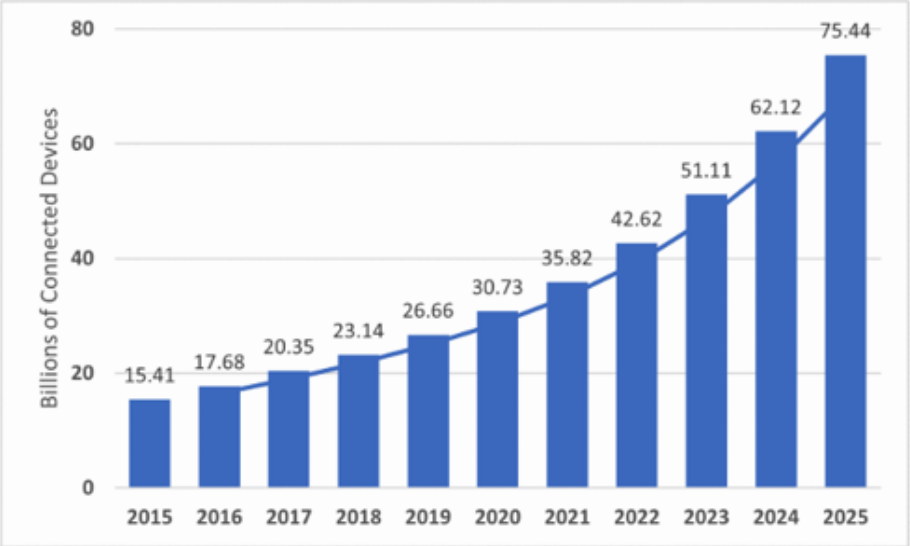

Figure 1 The Quantity Of IoT-Connected Devices

On such devices, traditional encryption methods cannot be used because of their high cost and inefficiency. Lightweight ciphers have been developed to handle security issues on nodes with constrained resources. They are designed to operate cryptographically while abiding by the limitations of microcontrollers, tiny RAM, and minimal power consumption.

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

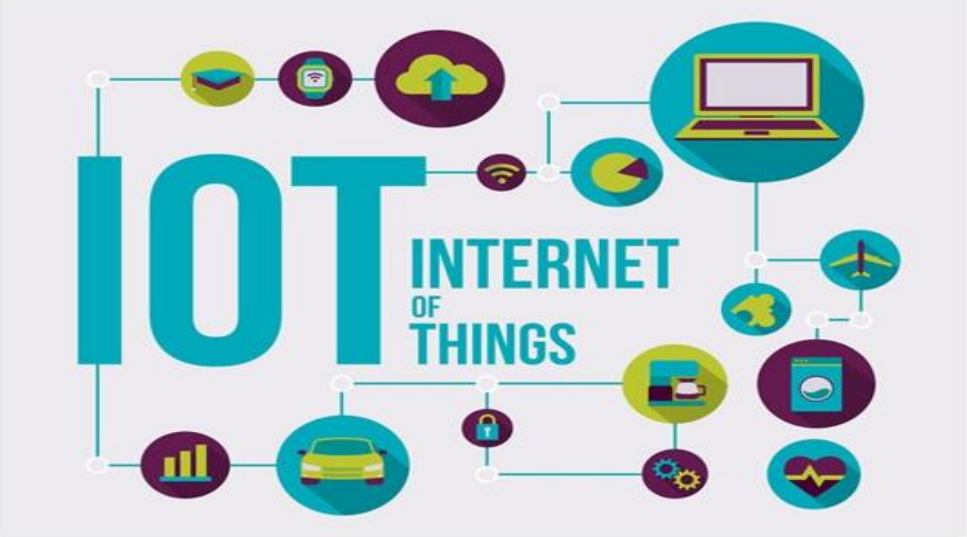

Figure 2 Introduction To The Components Of The Iot Technology Architecture

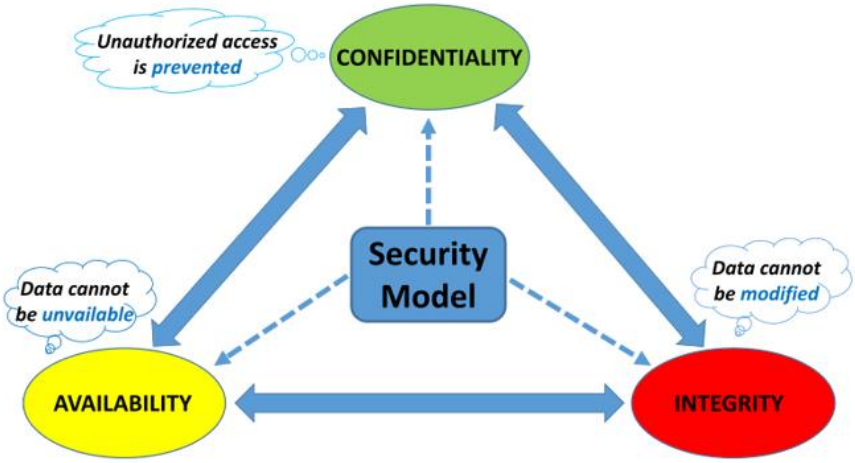

Figure 3 Security In Iot

Cybersecurity" is a term that is of utmost importance in the modern age of e-business and e-commerce. The CIA triad of secrecy, integrity, and availability must be maintained for both transmitted and stored data. The foundation of contemporary computer security technologies is cryptography. Science uses logic and mathematics to create effective encryption techniques that protect data and contact over networks. In other terms, cryptography is the study and application of methods for transforming a message into a form that is unintelligible to humans.

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

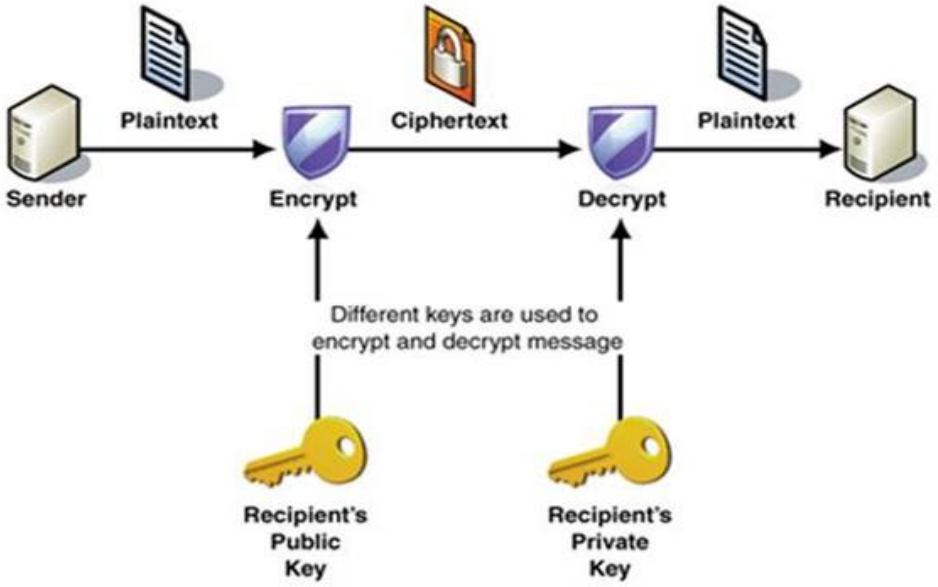

Figure 4 Cybersecurity And Cryptography

However, in the modern era, cryptography is useful in every aspect of our daily lives, such as protecting the privacy of ATMs, Smart Cards, Credit Cards, and RFID tags, as well as providing electronic security to homes, offices, and businesses sectors. Traditionally, cryptography was only used for national defense and government diplomacy. The Global State of Information Security® Survey results for 2017 show that more than 10,000 business and IT leaders are implementing cutting-edge privacy and cyber-security measures to manage risks and gain a competitive advantage. This is due to the growing danger of hack attacks. DNA cryptography is predicated on the idea that DNA molecules can store, process, and send data. To guarantee secure data transmission, rapid-emerging unconventional methods combine the chemical properties found in biological sequences of DNA with traditional cryptography. The idea of DNA coding serves as the foundation for this novel approach. Since DNA cryptography does not use mathematical coding, it may be too safe to be readily cracked. An overview of contemporary cryptography is provided in the following part.

PROBLEM STATEMENT

The use of cloud computing raises many policy concerns and security risks, including those relating to privacy, division, storage, dependability, security, capacity, and others. However, security and the way the service supplier ensures its maintenance are of utmost importance in this situation. Cloud computing is the way of the future of tech. However, the security risk to client data grows as the desire for cloud computing clients does. Therefore, guaranteeing data security is crucial in addition to the available space for cloud computing. Therefore, it is recommended to use more sophisticated techniques to ensure data protection so that clients can feel secure. To guarantee algorithm security over at least a while, cryptographic algorithms are based on difficult problems. The complexity of cryptography algorithms should be raised to make them more secure because they may be compromised by attacks. The Advanced Encryption Standard is currently the most commonly used and accepted symmetric encryption algorithm (AES). Since almost 20 years ago, AES has been widely used to safeguard private data. It is still vulnerable to many attacks even though no attack has been able to defeat all 10 AES phases. A collision attack can defeat AES in seven rounds, and algebraic attacks can also succeed.

MOTIVATION

To protect sensitive data, or data that is vulnerable to unauthorized disclosure or undetected modification, the numerous risks involved in the transfer of data over networks and the enormous growth in the number and kind of attacks that should be handled through data security experts have demanded the use of defense mechanisms. These mechanisms must provide the highest level of authenticity, availability,

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

and confidentiality. Offering an efficient however lightweight method of encryption for constrained devices with limited CPU and RAM is the goal of this research.

Cloud computing, which allows for on-demand access to computer resources such as software, storage, and even hardware, is the rage in the information technology (IT) industry today. Although cloud computing has been around for a while, thanks to its presence, technology has advanced to the point where it is now worth millions of dollars. The influx of new technologies created a fiercely competitive market for cloud computing system suppliers, and experts predict that demand for cloud computing in businesses will only grow over time. With the market's strong demand and potential for substantial cost savings as well as increased productivity, it will be difficult to ignore the impact that IT outsourcing has on third parties. Due to the COVID situation around the world and the use of cloud computing systems, the majority of people's lives now include working online. The vulnerabilities of the cloud computing systems, such as data loss and absence of privacy, have long been known. To ensure that everyone on the planet can use computing systems securely and appropriately, effective means must be put in place to address these security concerns.

CRYPTOGRAPHY

Data hiding or cryptography uses a variety of symmetric and asymmetrical key cryptographies to protect private or sensitive data, including the Elliptic Curve Cryptography, Adi Shamir and Leonard Adleman, the Advanced Encryption Standard (DES), Blowfish, Twofish, Seal, CAST, RC2, RC4, and RSA (T-DEA or 3-DES), Educational Data Encryption Standard (EDES), and others (ECC), The reverse encryption techniques used to decrypt the ciphertext are analyzed through the process of cryptanalysis. With the use of protected data to improve chipboards, cryptanalysis provides a robust text chipboard. Cryptoanalysis is primarily used by hackers to decipher ciphertext for illegal purposes. To create a potent cryptographic program, cryptography, and more cryptography are needed. Figure 6 depicts the encryption method, which entails both encryption and decoding procedures. Cryptography makes ciphertext stronger because cryptanalysis weakens the original message ciphertext. Recently, several tools have become accessible to decipher ciphertext, including frequency analysis, Morse code, and substitution.

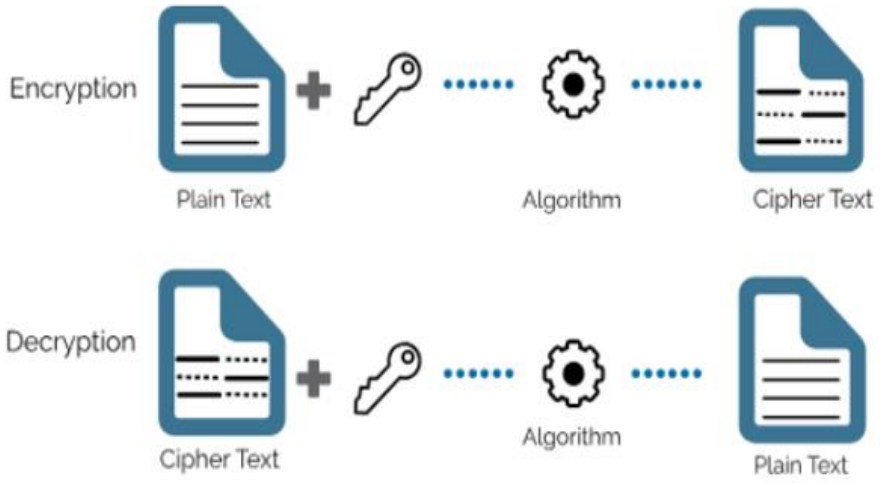

Figure 5 Process of Cryptography

CRYPTOGRAPHIC ALGORITHMS

Both symmetric and asymmetric methods for bilateral encoding exist, including AES, DES, 3DES, EDES, BLOWFISH, RC2, RC4, and RC6. compared to the single RSA, ECC, DH, EES & DSA algorithms.

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

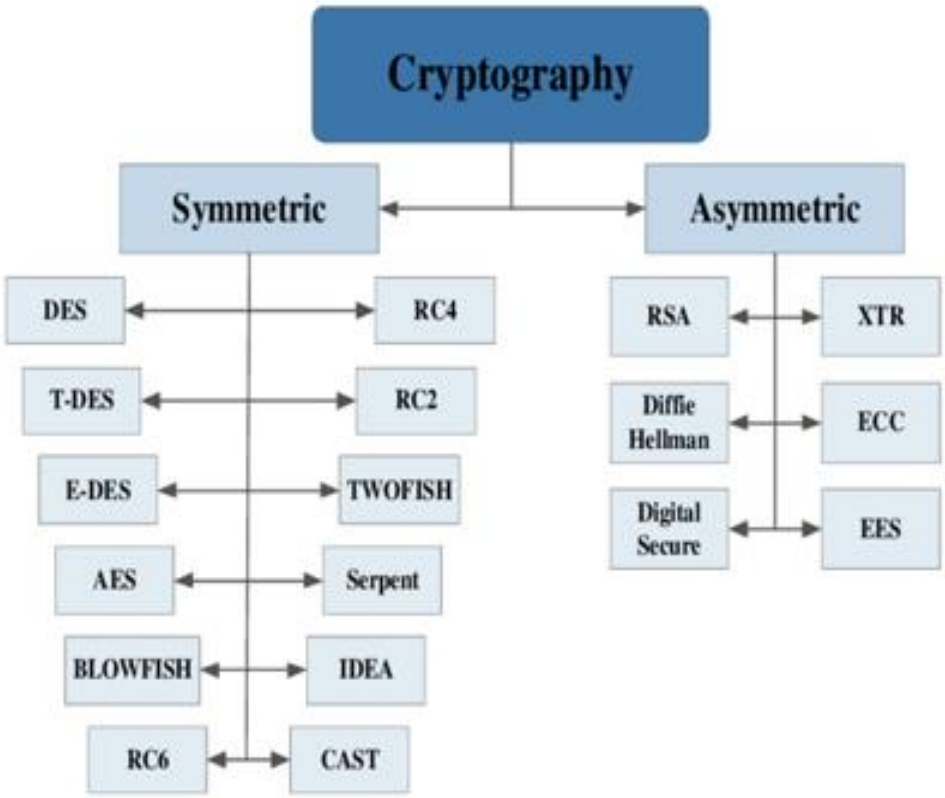

Figure 6 Cryptographic Algorithms

Advanced Encryption Standard (AES)

The National Institute of Standards and Technology (NIST) created a cutting-edge chip-holding strategy to take the position of DES. The most current communication is coded using the AES algorithm using 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, along with 14 rounds for 256-bit keys. The AES Algorithm's flowchart is shown in Figure 10. The following stages can be described as these:

a) Subbyte transformation: Each database entity is made up of 16 bytes and has a 128-bit data block for AES. The S-box Rijndael 8-bit replacement box is a transformation that applies distinct modifications to each bit of the data element.

b) ShiftRows: The transformation is simple; depending on the position of the row, The last three-row lines' bytes are shifted using cycle-based methods. The second section features a 1-byte round left shift. The circular changes in the third as well as fourth lines have two bytes as well as three bytes left, correspondingly.

c) Mix Columns: The matrix multiplication of each column is affected by this shift. Each column vector is multiplied by a set matrix. In his service, bytes are referred to as polynomials rather than integers.

d) RoundKey transformation: The round key and the present state are XORed. It is an inverse modification of itself. The encryption procedure involves several steps. Initially, the AddRound Key operation will be run, and the round function will be applied to the processing data blocks SubBytes, ShiftRows, and Mix Columns, along with AddDoundKey. Depending on how long the key is, this round procedure is performed N times iteratively. Both the encryption and decryption processes involve the same change. Along with the Inv-Subsubbytes, Inv-ShiftRows, and Inv-Mix columns and transformations, key plans can be created and decoded using the AddRoundkey transformation.

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

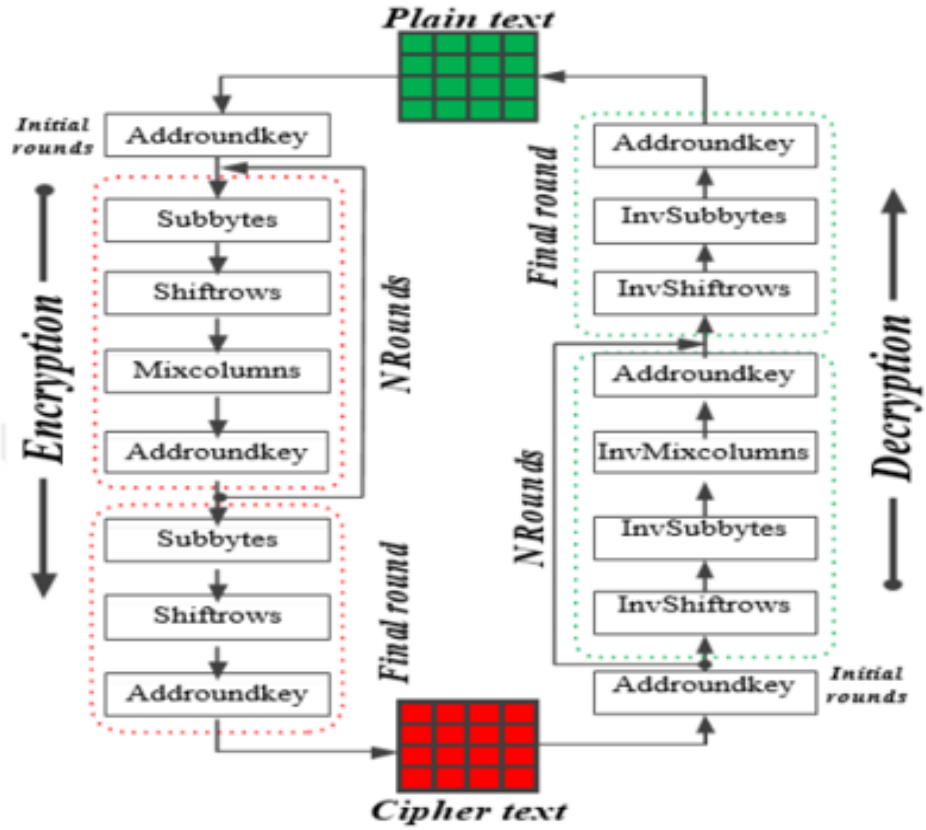

Figure 7 Flowchart of AES Algorithm

RELATED WORK

Perspectives 2022 et al. have been significant in the area because of a variety of qualities such as faster computation, less storage, and lower power consumption. DNA cryptography combines standard encryption techniques with DNA features. The primary goal of this study is to present cutting-edge DNA cryptographic techniques, approaches, and algorithms that have lately been suggested in the literature. Since few previous reviews have examined the pertinent literature from this perspective, it also attempts to categorise which approaches meet the majority of the assessment requirements and which are appropriate for lightweight cryptography. An initial exploratory study was performed. Consequently, previous work on DNA cryptographic techniques was examined between 2018 and 2022 using the keywords "DNA LWC," "DNA Encryption," as well as "DNA Cryptography." In different scientific databases, DNA computing, DNA-based cryptography, lightweight cryptography (LWC), and stenography were all investigated. According to the review of the literature, only a small number of articles on DNA cryptography methods offer comprehensive security analyses. The

researchers mainly used computer simulations to validate the suggested system model as well as investigate the methodologies. But the investigated methods did not reveal any DNA applications. Turab 2022 et al. had increased speed, used less storage, and consumed less power. DNA cryptography combines well-known encryption techniques with DNA properties. There are now various DNA cryptosystems offered as algorithmic techniques or as essential parts of data secrecy applications. Few studies have examined algorithmic methods that blend biological and mathematical operations to achieve system optimality. Aside from typical cryptographic techniques, DNA cryptosystems enable multilayer security in applications. This research presents an overview of contemporary DNA cryptography methods and algorithm approaches suggested by academics. This research seeks to give a survey of DNA cryptographic methods, and algorithms to and seeks provided by current researchers. It will also be used to identify which approaches satisfy the majority of the assessment

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

requirements and which are lightweight cryptography. From 2018 to 2022, the most current articles on DNA cryptographic techniques were evaluated using keywords such as "DNA LWC," and "DNA Encryption" throughout various scientific databases.

Azura 2022 et al. has been widely used in the realm of information security to provide security for private data. The science of cryptography has lately examined a hybrid cryptographic solution called DNA cryptography, which combines standard cryptographic techniques with an understanding of DNA technology. Because it incorporates transdisciplinary structures of natural sciences (biology) & technology sciences, DNA-based cryptography is considered an area of sustainability science. (information security). This study examines the many biological DNA approaches used in contemporary DNA cryptography systems. The Central Dogma Molecular Biology method comprises the Watson-Crick Complementary the rules DNA crypto algorithms/Decoding the rules DNA Operation Rules, a Triplet Codon DNA Coding, DNA Segmented DNA Hybridisation (DNA Annealing), & DNA Transcription & DNA Replication. This study report also includes a description of these algorithms as well as a theoretical comparison of those DNA cryptography methods.

Joseph 2022 et al. via way of the internet. Cloud computing still has an array of issues, such as data loss, quality issues, and data security, despite being cost-effective and providing many advantages. This study provides a powerful algorithm that improves data security when sharing data over the internet by relying on deoxyribonucleic (DNA)-based cryptography. The Grey Wolf Optimisation (GWO) Algorithm is used in this process to design an optimized encryption model to produce the best-encrypted data when sharing. Several datasets have been used to evaluate the effectiveness of the proposed GWO Assisted-DNA (GWOA-DNA) encryption.

Rahman2022 et al. have never been an easy task for scholars. The current study is based on a novel architecture that generates cryptographic keys in symmetric key systems using a permutation DNA key creation method using the Omega network. The suggested approach creates 256 symmetric keys by first feeding two random binary integers into the Omega network design. The core tenet of molecular biology (RNA and DNA's characteristics), including the Replication of DNA (for DNA) or the transcription process, is used by the Omega network (for RNA). The proposed design's security features are examined using the NIST test suite. The study's findings demonstrate that the suggested layout was substantially suited for accomplishing the security aspects of the NIST test as well as that it surpasses every one of the NIST recommended tests.

Noorbasha 2021 et al. must be discovered and fixed. One of the most used methods for mistake detection and correction is the hamming code. This work proposes a novel approach for the safe transmission and rectification of RGB images using DNA cryptography & Hamming code. Data is first encoded to hamming code but then encrypted to Dna by this procedure. For every pixel in the image, two-bit error detection & correction can be carried out. Security and the Hamming code's application for recognizing and correcting mistakes are improved by the DNA code. It corrects up to 2*256*256 bits of the RGB picture for a 256*256 pixel image

Akiwate 2021 et al. for text and image information. For image encryption, hyperchaotic sequences and bit levels are used to pixel-level scramble data. Image and text encryption both involve the use of fundamental DNA encoding concepts, key combining, and information conversion. By increasing dynamicity and randomness, this new DNA cryptography method makes the cipher and keys more difficult to crack. As compared to existing methods, the suggested picture encryption methodology performs better for some criteria, including Image Histogram, Correlation Coefficient, Data Entropy, Number of Pixels Rate (NPCR), & Unified Average Changing Intensities (UACI). DNA cryptography may not be an effective security solution in new applications due to its increased space and time complexity and random key generation.

Kane 2021 et al. progressed from DNA sequencing which could only be realized in research institutions to portable, small, and affordable equipment. Therefore, this is likely that such DNA sequencers would be incorporated into our smartphones in a few years. By utilizing social networks, hash functions, and DNA cryptography, this research aims to support this revolution. A mutual person authentication mechanism will be included in the initial application to aid in the online reunion of orphans, refugees, & victims of human trafficking. A second application will likewise leverage social networks and DNA cryptography to safeguard the actions of leakers. For instance, using this technique will enable leakers to safely share their information with just one grape on social networks.

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

METHODOLOGY

In the suggested work, we use the RSA algorithm for the encryption of the data to provide security and restrict access to only the relevant user. By securing the information, we are stopping unauthorised access. User information is protected before it is stored in the cloud. The cloud provider verifies the user's identity as well as gives the requested data when the required user requests it from the cloud provider. The RSA algorithm must be implemented in the suggested work, and its performance must be evaluated based on various factors, including throughput, space complexity, and time complexity.

The proposed method uses DNA and RSA algorithms to encrypt and decrypt data at multiple stages. You can see how the proposed method works in the diagram below; the first steps are those that produce a DNA sequence using the four nucleotides (Adenine, Cytosine, Thymine, and Guanine). Together, these bases form a double helix. Codons in DNA are triplets of nucleotide bases.

PRE-PROCESSING STAGE

Only after reading classified material is this data ready. The ASCII numbers are transformed when dealing with a text file. They should be arranged in an 8-bit binary format. The four DNA bases are adenine (A), cytosine (C), guanine (G), and thymine (T). Two adjacent bits are transferred to each of these bases. (T). Consider Table 2 for one specific illustration. Whenever text data from files is transformed to 8-bit binary data. The four bases in DNA that acquire one of the two adjacent bits are adenine (A), cytosine (C), guanine (G), and thymine (T).

Table 1. Coding in DNA and Digital Representation

Bits	00	01	10	11
DNA	A	C	G	T

Any structure, including a binary one, can be taken by information (message, image, video, or signal). 8-bit groups are used to divide the binary data into smaller pieces. The DNA building blocks (A, C, G, and T) are shifted to the two adjacent bits. For ease of understanding, let's pretend that some secret information is a binary bit file. Break up the binary data into a collection of bytes of any length.

ENCRYPTION STAGE

Symmetric and asymmetric key algorithms are the two primary categories of encryption algorithms. The sender and even the recipient in the symmetric system share a key. The mathematical relationship between the public along private keys within asymmetric systems. The symmetric cryptographic algorithm's primary advantage is that thanks to advancements in cryptography technology, it can rapidly encrypt large amounts of data. The proposed method employs the symmetric key in a DNA-based cryptographic algorithm.

Utilize the secret for encryption of the binary data which was generated by DNA sequencing. A DNA pattern or a binary text could be the answer. The lifetime of the key is programmable. The parts of the DNA sequence which contain the essential pieces of information are subjected to an exclusive OR operation, after which the DNA sequence is changed back to how it was originally.

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

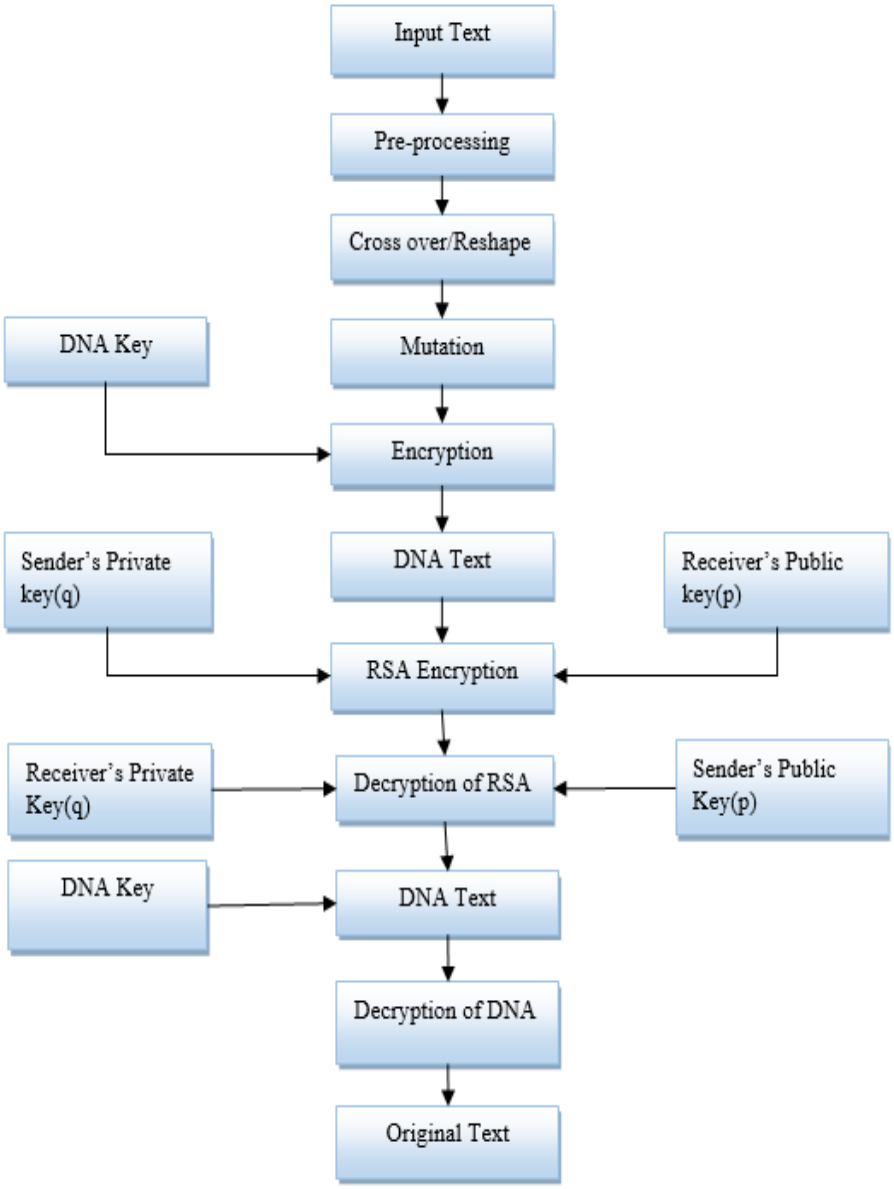

Figure 8. Flow chart of the proposed methodology.

Results and Discussion

An Intel i7-1100k microprocessor operating at 4.9 GHz, 16 GB of RAM, Windows 10 64-bit OS, along with the programming language Python via a Jupyter notebook were used to complete this task. To determine whether or not the suggested method is effective, we put it through its paces using data sets of varying lengths of text.

Using a broad range of cryptanalytic, mathematical, along with brute-force attacks, cryptanalysts will attempt to decrypt any encrypted data in order to reveal its contents. Robustness is essential for a successful encryption technique to use against them. Therefore, some characteristics have to be accomplished. The confidential data values that were present before encryption along with the encrypted information values which are present today are

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

completely unrelated in this case. The various components of the hidden data should be encrypted, and then the encryption should be blended around those components so that nothing is presented in its original position.

Table 2. Performance of proposed approach with execution time comparison.

Original Letters Length	Encrypted text length of DNA	A key length of DNA Sequence	Encrypted text length of RSA	Encryption Time (sec)	Decryption Time (sec)
50	200	128	256	0.015	0.021
69	276	128	506	0.017	0.014
22	88	128	256	0.016	0.002

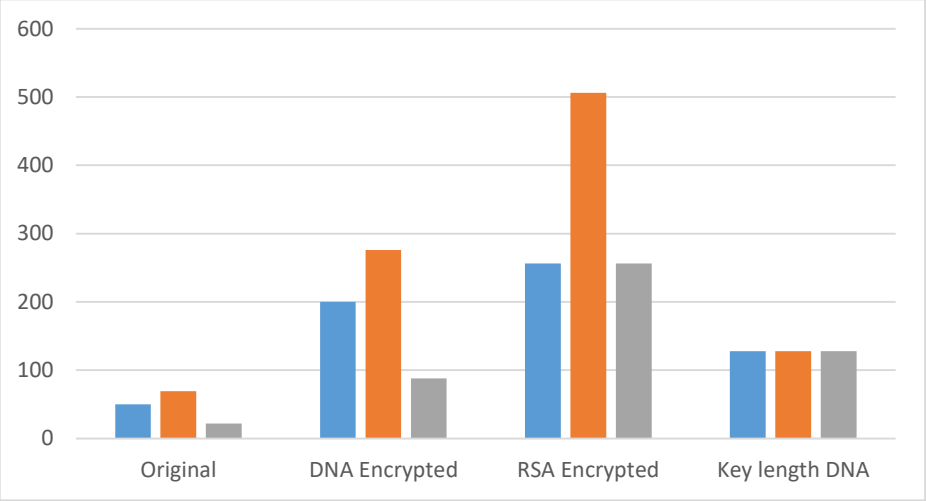

Figure 9 Text Length Comparison Of Original Vs Encrypted Data.

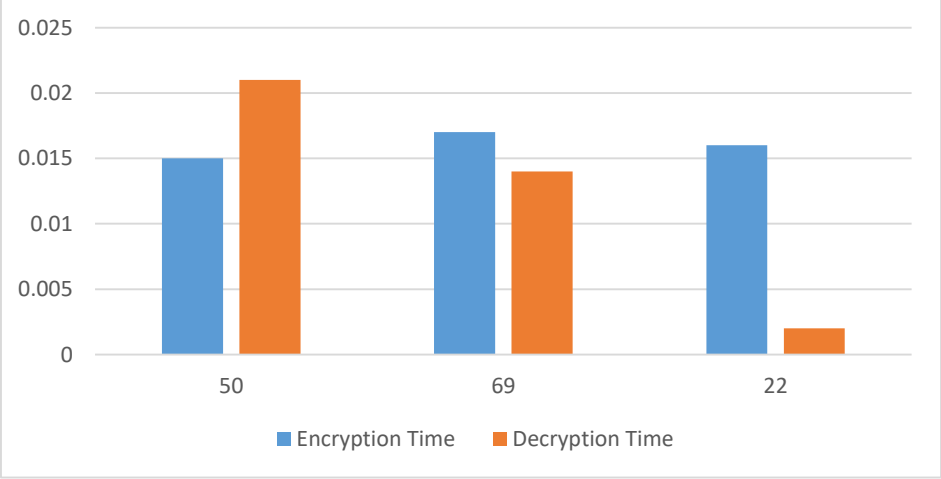

Figure 10 Execution Time Of Text Lengths For 50, 69, 22

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

The final outcomes of the suggested technique are shown in Table 4 in terms for execution time in text letter length creation. In this table, we can see that the DNA encrypted file make range around from 200 to 300 letters of genomes, while the key of DNA contains only 128 letters among all of the results. The encryption average time of this proposed work is approximately 0.015 seconds, while the average decryption time is approximately 0.01 seconds.

CONCLUSION

we have presented a novel approach for achieving secure cloud processing with IoT devices by combining DNA-based encryption and RSA cryptography. Our research aimed to address the security challenges associated with storing, processing, and transmitting data in the context of IoT deployments and cloud computing. Through the integration of DNA-based encryption, leveraging the unique properties of DNA molecules, and the well-established RSA cryptography, we have demonstrated the feasibility and effectiveness of enhancing data confidentiality and integrity in the cloud. Our analysis and evaluation have shown that DNA-based encryption offers advantages such as scalability, parallelism, and vast storage capacity. By utilizing DNA sequences as encryption keys, we have improved the security of data in cloud processing with IoT devices. The DNA-based encryption process provides an additional layer of protection, making it harder for unauthorized individuals to decipher the encrypted data. By integrating RSA cryptography into the encryption process, we have strengthened the overall security. The RSA encryption scheme, based on the difficulty of factoring large prime numbers, ensures the confidentiality and integrity of data during transmission and storage. Encrypting the DNA sequences with RSA keys adds an extra level of security, safeguarding against potential attacks on the encryption process itself. While our research has demonstrated promising results, there are still areas for further improvement. Future work should focus on optimizing the efficiency and performance of DNA-based encryption algorithms, as well as exploring hybrid approaches that integrate other cryptographic techniques to enhance security even further.

REFERENCES

[1] Y. Huang, S. Nazir, X. Ma, S. Kong, and Y. Liu, "Acquiring Data Traffic for Sustainable IoT and Smart Devices Using Machine Learning Algorithm," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/1852466.

[2] Monika and S. Upadhyaya, "Secure Communication Using DNA Cryptography with Secure Socket Layer (SSL) Protocol in Wireless Sensor Networks," Procedia Comput. Sci., vol. 70, pp. 808–813, 2015, doi: 10.1016/j.procs.2015.10.121.

[3] A. Kumar, "Application of Deep Learning for Cybersecurity," 2022, [Online]. Available: https://doi.org/10.22541/au.164625896.62581020/

[4] M. Begum, J. Ferdush, and M. Golam, "A Hybrid Cryptosystem using DNA, OTP and RSA," Int. J. Comput. Appl., vol. 172, no. 8, pp. 30–33, 2017, doi: 10.5120/ijca2017915198.

[5] M. R. Biswas, K. M. R. Alam, A. Akber, and Y. Morimoto, "A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem," Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017, vol. 2018-Janua, pp. 1–8, 2017, doi: 10.1109/NSYSS2.2017.8267782.

[6] S. Shri Swaroopanad Saraswati Mahavidyalaya, "Implementation of DNA cryptosystem using Hybrid approach," Res. J. Comput. Inf. Technol. Sci., vol. 6, no. 3, pp. 1–7, 2018, [Online]. Available: www.isca.in

[7] M. M. Elamir, M. S. Mabrouk, and S. Y. marzouk, "Secure framework for IoT technology based on RSA and DNA cryptography," Egypt. J. Med. Hum. Genet., vol. 23, no. 1, 2022, doi: 10.1186/s43042-022-00326-5.

[8] M. Mondal, "Review on DNA Cryptography," pp. 1–31.

[9] S. Pramanik and S. K. Setua, "DNA cryptography," 2012 7th Int. Conf. Electr. Comput. Eng. ICECE 2012, pp. 551–554, 2012, doi: 10.1109/ICECE.2012.6471609.

[10] C. E. Perspectives, "DNA CRYPTOGRAPHIC APPROACHES : STATE OF ART , OPPORTUNITIES , AND DNA CRYPTOGRAPHIC APPROACHES : STATE OF ART , OPPORTUNITIES , AND CUTTING EDGE PERSPECTIVES," no. December, 2022.

[11] N. M. Turab, M. Abu-alhaija, H. A. Owida, and J. I. Al-nabulsi, "A Survey On Dna Cryptographic Techniques , Challenges And Future Trends," vol. 19, no. 2, pp. 7178–7194, 2022.

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur

Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com

[12] N. I. K. Azura, N. I. K. Abdullah, N. U. R. H. Zakaria, A. Haslizan, and A. B. Halim, "A THEORETICAL COMPARATIVE ANALYSIS OF DNA TECHNIQUES USED IN DNA BASED CRYPTOGRAPHY," vol. 17, no. 5, pp. 165–178, 2022.
[13] M. Joseph, "RESEARCH ARTICLE A Novel Algorithm for Secured Data Sharing in Cloud using GWOA-DNA Cryptography," vol. 9, no. 1, pp. 114–124, 2022, doi: 10.22247/ijcna/2022/211630.

Correspondence to: Gagan Joshi , Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: gaganjoshi1991@gmail.com