iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5412

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Enhanced Cloud Security based on DNA Cryptography

Vandana CP[1], Abir bhattacharjee[2], Yashwant Pandit[3], Rakshith P[4], Peshal Parajuli[5]
[1]*Assistant Professor,* [2, 3, 4,5] *Students, Department of Information Science, New Horizon College of Engineering, Ring Road, near Marathahalli, Bangalore-560103, Karnataka, India*

Abstract: ***The two-level security level needs data storage into a medium-sized medium that has also been inserted into another media. Two covers can be the same or different depending on the features and applications. DNA cryptography is a neutral source that utilizes the evolution of the molecular and gives us the new hope of the algorithm that can not be explored but the principles need to be even more explored in DNA analyzes. Focus on DNA security protection by using an image design using DNA. This template explains how to apply to DNA Cryptosystem for securing data.***
Keywords: DNA, cryptography, DNA

I. INTRODUCTION

Cloud computing agrees that it should be very important in the development of technical knowledge as it provides important infrastructure, software and software as services. Cloud protection helps to increase the size of the volume that is crucial to money and individuals and a solution for the detection of the data that is being explored. Cloud calculations will become a major part of the future as of the Big data.

Cryptography is a mystery and private philosophy [1] [2]. It is studying some of the mathematical ideas and provides important guidelines for providing relevant privacy information such as privacy, data accuracy, personal information, and original source information

The potential algorithm is cryptosystems that whether the keypad is allocated for encryption and decryption [1] [5]. The algorithm of the best cryptosystems is very strong against possible possibilities, but it is a great disorder for the best cryptosystems that are harmful-to boost the keypad. This feature creates the greatest function in any cryptosystem that uses the algorithm software that distributes the securities shared between two such as DES algorithms. The algorithm loans use different levels for encryption and recording and do not need to share the privacy of the two. Each one has to keep his privacy confidential. The first foundation of the asymmetric algorithm known as cryptosystems key features comes from the major exchange problem of the algorithms software

In 1976, Whitfield Diffie and Martin Hellman considered one way as an agent and the recipient did not have to share a secret. This is the first function on cryptosystem storage.

DNA cryptography, a new component of DNA's cryptography as information and computer operators with the help of the recovery process. It is a new feature that appears after the DNA's influence [5]. DNP cryptography is cautious because DNA storage capability, which is the toolbar of this site. One DNA rate is known to keep 1010 degrees. This will exceed the capacity of any electrical, optical or medium-sized storage [5], [6]. Former urban systems that have been anchored and built on a powerful mathematical basis and process. Traditional security methods such as RSA, DES or NTRUs are also found in real time. Therefore, we need to note that DNA propaganda is not to stop the rule, but to create a way between existing devices and new technologies.

The clear difference between the traditional and DNA based cryptography that is specified in the table 1.

Characteristics	Traditional Cryptography	DNA cryptography
Security	Less	More
Time	Minutes to hours	Hours to days
Storage capacity	In MB	In TB
Dependency	On Implementation environment	On environmental condition

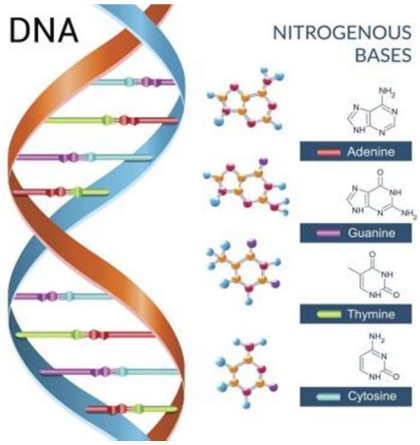
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

II. LITERATURE SURVEY

A. Universe of Cryptosystem

Different techniques have been used to preserve the information on the system. Survival is a model of conversion on the first message into an incoherent code, which can not be changed to the first message. Photo design is an important feature of compliant information in three levels of CIA set of three (Coalition, Stability, and Availability). CIA is a very important concept.

B. Why DNA Cryptography?



DNA cryptography is one of the fastest growing innovations in the DNA concept. Another way for safe information is presented using the organic method called DNA computing (otherwise known as atomic processing or physical amplitude). Leonard Max Adleman arrested you in 1994, caring for issues that are sure, for example, Hamilton's recommendation, NP-concluded as Traveling Salesman. Adleman is called 'An' in the form of RSA - estimating that some responses are going to the truth for today's exceptions sent on the web. The step later on different vendors for sensitivity and reduces the size of the information force that informs information on system and secrecy.

C. Advantages

1) Speed – Conventional PCs can perform around 100 MIPS (a huge number of direction every second). Consolidating DNA strands as exhibited by Adleman, made calculations proportionate to 10^9 or better, seemingly more than 100 times speedier than the quickest PC.

2) Minimal Storage Requirements – DNA stores memory at a thickness of around 1 bit for every cubic nanometer where traditional capacity media requires 10^12 cubic nanometers to store 1 bit.

3) Minimal Power Requirements – There is no power required for DNA processing while the calculation is occurring. The concoction bonds that are the building squares of DNA occur with no outside power source. There is no correlation with the power necessities of traditional PCs.

Customary cryptography and its security depends on troublesome mathematic issues which are develop both in principle and acknowledgment. Both the mystery key and open key strategies for cryptology have novel blemishes. The keys utilized as a part of present day cryptography are so extensive, actually, that a billion PCs working in conjunction with each handling a billion estimations for each second would even now take a trillion years to conclusively split a key. This isn't an issue now, yet it soon will be, given the development of the figuring force and advancements.

Various DNA crypto calculations has been inquired about and distributed like the Symmetric and Asymmetric Key crypto System utilizing DNA, DNA Steganography Systems, Triple stage DNA Cryptography, Encryption calculation motivated by DNA and Chaotic figuring. Cryptographic procedure in which each letter of the letter set is changed over into an alternate mix of the four bases that make up the human deoxyribonucleic corrosive (DNA).

Indeed, even today, individuals are not so much beyond any doubt what they expect a decent encryption component framework to do. A straightforward system of transmitting two related messages by concealing the message isn't sufficient to keep an assailant from breaking the code.

Customary Cryptography can be followed back to Caesar Cipher 2000 years prior or significantly prior. With time, it has advanced to give a to a great degree high computational security. Be that as it may, a foe with unbounded figuring force can break them hypothetically. Then again DNA Cryptography can have unique preferred standpoint for secure information stockpiling, validation, computerized marks, steganography, et cetera. DNA can likewise be utilized for delivering recognizable proof cards, and tickets. The following is an Image Encryption utilizing Chaotic Maps and DNA expansion.

Numerous investigation has been completed on assortment of bimolecular techniques for encoding and unscrambling information that is put away as a DNA. Despite the fact that DNA Cryptography is in its early stages. Just over the most recent couple of years has work in DNA registering seen genuine improvement. DNA cryptography is even less very much examined, yet increase work in cryptography in the course of recent years has laid great basis for applying DNA techniques to cryptography and steganography. Various plans have been suggested that offer some level of DNA cryptography, and are being investigated. At introduce, work in DNA cryptography is focused on utilizing DNA successions to encode paired information in some shape or another. In spite of the fact that the field is to a great degree unpredictable and current work is still in the formative stages, there is a considerable measure of expectation that DNA registering will go about as a decent strategy for Information Security.

III. RELATED WORK

Cryptography systems of DNA based-

A. Plaintext text message has transformed the DNA code by using known (known) shortcomings of alphabialcleotide.
B. Depending on the encryption process and the process of recording.
C. DNA provides additional media, and the minimum amount of DNA available for even encoding content and decryption.
D. There are each systematic setting: The origin of the event, good pictures XOR software that uses microphone and reference, key words.

IV. DNA COMPUTATION

Today, different techniques are used to calculate DNA. Researchers use these tips for performing functions on the DNA material Biocomputing is a stylish design that has an overview application to illustrate protected algorithm by using the reading function of bimolecular-based techniques in addition to traditional techniques. The bimolecular displacement procedures have originally been introduced to the new category of cryptography, DNA cryptography such as the evolution of the DNA and the biological orientation of the molecules. DNA, Deoxyribonucleic acid is the double helix of nucleotides with each nucleotide having one of four A, G, C, T wherein A is waiting for adenine, G for guanine, C for serum and T for refining

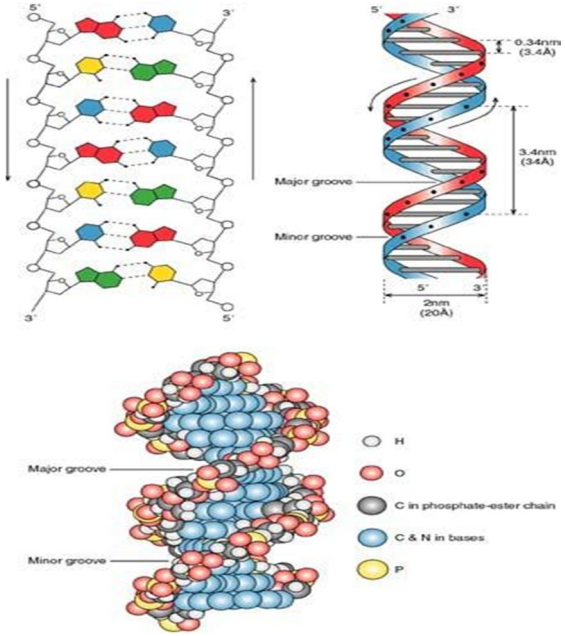


Figure 1: Helical structure of DNA

Figure 1 is the helical structure of DNA, which depicts nitrogenous bases, sugar phosphate backbone and base pair bonding [21]. Figure 2 represents the structure of

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

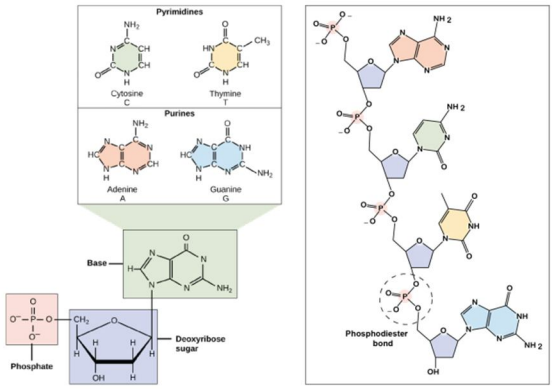


Figure 2: Structure of DNA base pairs

A. DNA Base Pairs And The Bonding Between Adenine

And thymine, cytosine and guanine [19]. In eukaryotic genes, the coding regions referred as exons and no coding regions are introns and the exons are interrupted by introns. Figure3 shows coding and non coding regions in a segment of eukaryotic DNA

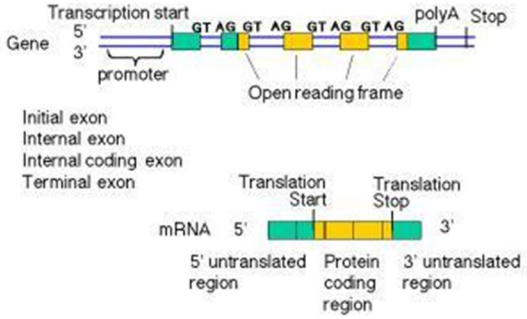


Figure 3: Structure coding region in a segment of eukaryotic DNA

V. DNA ENCRYPTION FOR SECURITY

Computational properties of DNA became a new branch of science and a research area for cryptographers from 1994 when Dr. Leonard M. Adleman used the computational properties of DNA to solve Hamiltonian path problem [1]. Research on DNA based encryption techniques can be broadly classified into three:

A. DNA Cryptography;
B. DNA Steganography;
C. Pseudo DNA Cryptography.

DNA Cryptography is built on DNA based computations for encryption and various methodologies for both
Symmetric and Asymmetric DNA cryptography has been proposed by researchers. The techniques based on bio-computations got wide acceptance due to secure nature of algorithms.
DNA digital coding technology denotes the bases A, C, T, G as 00, 01, 10,11 and the binary values can be interchanged with bases and this coding forms the basis of algorithms using Digital DNA [16]. DNA computing can be performed in two ways one by the means of biological operations using real DNA and the other technique involves simulation using Digital DNA and Pseudo DNA.DNA based encryption for data stored in the cloud will be a combination of trending techniques which ensures data security, Confidentiality, integrity and authentication are considered as most important aspects of information security whereas context is also an important aspect depending on it, the level required for data security will be different. Cryptographic techniques have a major role in securing data and depending on the context divergent encryption techniques can be used. The encryption techniques are broadly classified as symmetric key cryptography and asymmetric key cryptography depending on the context it can be used in conjunction with DNA Computing.

VI. HIDING THE DATA

Boris Shimanovsky at (2003) proposed the original DNA and RNA databases. The first is the simple way to store data in non-coding DNA such as non-open and non-converted genes and DNA-genes such as DNA computer solutions. Other procedures can be used to transfer data into active encoding levels without changing the amino acid conversion. Monica Borda et al (2010) introduced molecular calculations (BMC) and many algorithms for DNA (deoxyribonucleic acid) steganography and cryptography: A-Time-Pad (OTP), DNA XOR OTP and DNA chromosomes. Hayam Mousa is designed to designate a storage solution that has a DNA-based conversion based on variant imaging. The program uses two formats of formats with a variant difference that varies to correct correction.

Each DNA has been split between the user and the recipient. This only DNA reference can be downloaded from the EBI or NCBI databases but you can also select from any data storage. Therefore, by analyzing any such data storage, there are 163 million targets to choose. Shortly, the attractive DNA approach that steals by trackers is reliable.

VII. DATA INTEGRITY

The proposed system can be used as a client-side encryption. To ensure th integrity of the data the user can generate a hash of the encrypted data and store it in a local repository. After retrieving data from the cloud each time user can compute the hash of data and can be compare with the hash value stored in the local hash repository to ensure data integrity.

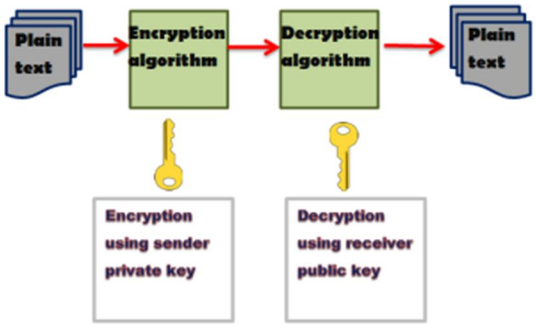


Fig 4: Sequence diagram for data integrity check

The proposed technique is feasible and easy to use and ensures the data integrity using hashing technique. Figure 4 is depicting the sequence diagram of the proposed system for data integrity check.

VIII. RESULTS

The implementation results are obtained both on decryption and encryption Command Window and GUI. The screenshot of Graphical User Interface of the implemented algorithm in DNA crypto is as follows:

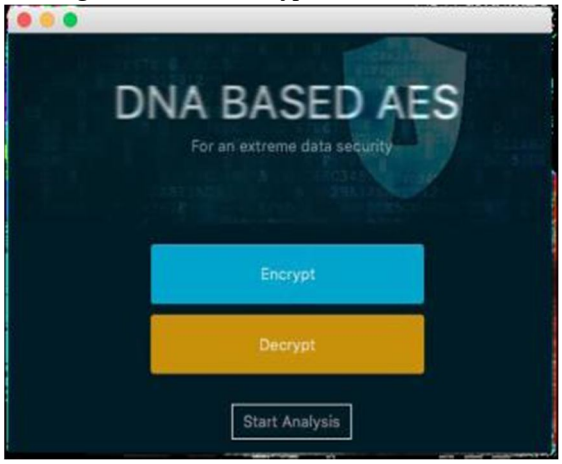


Figure 5:Screen Layout of Main Page

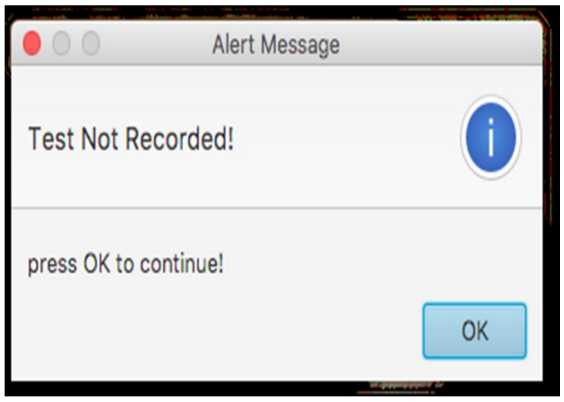


Figure 6: Screen Layout of Alert message on clicking encrypt/decrypt

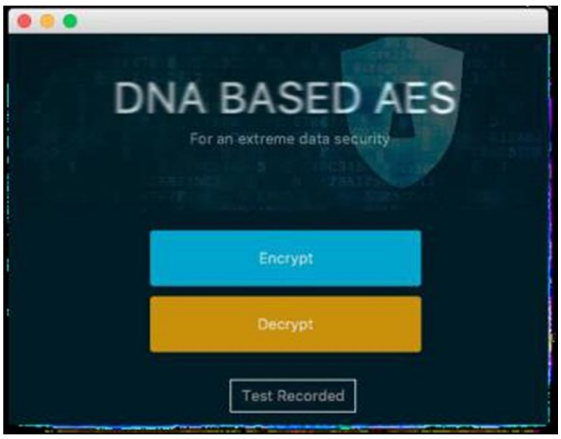


Figure 7: Screen Layout main scene after clicking start analysis button

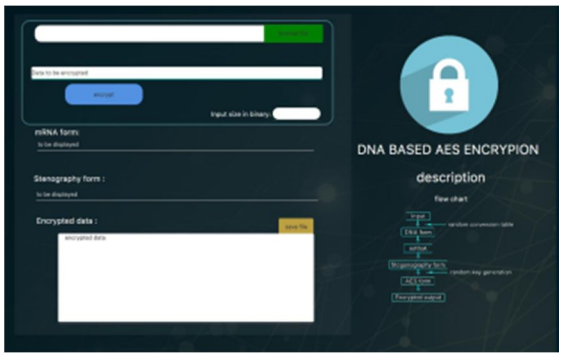


Figure 8: Screen Layout of Encryption screen

Figure 9: Screen Layout of browse file button /File Chooser

Figure 10: Screen Layout after a file is opened

Figure 11: Screen Layout after successful Encryption

Figure 12: Screen Layout of message after save file

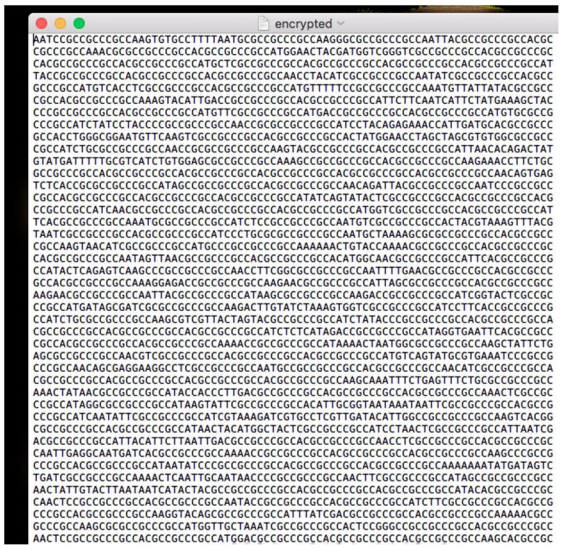


Figure 13: A sample saved file(encrypted.txt)

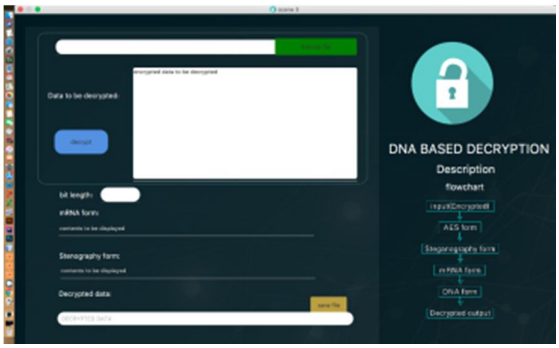


Figure 14: Screen Layout of Decryption screen

Figure 15: Screen Layout of browse file button /File Chooser

Figure 16: Screen Layout after a file is opened

Figure 17: Screen Layout after successful Decryption

Figure 18: Screen Layout of message after save file

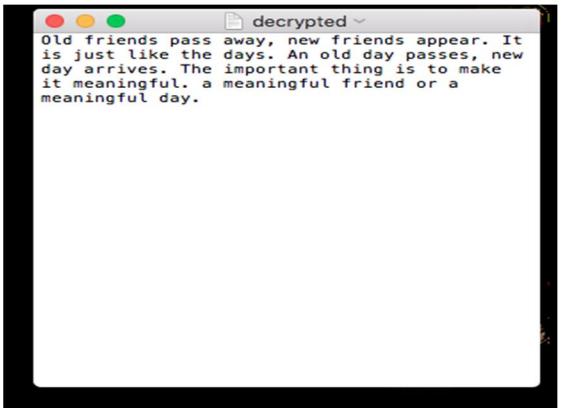


Figure 19: A sample saved file(encrypted.txt)

IX. CONCLUSIONS

In this template, the DNA encryption process is created for secure data storage in the cloud even in the cloudy cloud where data storage is a major problem and for SaaS customers where security is a major problem. The procedure will provide enhanced care that adds reading activity using bio computing techniques in addition to Cryptography and user can check the accuracy of data without a third party. The difference between traditional and DNA patterns reflects the importance of DNA. The results of the previous work illustrate the area of knowledge that exists in the field of cryptography DNA. In the future an algorithm can be designed for steganography cascaded stenography and cryptography

X. FUTURE WORK

The DNA cryptography designed is a community-based recording system for a secure storage of data around the cloud, the way is generally universal, but the use of DNA cryptography for the cloud has the special significance of the important observation of the storage Cloud at Work and day to day. "Here all data is bomb in pictures, videos and other templates. Therefore, baseline for storage is very important and DNA intensive is an overview of the future security perspective.

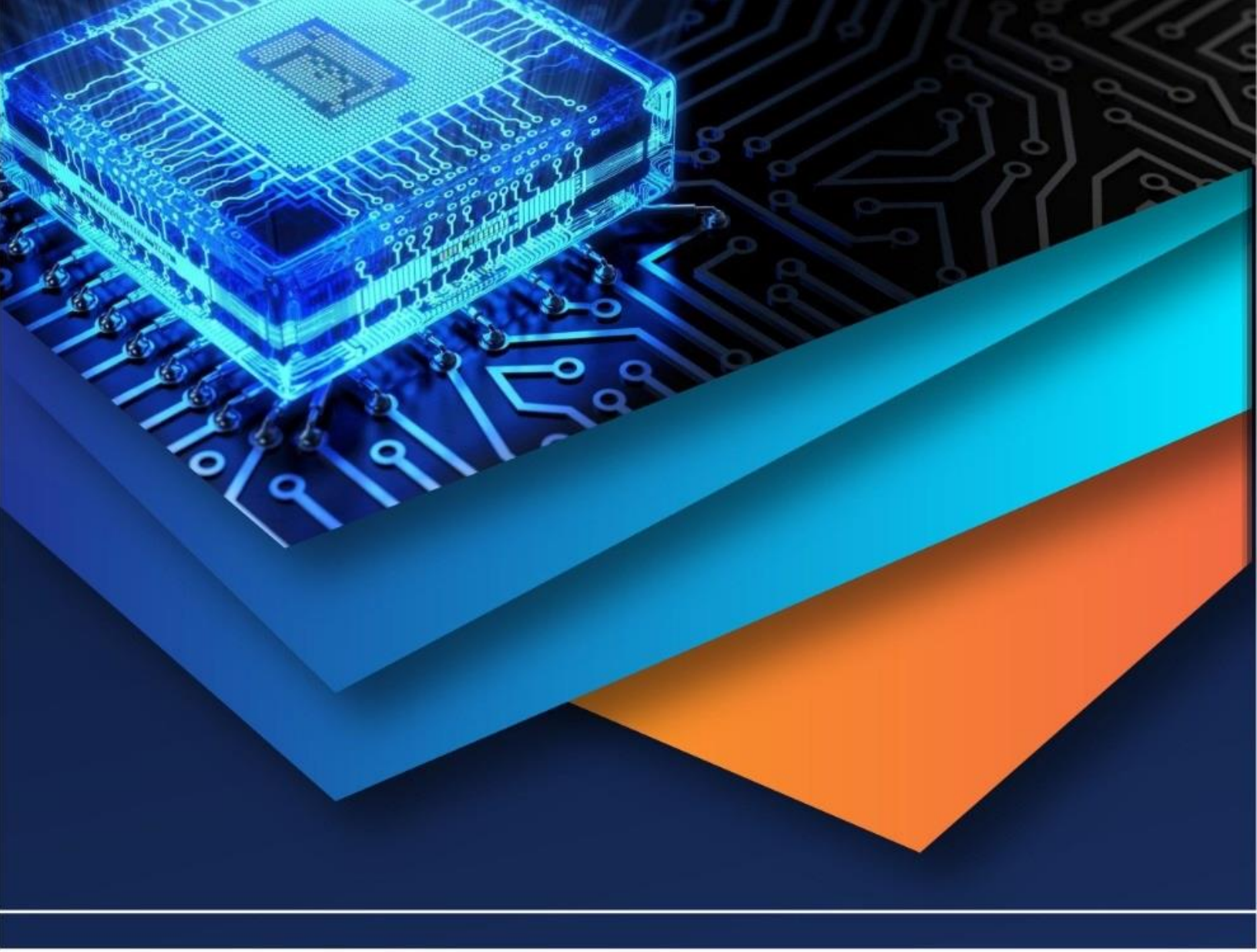
XI. ACKNOWLEDGEMENT

We owe our deep gratitude to our project guide Vandana CP, who took keen interest on our paper work and guided us all along, till the completion of this paper by providing all the necessary information for developing a good manuscript.

REFERENCES

[1] L. M. Adleman, \Molecular computation of solutions to combinatorial problems," Nature, vol. 369, pp. 40, 1994.
[2] E. S. Babu, C. N. Raju, and M. H. K. Prasad, \In- spired pseudo biotic DNA based cryptographic mech- anism against adaptive cryptographic attacks," In- ternational Journal of Network Security, vol. 18, no.2, pp. 291-303, 2016.
[3] R. Bhadauria and S. Sanyal, \Survey on security is- sues in cloud computing and associated mitigation techniques," arXiv preprint arXiv:1204.0764, 2012.
[4] K. Brindha and N. Jeyanthi, \Securing portable doc- ument format _le using extended visual cryptogra- phy to protect cloud data storage," International Journal of Network Security, vol. 19, no. 5, pp. 684- 693, 2017.
[5] Borda, M., &Tornea, O. (2010, June). DNA Secret Writing Techniques.In IEEE conferences
[6] Mousa, H., Moustafa, K., Abdel-Wahed, W., &Hadhoud, M. M. (2011). Data hiding based on contrast mapping using DNA medium. Int. Arab J. Inf. Technol., Volume- 8 Issue (2), pp 147-154.

[7] Taur, J. S., Lin, H. Y., Lee, H. L., & Tao, C. W. (2012). Data Hiding In DNA Sequences Based On Table LookUp Substitution. International Journal of Innovative Computing, Information and Control, Volume 8 Issue (10).
[8] Torkaman, M. R. N., Kazazi, N. S., &Rouddini, A. (2012). Innovative approach to improve hybrid cryptography by using DNA steganography.International Journal of New Computer Architectures and their Applications (IJNCAA), Volume-2 Issue (1), pp. 224- 235.
[9] X. Li, C. Zhou, N. Xu, \A secure and e_cientim-age encryption algorithm based on DNA coding and spatiotemporal chaos," International Journal of Net- work Security, vol. 20, no. 1, pp. 110-120, 2018.
[10] Jacob, G., &Murugan, A. (2013). DNA based Cryptography: An Overview and Analysis. International Journal of Emerging Sciences, Volume 3 Issue (1), pp.36-27.
[11] Bhattacharyya, D., &Bandyopadhyay, S. K. (2013) Hiding Secret Data in DNA Sequence. International Journal of Scientific &Engineering Research Volume 4.
[12] Mitras, B. A., &Aboo, A. K. (2012). Proposed Steganography Approach Using Dna Properties. International Journal of Information Technology and Business Management, Volume-14 Issue 1.
[13] Yamuna, M., Dangi, M. K., & Singh, K. (2013). Encryption of a Binary String Using DNA Sequence.International Journal of Computer Science, Volume 2, Issue (02).
[14] H. Lodish, A. Berk, P. Matsudaira, C. A. Kaiser, M. Krieger, M. P. Scott, S. L. Zipursky, and J. Darnell “Molecular Cell Biology”, 5th ed. New York: W. H. Freeman and Co. 2003.
[15] G. Cui, L. Qin, Y. Wang, and X.Zhang, “An encryption scheme using DNA technology,” in IEEE 3rd International conference on Bio-Inspired Computing: Theories and Applications (BICTA08), Adelaid, SA, Australia, pp. 37–42, 2008



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY