International Journal of Science and Engineering Applications
Volume 14-Issue 08, 10 – 15, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1408.1003

Securing Cloud Data with DNA and RNA-Based Cryptographic Algorithms: A Python Implementation

Md. Irfan Alam
Associate Professor
Department of CSE & IT
Jharkhand Rai University
Ranchi, Jharkhand, India

Kailash Pati Dutta
Associate Professor
Department of CSE & IT
Jharkhand Rai University
Ranchi, Jharkhand, India

Shivangini Bihari
Assistant Professor
Department of CSE & IT
Jharkhand Rai University
Ranchi, Jharkhand, India

Abstract: Cloud computing represents a transformative advancement in modern technology. However, as it evolves, so do the security threats faced by users. This has made safeguarding data during storage and transmission a growing concern. Traditional cryptographic methods are increasingly susceptible to sophisticated attacks, prompting the exploration of alternative techniques. One promising direction is the use of DNA and RNA-based cryptography, which offers the potential for highly secure encryption. Numerous researchers worldwide have proposed methods to enhance cloud data protection. In this study, a novel encryption algorithm is introduced that merges arithmetic operations with biological concepts. It employs biological mechanisms to generate symmetric keys by converting DNA sequences into RNA sequences. Encryption is achieved through XOR operations, integrating biological principles into digital computing. This approach leverages the natural efficiency of biological systems—particularly their capabilities in parallel processing and dense data storage—which remain underutilized in conventional computational methods**.**

Keywords: Cloud Computing, Cloud Security, DNA-based cryptography, RNA, XOR Operation, Biological Operations

1. INTRODUCTION

Cloud computing is a domain of computing in which information in the form of text, images, and videos is stored remotely on hosted servers, rather than on a local machine or computer. There has been a tremendous increase in the number and types of attacks that must be addressed by information security experts to protect sensitive data from unauthorized disclosure or undetected alteration during transmission or while in storage [1]. Over time, various technologies have been explored for securing data through cryptography, which requires a strong understanding of physics or mathematics [2]. The concept of cloud computing has existed since the late 1970s in the form of distributed computing, but it was popularized by Amazon.com in 2006. Today, cloud computing is one of the most widely used computing technologies.

1.1 Motivation

Cloud storage service offers tremendous benefits to customers. In spite of these benefits, the concern over security and privacy linked with cloud model seem to be the major obstacle in adopting cloud by the individuals and organizations. First problem is, since the data resides on third party's premises, data owners lose control over their outsourced data. Second problem is data owners need to take high risk in trusting cloud service provider on all circumstances. Finally, the multi-tenancy nature of cloud brings in several malicious internal and external attacks. Lack of data security in cloud environment poses major challenges to data owners. The motivation of this research work is to seek cloud data security concerns and proposes secure and efficient protocols for security in cloud environment to preserve confidentiality, authorized access to stored data, authenticity and integrity of data from the perspective of data owners.

1.2 Contributions of the Paper

The main contribution of this paper is to design and implement Cloud Security based on DNA and RNA Cryptographic Algorithm for the data outsourced to cloud data storage that preserves data confidentiality, authenticity and integrity from the view of data owner. The key aim of this work is to provide model for data security [19, 20]. This model is intended in such a way to resist vulnerabilities and threats that put at risk the data being transferred through an open communication medium. This could be achieving with the strong cryptographic schemes with strong key generation method.

2. Cryptography

Cryptography is a technique of coding/decoding data so that it becomes unreadable or not accessible by unauthorized users, which is often used to protect data during their transmission or in storage [3]. Cryptography is specialized in building, analyzing and building protocols that resist the influence of enemies and which are connected to various aspects in information security such as data confidentiality, authentication, non-repudiation and data integrity [4]. Information security experts found that binary computers (digital computers) have various kinds of physical constraints, especially in computation processes and data storage so they focused on DNA-RNA computers (bimolecular computers) and quantum computers [5]. DNA computing is a current field which is growing in the modern days and it is providing a new data structure and evaluating techniques for the parallel processing capabilities of molecules. The path of DNA cryptography taking place with the growth of DNA computing [21]. DNA computing was discovered by Dr. Leonard M. Adleman for solving complex computational problem in 1994[6]. In this paper, DNA-RNA and its components and sequence are explained; also DNA-RNA cryptography is explained and implemented in Python. The biological operations on this, has been explained and used in the proposed algorithm. The Key generation, encryption and decryption in the proposed algorithm has been explained and implemented. Cryptography is time taking and require intensively complex processing but yet maintaining the security as maximum as possible. To make DNA-RNA based Cryptography, a more reliable and fast medium to implement security, the Symmetric Cryptography Technique is used. There are various Cryptography implementing techniques but the core thing among all is that the degree of uncertainty and randomness in the process of generation of Secret Key.

2.1 DNA Structure

DNA is a biological molecule term, stands for Deoxyribo Nucleic Acid, which is the basic building block of the human body which represents the genetic blueprint of living creatures. DNA is unique for each and is a collection of the complex organic molecules. There is DNA in every cell of the organism which is important for the identity of any living being [7,8]. DNA is a sequence of nucleotides; these sequences of the nucleotides give the code of each gene. DNA sequences represent biological information such as skin color, weight, nose shape, eye, and hair as well as other features [8]. In 1953, James Watson formed the first 3D structure of DNA which depends on an X-Ray print. Most DNA molecules consist of two biopolymer strands coiled around each other to form a double helix / stranded like a spiral ladder [9]. The two DNA strands are known as polynucleotide's, since they are composed of same units called nucleotides. Each nucleotide is composed of nucleobase which is Guanine (G), Adenine (A), Thymine (T) or Cytosine (C) as well as a phosphate group and a monosaccharide sugar called deoxyribose [4]. In DNA , there is a base rule which decide that Guanine pairs with Cytosine and forms three hydrogen bonds, Adenine pairs with Thymine and forms a two hydrogen bonds [4]. Complementary theory of Watson-Crick is basically called the base pairing rule. DNA sequence has two strands, an individual strand as single stranded DNA (ssDNA) and double stranded DNA (dsDNA) [10-11]. There is a way called Hybridization that contains two strands ssDNA, which are anti-parallel to each other, and form dsDNA. The two ssDNA in dsDNA must be complementarily. This makes DNA a single data structure for computation and can be used in many places [7]. In DNA strands there is directionality where one end of a DNA polymer has an exposed hydroxyl group on the deoxyribose; this is known as the 3' end of the molecule. The other end has an exposed phosphate group; this is the 5' end. Directionality of DNA is vitally important to many cellular processes, since double helices are necessarily directional [9]. DNA computing has lot of advantages on the silicon machines. These advantages mainly include speed of computation, size, and high parallelism. One gram of DNA has 1021 DNA bases which can store up to 108 Terabytes of data. It exceeds the capacity of traditional storage media such as magnetic media, optical, electronic etc. Every molecule of DNA act as a single processor thus parallelism is achieved. Operations can thus be done in parallel, which increases the speed of computations. It is highly energy competent i.e., 1019 operations per Joule [5]. DNA Molecule is responsible for transmitting information among the cells. Proteins in DNA are used to interact with its environment. mRNA (messenger Ribonucleic Acid) present in DNA sends information. There are two ways that are involved in transmitting a message: i) Transcription ii) Translation. In Transcription, DNA moves its information to the mRNA. In Translation, mRNA uses the information to interact with proteins and moves on the desired message. DNA has the biological property where it replicates without losing the original DNA.

2.2 DNA Computing and DNA Cryptography

The area of DNA cryptography is an untouched one. Over the years, many initiatives have been suggested to explore the process of DNA cryptography, but very few have been implemented [5]. The cryptography and molecular biology are not relevant initially, but with study of modern biotechnology and DNA computing, the relation became more and more close. DNA information science and cryptography was discovered after research of DNA computing by Adleman. Many scholars have done a big number of studies on DNA cryptography [4]. The important development in the area of cryptography is the establishment of DNA computing on the traditional cryptographic [5]. At present, DNA cryptography is not more influential than traditional cryptography but it can give a hybrid security by adding the concept of DNA cryptography with traditional cryptography [9]. DNA cryptography depends on conventional cryptographic consists of key generation, encryption and decryption process [11]. During the last two decades, many DNA based algorithms have been developed and used for data cryptography and key generation [10]. DNA can be used in future in computing and cryptography by replacing silicon chip with bio-chips or DNA chips.

2.3 Biological Operations

DNA cryptography can make use of arithmetic operations, biological operations or both. Arithmetic operations are used to manipulate the data entered in the cryptography system. The examples of arithmetic operation are Addition, subtraction, complement, XOR, substitution, insertion, random number etc. The biological operations on DNA are applicable to solve computational and mathematical problem [5].

These operations are as follows:

A. Hybridization (Anneal): In this process single stranded DNA chain or sequence are combined with other single stranded DNA to form double stranded DNA, where they are complementary strands [11,12].

B. Transcription: Transcription is performed when two DNA strands in double stranded DNA are separated by an enzyme; the separation forms a single strand messenger RNA by mapping from DNA sequences. RNA consists of (U, A, G, C) while DNA strand which consist of (T, A, G, C). The transcription processes noncoding segments are called introns which are removed by splicing and the other remaining segments are called exons that encode information for protein, synthesis and assembled in mRNA [13]. RNA is a biological molecule term as Ribonucleic Acid, which contains the nucleotides, A, C, G, and U. DNA is different from RNA in the nucleotides where Thymine (T) nucleotide in DNA is replaced by Uracil (U) nucleotide in RNA. RNA is basically two types, the mRNA (Messenger Ribonucleic Acid) and tRNA (Transfer Ribonucleic Acid). In this paper we used mRNA type [14] Structure of RNA [15]. The simple concept of transcription where Thymine in DNA get replaced by Uracil to form mRNA [15,16].

C. Translation: Central Dogma of Molecular Biology is an operation of converting DNA molecules into protein sequence. Genetic code is made up of three letter codes and called codons, where DNA and RNA have these codons. To convert DNA to protein we have two stages Transcription and Translation. First stage transcription is as mentioned in previous section, which convert DNA molecules to mRNA. Second stage is translation which converts mRNA sequence to protein form [14]. Only one strand of DNA is copied. A single gene may be transcribed number of times. After transcription, the DNA strands re-join and form amino acids and subsequently form the protein.

DNA Computing is the field of computing bringing together the Computer Science, Biological Science and Molecular Science to understand and solve some primary NP problem [16, 17]. Initially it was introduced by Leonard Max Adleman but now it has evolved as one of the most fascinating platform to do something new by teachings of Mother Nature. It is the best example of Bimolecular Computing. Bimolecular

Computers are those computers where all the computing components are made up of Molecular Compounds meansall Software/Hardware and Input/output are all in form of a Molecular Compound. DNA Computing has various steps like Melting, Annealing, Merging, Amplification and Selection. DNA actually behaves like a Turing Machine that is why it can be used as a Data Storage Device. Adleman has showed that DNA Computing can be used as an effective tool to solve the NP problems like Hamiltonian Graph Problem or Travelling Salesman Problem (TSP) [17, 18]. He showed that DNA Computing can be used to solve complex Combinatorial Problems like TSP and Finite State Problem. Here, the basic idea is that all the operations are performed over DNA (more precisely using DNA Bases or Nucleotide) not in DNA. DNA Computing can be classified as Intramolecular DNA Computing and Supramolecular DNA Computing. DNA Computers form a self-replicating system. In DNA Cryptography DNA Nucleotides is used to generate a set of Symmetric Cryptographic Key. For, DNA Cryptography, many Techniques has already been established in many researches[18,19]but here, I aimed to develop a Technique to make the existing Cloud-Based data storage security systems more accurate and giving the encrypting and decrypting capability directly to the Authorized Client on its own Machine. In this technique, first, we have to define three types of information. We need standard Library named as DNA Reference Sequence which includes the 4-Bit Base Sequence distinct for all 256 ASCII characters in random order which is shown in Table 1[20]. This DNA Reference Sequence encodes the Plain Text message into DNA Bases Sequence Text. Fourth table will replace the existing Genome DNA Base Sequence to other DNA Base Sequence [20]. Second table convert the DNA to RNA[20]. Third table we need is the Base-Binary Library that store the information about the equivalent conversion of RNA Base Sequence Message to a long binary string [20] .This Base-Binary Library is also not standardized as it can be defined by the user itself.

Table 1. Codon-to-Character Mapping

Code	Char	Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
TTTT	NUL	TTTC	Space	TTTG	@	TTTA	`	TTCT	Ç	TTCC	á
TTCG	└	TTCA	Ó	AAAG	■	AAAA	nbsp				
TTGT	SOH	TTGC	!	TTGG	A	TTGA	a	TTAT	ü	TTAC	í
TTAG	┴	TTAA	ß	TCTT	STX	TCTC	"	TCTG	B	TCTA	b
TCCT	é	TCCC	ó	TCCG	┬	TCCA	Ô	TCGT	ETX	TCGC	#
TCGG	C	TCGA	c	TCAT	â	TCAC	ú	TCAG	├	TCAA	Ò
TGTT	EOT	TGTC	$	TGTG	D	TGTA	DEL	TGCT	ä	TGCC	ñ
TGCG	─	TGCA	õ	TGGT	ENQ	TGGC	%	TGGG	E	TGGA	e
TGAT	à	TGAC	Ñ	TGAG	┼	TGAA	Õ	TATT	ACK	TATC	&
TATG	F	TATA	f	TACT	å	TACC	ª	TACG	ã	TACA	µ
TAGT	BEL	TAGC	'	TAGG	G	TAGA	g	TAAT	ç	TAAC	º
TAAG	Ã	TAAA	þ	CTTT	BS	CTTC	(	CTTG	H	CTTA	h
CTCT	ê	CTCC	¿	CTCG	╚	CTCA	Þ	CTGT	TAB	CTGC	)
CTGG	I	CTGA	i	CTAT	ë	CTAC	®	CTAG	╔	CTAA	Ú
CCTT	LF	CCTC	*	CCTG	J	CCTA	j	CCCT	è	CCCC	¬
CCCG	╩	CCCA	Û	CCGT	VT	CCGC	+	CCGG	K	CCGA	k
CCAT	ï	CCAC	½	CCAG	╦	CCAA	Ù	CGTT	FF	CGTC	,
CGTG	L	CGTA	l	CGCT	î	CGCC	¼	CGCG	╠	CGCA	ý
CGGT	CR	CGGC	-	CGGG	M	CGGA	m	CGAT	ì	CGAC	¡

CGAG	═	CGAA	Ý	CATT	SO	CATC	.	CATG	N	CATA	n
CACT	Ä	CACC	«	CACG	╬	CACA	¯	CAGT	SI	CAGC	/
CAGG	O	CAGA	o	CAAT	Å	CAAC	»	CAAG	¤	CAAA	´
GTTT	DLE	GTTC	0	GTTG	P	GTTA	p	GTCT	É	GTCC	░
GTCG	ð	GTCA		GTGT	DC1	GTGC	1	GTGG	Q	GTGA	q
GTAT	æ	GTAC	▒	GTAG	Ð	GTAA	±	GCTT	DC2	GCTC	2
GCTG	R	GCTA	r	GCCT	Æ	GCCC	▓	GCCG	Ê	GCCA	‗
GCGT	DC3	GCGC	3	GCGG	S	GCGA	s	GCAT	ô	GCAC	│
GCAG	Ë	GCAA	¾	GGTT	DC4	GGTC	4	GGTG	T	GGTA	t
GGCT	ö	GGCC	┤	GGCG	È	GGCA	¶	GGGT	NAK	GGGC	5
GGGG	U	GGGA	u	GGAT	ò	GGAC	Á	GGAG	ı	GGAA	§
GATT	SYN	GATC	6	GATG	V	GATA	v	GACT	û	GACC	Â
GACG	Í	GACA	÷	GAGT	ETB	GAGC	7	GAGG	W	GAGA	w
GAAT	ù	GAAC	À	GAAG	Î	GAAA	¸	ATTT	CAN	ATTC	8
ATTG	X	ATTA	x	ATCT	ÿ	ATCC	©	ATCG	Ï	ATCA	°
ATGT	EM	ATGC	9	ATGG	Y	ATGA	y	ATAT	Ö	ATAC	╣
ATAG	┘	ATAA	¨	ACTT	SUB	ACTC	:	ACTG	Z	ACTA	z

Table 2: DNA Base Sequence to RNA Base Sequence

DNA Base	RNA Base
A	A
T	U
G	G
C	C

Table 3:RNA Base to Binary Number

RNA Base	Binary Value
A	00
U	01
G	10
C	11

Table 4: DNA Base to Other DNA Base

DNA Base	Other DNA Base
A	T
T	A
G	G
C	C

3. Proposed Algorithm

Aim of this proposed algorithm is to provided client end cryptography using DNA and RNA. Important feature of this algorithm is that the data getting stored or data under transmission if even get hacked or intruded, that data will be of no use for the middle man even to that data administrator of the cloud storage facility.

Algorithm 1: Proposed DNA-based Key Generation

Input: Random character passed through table 1, table 2 and table 4.
Output: Final Key generated
Step1: Let Message be: K1='A'
Step 2: K1 is encoded as: K2=TTGG (Using table 1)
Step 3: K2 is encoded as: K3=AACC (Using table 4)
Step 4: K3 is encoded as: K4=AACC (Using table 2)

Algorithm 2: Proposed DNA-based Encryption

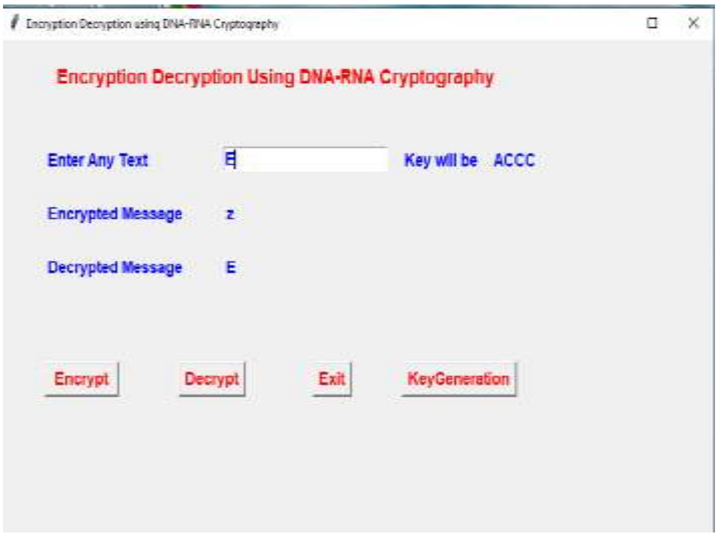
Input: Any plain text
Output: Cipher Text
Step1: Let Message be: E1 = "A"
Step 2: E1 can be encoding as: E2=ASCII (M1)
E2 = 65.
Step 3: Message E2 can be encoded as: E3=BINARY (E2)
E3 = 01000001
Step 4: Perform XOR operation on E3 and binary value of K4; we got the cipher text in binary form
C1 = XOR (E3, binary (K4)) (for binary conversion of K4, table3 is used) .
Step 5: Convert the cipher text C1 to its corresponding decimal number which will be like the ASCII number
C2=decimal (C1)
i.e. C2=78

Step 6: Convert the cipher text C2 to its corresponding character
C3=character (C2) i.e. C3=N

Send this data, C3 to the Cloud Server.

Algorithm 3: Proposed DNA-based Decryption
Input: Cipher text
Output: Original plain Text
Step1: Download the file from the Cloud Server i.e.C3
Step 2: Perform XOR operation on binary of K4 and binary of ASCII of cipher text C3,
we got the original message
M=XOR (binary of (K4), binary (ASCII (C3)).

4. Implementation of Algorithm in Python



Encryption Decryption Using DNA-RNA Cryptography

Enter Any Text E

Key will be ACCC

Encrypted Message z

Decrypted Message E

5. Complexity Analysis of Algorithm

The proposed DNA algorithm has a time complexity of O (n^2) for the encryption process, where "n" represents the number of operational data points, and the key size is 32 bits. The key generation algorithm, on the other hand, has a time complexity of O (1). Similarly, the decryption algorithm also has a time complexity of O (n^2). Thus, it can be concluded that the proposed approaches are computationally efficient and feasible.

6. Conclusion

This paper proposes a DNA-RNA-based encryption technique for securing data stored in the cloud, particularly in public cloud environments and for SAAS users where security is a critical concern. The technique will provide improved security as it includes the computational complexity by using bio-computing techniques in addition to Cryptography. User can check the integrity of the data without relying on the third party. The proposed DNA-RNA Cryptography is an encryption technique for secure storage of data in the cloud environment, using DNA-RNA cryptography for cloud has great scope considering the importance of cloud storage in the industries and day to day life. Everywhere data are present in the form of video, image and other digital forms. Storage platforms are crucial, and DNA-RNA encryption is an emerging concept that will dominate the future of security. The proposed DNA-RNA cryptographic method uses a dynamic Character-DNA succession table, a DNA Base to equivalent DNA Base table, and a DNA Base-Binary table to enhance data security. This algorithm is implemented using Python. Many cryptanalysts have suggested that the future of cryptography lies in multidisciplinary studies combining various aspects of science and mathematics.

References

1. Zhang, M., Cheng, M. X., & Tarn, T. J. (2006). A mathematical formulation of DNA computation. *IEEE Transactions on NanoBioscience*, *5*(1), 32–40. https://doi.org/10.1109/TNB.2006.872025
2. Leuenberger, M. N., & Loss, D. (2001). Quantum computing in molecular magnets. *Nature, 410*, 789–793. https://doi.org/10.1038/35071024
3. Saxena, P., Singh, A., & Lalwani, S. (2013). Use of DNA for computation, storage and cryptography of information. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), 3*(2).
4. Varma, P. S., & Raju, K. G. (2014). Cryptography based on DNA using random key generation scheme. *International Journal of Science Engineering and Advance Technology (IJSEAT), 2*(7).
5. Ouseph, N. (2016). A survey on diverse DNA cryptographic techniques. *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), 4*(9).
6. Adleman, L. (1994). Molecular computation of solutions to combinatorial problems. *Science, 266*, 1021–1024. https://doi.org/10.1126/science.7973651
7. Dhawan, S., & Saini, A. (2012). Secure data transmission techniques based on DNA cryptography. *International Journal of Emerging Technologies in Computational and Applied Sciences*, 95–100.
8. Kartalopoulos, S. V. (2005). DNA-Inspired cryptographic method in optical communications, authentication and data mimicking. *MILCOM 2005 - IEEE Military Communications Conference*, *2*, 774–779. https://doi.org/10.1109/MILCOM.2005.1605822
9. Jeevidha, S., Saleem Basha, M. S., & Dhavachelvan, P. (2011). Analysis on DNA based cryptography to secure data transmission. *International Journal of Computer Applications (IJCA)*, *29*(8).
10. Anwar, T., Paul, S., & Singh, S. K. (2014). Message transmission based on DNA cryptography: Review. *International Journal of Bio-Science and Bio-Technology*, *6*(5), 30.
11. Anwar, T., Kumar, A., & Paul, S. (2015). DNA cryptography based on symmetric key exchange. *International Journal of Engineering and Technology (IJET)*, *7*(3), June–July.
12. Karimi, M., & Haider, W. (2017). Cryptography using DNA nucleotides. *International Journal of Computer Applications*, *168*(7).

13. Lloyd, S., & Snell, Q. O. (2008). Sequence alignment with traceback on reconfigurable hardware. *2008 International Conference on Reconfigurable Computing and FPGAs*, 259–264. https://doi.org/10.1109/ReConFig.2008.50
14. Krishna, B. M., Khan, H., Madhumati, G. L., Kumar, K. P., Tejaswini, G., Srikanth, M., & Ravali, P. (2017). FPGA implementation of DES algorithm using DNA cryptography. *Journal of Theoretical and Applied Information Technology, 95*(10), 31 May.
15. Mandge, T., & Choudhary, V. (2012). A review on emerging cryptography technique: DNA cryptography. *International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS)*.
16. Adleman, L. (1994). Sub-atomic calculation of arrangements of combinatorial issues. *Science, 266*, 1021–1024. https://doi.org/10.1126/science.7973651
17. Nimje, A. R. (2012). Cryptography in cloud-security using DNA (genetic) techniques. *International Journal of Engineering Research and Applications (IJERA), 2*(5), 1358–1359.
18. Rahman, N. H. U., Balamurugan, C., & Mariappan, R. (2015). A novel DNA computing based encryption and decryption algorithm. *International Conference on Information and Communication Technologies*.
19. Jain, A., & Rajpal, N. (2013). Adaptive key length based encryption algorithm utilizing DNA approach. *International Conference on Machine Intelligence Research and Advancement*.
20. Irfan Alam, M., & Singh, S. N. (2021). Designing and Implementing Cloud Security Using Multi-layer DNA Cryptography in Python. *Trends in Wireless Communication and Information Security: Proceedings of EWCIS 2020*, 375-385.
21. Alam, I. (2020). Enhancing cloud security using multi-Level dna cryptography. *Splint International Journal of Professionals*, *7*(1), 75-82.