INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN: 2455-0620 [Impact Factor: 6.719]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 8, Issue - 7, JULY - 2022 Publication Date: 31/07/2022

DOIs:10.2015/IJIRMF/202207004 --:-- Research Article

A NOVEL CLOUD COMPUTING DATA PROTECTION METHOD BASED ON GENETICS APPROACH AND LOGICAL MATHEMATICAL FUNCTIONALITIES

[1]Dr. Rajeev Kumar Tripathi, [2]Dr. Alok Mishra, [3]Dr. Pankaj Prajapati
[1]Professor, DAV Degree College, Lucknow, India
[2]Associtae Professor, Ambalika Institute Of Professional Studies,India
[3]Associtae Professor, Ambalika Institute Of Professional Studies,India
Email - [1]rajeevtripathi@gmail.com, [2]dralokmishra72@gmail.com, [3]assocdean1@ambalika.co.in

Abstract: *Cloud computing is an essential part of the IT sector because it allows customers to access services from anywhere on earth. Because the need for and reputation of cloud computing grows, so does the number of threats and vulnerabilities. Facts integrity and privateness are crucial concerns in cloud computing, and they need to be taken into consideration due to the fact facts is stored in a couple of locations. As a end result, the maximum important causes of users' worries about the cloud computing surroundings are statistics integrity and privateness safety safeguards. The maximum vital method for statistics protection is encryption. As a result, an expansion of encryption strategies are utilized to offer protection, integrity, and authorised get right of entry to using a diffusion of mechanisms, together with DNA. They do, but, have some limits. This study's investigation revealed cloud data protection troubles, cloud assaults, and found vulnerabilities for plenty factors affecting cloud computing. The goal of this evaluation is to study the numerous additives of cloud computing in addition to present day massive protection and security challenges. Further, this text discussed an expansion of protection worries, in addition to a few novel security concepts and mitigation techniques, in addition to destiny instructions.*

The effects of the experiment improved facts security, which can be utilised to shield cloud computing applications. The testing findings of the counseled set of rules confirmed a excessive level of security, in addition to an obvious boom in cipher size and execution time whilst in comparison to existing cloud computing answers.

Key Words: *Cloud computing, Data security, DNA, Logical-mathematical functions.*

1. INTRODUCTION :

Since the twenty-first century has been dubbed the "generation era," online transactions, e-trade, and e-commercial enterprise have all relied on the reliability and accuracy with which records is transferred across the network. Data go with the flow has historically encountered issues which includes facts tampering, degradation, loss, and publicity to unauthorised people. Despite the fact that the computing world has excelled at managing cloud computing offerings, the cloud computing surroundings does offer sizable risks and risks. There are various techniques for enhancing the security of cloud computing, such as cryptography, that's the number one component of facts safety inside the cloud. It is a method of transforming the sender's letter right into a mystery word referred to as the ciphertext, wherein only the supposed recipient may additionally find out the hid message[1]. Cloud computing has given facts technology (IT) a brand new path, with abilties such as resource sharing, multi-tenancy, and faraway statistics sharing distinguishing it from a conventional computing surroundings. Cloud computing's essential intention is to deliver short, smooth-to-use computing services and records garage. Infrastructure as a carrier (IaaS), Platform as a provider (PaaS), and software as a service (SaaS) are the maximum distinguished cloud computing service models (SaaS). In IaaS, a cloud carrier provider presents customers with compute and garage offerings to assist them boom their enterprise abilities. PaaS is a service model wherein a carrier issuer offers consumers with a fixed of software programmes that take care of their person issues. A cloud service issuer deploys software program together with accompanying statistics, and customers get right of entry to it thru the net [2]. Cloud computing dynamically improves and expands IT capabilities with out requiring new infrastructure, licensing new software, or education new personnel. It additionally extends and grows

current IT talents [3]. DNA cryptography guarantees to provide greater confidentiality than classical encryption even as encrypting information by way of integrating biological and computational residences [4]. Traditional cryptosystems frequently offer just unmarried-layer protection, and their secrecy may be compromised when the underlying computational techniques are found out. DNA cryp- tography, however, makes use of the self-assembling abilities of DNA bases [5] in aggregate with a cryptographic technique to gain multi-fold safety [6] that improves records secrecy.

2. LITERATURE REVIEW :

[7] Present a survey inquiry into issues about cloud computing security and protection. Numerous forms of known security threats and assaults are ordered in these works, as well as various types of cloud flaws. In addition, this survey work looks at the drawbacks of current solutions and analyses potential security concerns. Cryptography [8, 9] is the fundamental technique that satisfies security criteria. RSA, DES, and other algorithms based on symmetric and asymmetric key approaches and genetic mechanisms have all been suggested, developed, and implemented. [10, 11] The design, flexibility, scalability, restrictions, security, execution time, and memory needs of cryptographic algorithms can all be compared [12]. In the cloud context, dealing with data integrity and privacy issues is crucial [13 14, 15]. Researchers have focused on cloud data integrity, with several techniques such as Provable Data Possession (PDP) and Prove of Retrievability (PoR) [16, 17] being proposed to provide data integrity. [18] Provides a review of the most vulnerable security concerns in cloud computing. In addition, this audit job covers both end-clients' and vendors' important cloud security concerns by providing analysis associated with various security models and apparatuses. This paper also shows a programme key interpretation technique that allows a product as a service application to provide privacy services. The authors of [19] presented a DNA-based symmetric security system for binary data in DNA form. The method employs a block cipher with a 128-bit or 64-nucleotide block size. This encryption technique, like DES and AES, uses a Feistel structure with 16 rounds.

Although DNA adds unpredictability to the algorithm, it is not practical in real-world applications. Despite the fact that it is a novel concept, it is slower than traditional symmetric key methods.

The authors of research [20] provided a cloud data security cryptosystem based on the Elliptic curve with the integration of the Diffie- Hellman algorithm. They stated that when compared to the state-of-the-art method RSA, the proposed cryptosystem lowered the average computational complexity of encryption and decryption by around 70%. The proposed approach, on the other hand, has not been tested on relevant data retrieval procedures for cloud data. The authors of [21] focused on data segregation and privacy protection when analysing the privacy and data security challenges of cloud computing. Data security is a major concern at the IaaS, PaaS, and SaaS levels, and data sharing is a major issue in cloud computing. One of the most basic requirements of cloud customers is data integrity. Cloud computing typically includes data processing services in addition to data storage. Organizations can have more trust in data integrity by avoiding unwanted access to cloud resources. The ability to separate information and reveal it selectively is defined as privacy. Practical countermeasures against attacks, on the other hand, have not been observed. Furthermore, a cloud data deduplication approach based on certificate-less proxy re-encryption has been proposed for cloud security in a recent research study [22]. Proof-of-ownership based on certificate-less proxy re-encryption (PoW-CLS) and certificate-less proxy re-encryption are the two techniques presented (CL-PRE). The suggested certificate-less cryptosystem addresses the issues of key escrow and decryption impersonation attacks. Lemma proofs and theoretical analysis have been used to validate the suggested mechanism. For public auditing in cloud computing, the authors of [23] presented a hierarchical attribute-based encryption approach based on semantic ontology. The suggested technique structures the data hierarchically for encryption and decryption of cloud data, and the semantic relations of the characteristics are used to pick the key parameter. The key from the semantic ontology is used to do the verification. Then, to protect data integrity and privacy, a random integer is used to execute modular padding of 0 and or 1. The proposed strategy, according to the authors, has increased the quality of public cloud data audits and the efficiency of data sharing in the cloud environment. However, the proposed technique does not take into account cloud data retrieval authentication and authorisation.

3. METHODOLOGY :

Encryption Algorithm

1. Read the plain text file and convert the plaintext to corresponding ASCII.
2. Convert the ASCII into HEX code.
3. Convert the HEX Code to binary (B1).
4. Make the groups of 256-bit from binary input file (B11, B12….). If needed append the extra bits to make a group of 256-bit.

5. XOR the B11 with K1. Similarly, B12 with K1 and so on.
6. Divide the obtained resultant R1 into two parts i.e., R11 and R12
7. Now XOR R11 with K3 and R12 with K2.
8. Again, divide the obtained resultant RK113 into two parts i.e., RK113a and RK113b.
9. XOR RK113a with K5 and RK113b with K4
10. Concatenate all the obtained resultant.
11. Convert the obtained resultant into DNA as A = 00, T = 01, G = 10 and C = 11.
12. Convert the DNA sequence to mRNA sequence by replacing (T) Thymine with (U) Uracil.
13. Convert the mRNA sequence to tRNA sequence by replaces each alphabet of DNA with its own complementary DNA alphabet. i.e. A-U, U-A, G-C, and C-G transformations are performed.
14. Upload cipher text to cloud

Decryption Algorithm

1. Read the cipher text
2. Convert the tRNA sequence to mRNA.
3. Convert the mRNA sequence to DNA sequence
4. Convert the DNA sequence to binary
5. Make group of 64 bit and named them as RK113a and RK113b.
6. XOR RK113a with K5 and RK113b with K4.
7. Similarly perform the operation for next groups
8. Concatenate the group and XOR it with K3 and K2.
9. Again, Concatenate the group and XOR it with K1.
10. Convert the binary string to HEX code.
11. Convert the HEX code to ASCII.
12. Obtain the plaintext.

Key Generation

1. Generate the random 256-bit binary key (K1).
2. Divide K1 into two parts of 128-bit each say K2 and K3.
3. Divide K2 into two parts of 64-bit each and form K4 and K5.
4. Divide K3 into two parts of 64-bit each and form K6 and K7.

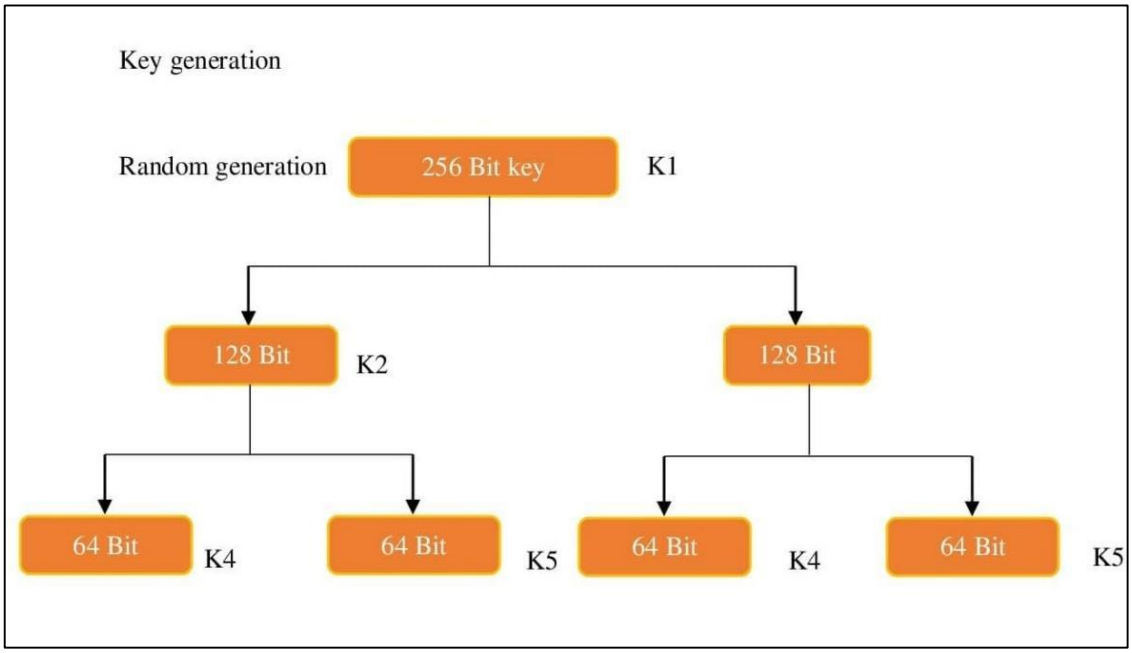

Fig. 1. Key generation process

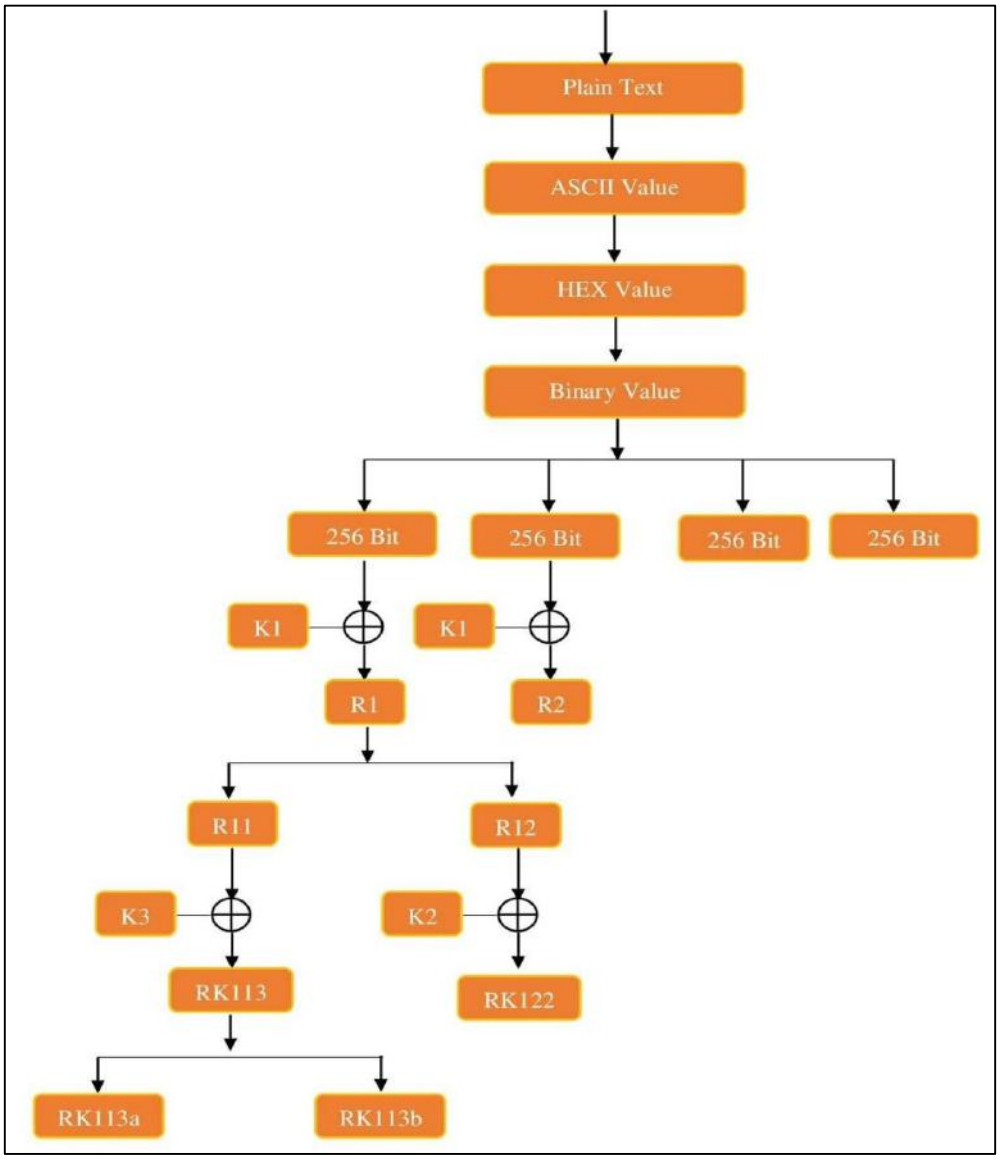

Fig. 2. Encryption process

4. RESULT ANALYSIS :

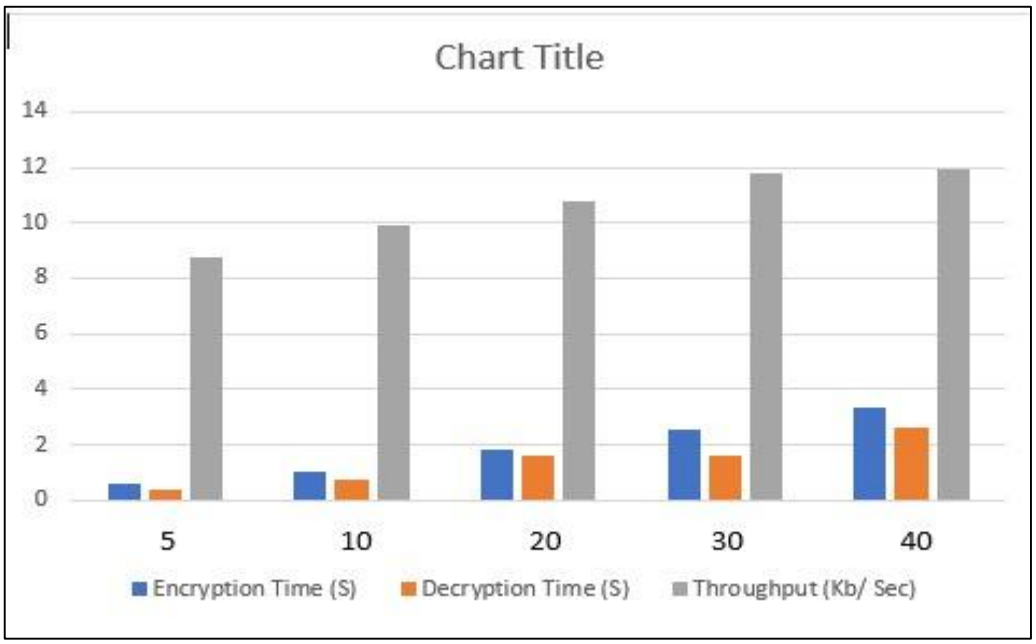

Fig. 3. Processing time of the new technique with throughput

Plaintext Size (KB)	Encryption Time (S)	Decryption Time (S)	Throughput (Kb/ Sec)
5	0.57	0.375	8.77193
10	1.01	0.706	9.90099
20	1.85	1.577	10.81081
30	2.54	1.589	11.81102
40	3.36	2.578	11.90476
50	4.27	2.985	11.7096

Table 1 Processing time of the new technique with throughput

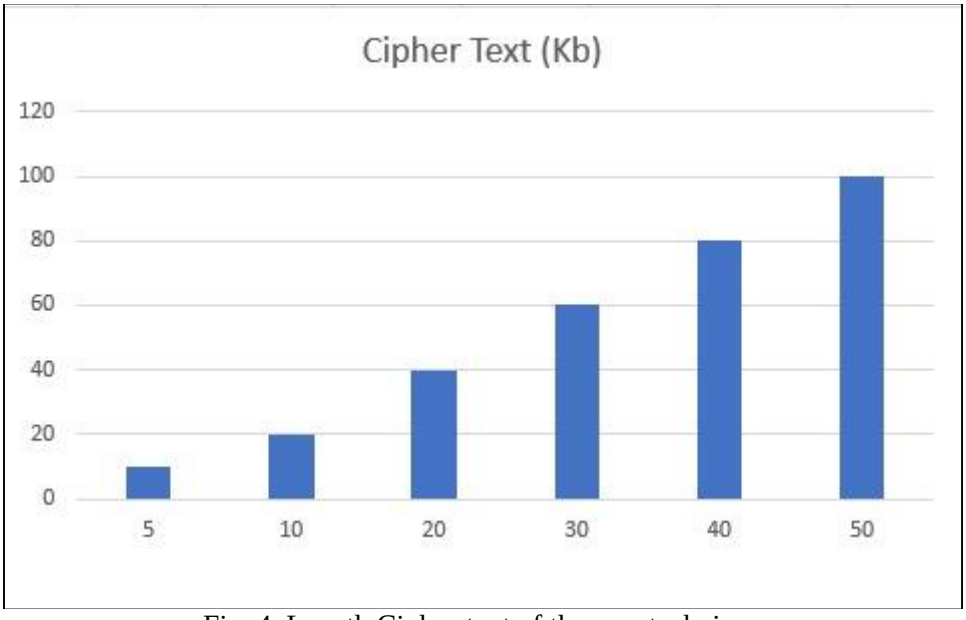

Fig. 4. Length Cipher-text of the new technique

Plaintext Size (KB)	Cipher Text (Kb)
5	10
10	20
20	40
30	60
40	80
50	100

Table 2 Length cipher-text.

Parameters for evaluating the proposed methodology-

Encryption time-

The time it takes to transform plain text to ciphertext is known as encryption time. The efficiency of an encryption algorithm is inversely proportional to the time it takes to encrypt data; the technique will always be more efficient if it takes less time to encrypt data. This metric can be measured in two different ways:

1. Analyze the encryption time based on the input size (10, 20, 30, 40, 50KB).

2. We analyse the encryption time based on input by variable count characters, time encryption and decryption is calculated.

Decryption time-

Decryption of Algorithms The time it took to recover the original data via cypher text entering is displayed. The time complexity of the decrypting algorithm is the amount of time it takes. The following formula can be used to calculate the amount of time spent decrypting.

Time consumed = end time-start time

Throughput-

The throughput of an algorithm can be used to determine its efficiency. The algorithm's throughput is proportional to its performance; that is, the higher the algorithm's performance, the higher the throughput. The following is the formula for calculating the encryption technique's throughput:

Throughput=Plain Text Size/Encoding Time

Length cipher-text

Since then, this technology has been created to store data in a Cloud file, therefore cloud storage has been factored into the design of this method to keep the data's size from increasing after encryption. Furthermore, the transfer time is proportional to the total amount of data received. Since then, data is encrypted on the client before being transferred to the server, and the amount of data downloaded has a direct impact on transmission time.

5. CONCLUSION :

With the rapid advancement of data and computing technology, the number of cloud users for both personal and professional purposes is increasing. The reason for their success is that they give effective and adaptable computational and storage solutions based on the needs of the applications. The cloud also delivers data and computational services on demand. There are still numerous obstacles to overcome in terms of data security and privacy. Despite the fact that the cloud allows for more flexibility and simplicity of control when it comes to data storage, there are still risks of unauthorized attacks and criminal actions. Several security experiments and analyses are carried out to assess the robustness of the proposed coding scheme using the following evaluation parameters: encryption time, decryption time, throughput, and cipher-text length. Based on the quantity of plain text and the time necessary to encrypt/decrypt, the proposed algorithm was compared to alternative genetic encryption techniques and existing symmetric key encryption techniques such as AES, DNA, DES, and Blowfish. For brute force, known plain-text attacks, encrypted text alone, and differential cryptanalysis assaults, the suggested encryption technique has been demonstrated safe. It has been tested on a variety of data, including whitespace and special characters, and it also adheres to the CIA's principles.

REFERENCES :

1. Fursan Thabit , Sharaf Alhomdy , Sudhir Jagtap,:A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions, International Journal of Intelligent Networks 2 (2021) 18–33
2. Sun, Y., Zhang, J., Xiong, Y., Zhu, G.: Data security and privacy in cloud computing. Int. J. Distrib. Sens. Netw. 10(7), 190903 (2014)
3. Senyo, P.K., Addae, E., Boateng, R.: Cloud computing research: a review of research themes, frameworks, methods and future research directions. Int. J. Inf. Manag. 38(1), 128–139 (2018)
4. Lu M , Lai X , Xiao G , Qin L . Symmetric-key cryptosystem with DNA technology. Sci China Ser F 2007;50(June (3)):324–33 .
5. B. Anam, K. Sakib, M. Hossain and K. Dahal, Review on the advancements of DNA cryptography, (2010). arXiv: 1010.0186 .
6. Pelletier O , Weimerskirch A . Algorithmic self-assembly of DNA tiles and its ap- plication to cryptanalysis. In: Proc. of the 4th Annual Conf. on Genetic and Evolutionary Computation. Morgan Kaufmann Publishers Inc; 2002. p. 139–46.
7. I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," Computers, 2014, doi: 10.3390/computers3010001.
8. Kardas, S., C¸ elik, S., Bingo¨l, M.A., Levi, A.: A new security and privacy framework for RFID in cloud computing. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, IEEE, vol. 1, pp. 171–176 (2013)
9. Bhardwaj, A., Subrahmanyam, G., Avasthi, V., Sastry, H.: Security algorithms for cloud computing. Proc. Comput. Sci. 85, 535–542 (2016).
10. Mushtaq, M.F., Jamel, S., Disina, A.H., Pindar, Z.A., Shakir, N.S.A., Deris, M.M.: A survey on the cryptographic encryption algorithms. Int. J. Adv. Comput. Sci. Appl. 8(11), 333–344 (2017)
11. Dixit, P., Gupta, A.K., Trivedi, M.C., Yadav, V.K.: Traditional and hybrid encryption techniques: a survey. Networking Communication and Data Knowledge Engineering, pp. 239–248. Springer, New York (2018)
12. Chowdhury, S.R., Ghosh, A., Paul, S.: Design and implementation of a novel cryptographic technique for network security using genetic algorithms (gas). Int. J. Innov. Knowl. Concepts 7(Special 1), 119–129 (2019)
13. Pujari, S.K., Bhattacharjee, G., Bhoi, S.: A hybridized model for image encryption through genetic algorithm and dna sequence. Proc. Comput. Sci. 125, 165–171 (2018)
14. Delman, B.: Genetic algorithms in cryptography (2004)
15. Jhingran, R., Thada, V., Dhaka, S.: A study on cryptography using genetic algorithm. Int. J. Comput. Appl. 118, 20 (2015)
16. Juels, A., Kaliski, Jr B.S.: Pors: Proofs of retrievability for large files. In: Proceedings of the 14th ACM conference on Computer and communications security, ACM, pp. 584–597 (2007)
17. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L.,Peterson, Z., Song, D.: Provable data possession at untrusted stores. In: Proceedings of the 14th ACM conference on Computer and Communications Security, ACM, pp. 598–609 (2007)
18. M. M. Alani, "Security threats in cloud computing," in SpringerBriefs in Computer Science, 2016.
19. Amin, S.T., Saeb, M., El-Gindi, S.: A DNA-based implementation of YAEA encryption algorithm. In: Computational Intelligence, pp. 120–125 (2006)
20. Subramanian, E., Tamilselvan, L.: Elliptic curve Diffie–Hellman cryptosystem in big data cloud security. Cluster Computing, pp. 1–11 (2020)
21. Chen, D., Zhao, H.: Data security and privacy protection issues in cloud computing. In: 2012 International Conference on Computer Science and Electronics Engineering, IEEE, vol. 1, pp. 647–651 (2012)
22. Zheng, X., Zhou, Y., Ye, Y., Li, F.: A cloud data deduplication scheme based on certificateless proxy re-encryption. J. Syst. Arch. 102, 101666 (2020)
23. Kalaivani, A., Ananthi, B., Sangeetha, S.: Enhanced hierarchical attribute based encryption with modular padding for improved public auditing in cloud computing using semantic ontology. Clust. Comput. 22(2), 3783–3790 (2019)