Scientific Research Publishing

Journal of Computer and Communications, 2024, 12, 201-210
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Nested Levels of Hybrid Cryptographical Technique for Secure Information Exchange

Pawan Kumar, Vipin Saxena

Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, India
Email: pawan0871@gmail.com, profvipinsaxena@gmail.com

How to cite this paper: Kumar, P. and Saxena, V. (2024) Nested Levels of Hybrid Cryptographical Technique for Secure Information Exchange. *Journal of Computer and Communications*, **12**, 201-210.
https://doi.org/10.4236/jcc.2024.122012

Received: December 27, 2023
Accepted: February 26, 2024
Published: February 29, 2024

Abstract

Data security is a very important part of data transmission over insecure channels connected through high-speed networks. Due to COVID-19, the use of data transmission over insecure channels has increased in an exponential manner. Hybrid cryptography provides a better solution than a single type of cryptographical technique. In this paper, nested levels of hybrid cryptographical techniques are investigated with the help of Deoxyribonucleic Acid (DNA) and Paillier cryptographical techniques. In the first level, information will be encrypted by DNA and at the second level, the ciphertext of DNA will be encrypted by Paillier cryptography. At the decryption time, firstly Paillier cryptography will be processed, and then DAN cryptography will be processed to get the original text. The proposed algorithm follows the concept of Last Encryption First Decryption (LEFD) at the time of decryption. The computed results are depicted in terms of tables and graphs.

Keywords

Encryption, Decryption, DNA, Paillier Cryptography, Nested Levels, Hybrid Cryptography

1. Introduction

In the digital world, the security of the information transmitted over the network is a major problem. Many populations around the globe are using the high-speed internet connectivity and this is because of the growth of digitization and e-commerce. Large-scale storage and management of information are made possible by cloud computing. It provides flexibility for data retrieval at any time and from any location. Data storage on the cloud has been popular among the various businesses and individual users. Although the cloud is receiving a lot of close attention, there are still issues with data security, privacy, dependability, and portability that must be addressed in the current era of technology.

On the other hand, COVID-19 was investigated as an infectious disease due to corona virus in the year 2019, due to this pandemic situation, many people were attached the high-speed network from home. Most of the organizations were functioning from the isolated platform and employees of the organizations are working from home and the same concept is also trending in the current scenario. The said virus has completely changed the life of human beings and forced them to work from the isolated places due to the large number of organizations alongwith their employees is well connected over the network. Hence, it is important to resolve the issues of the security related to information exchange between the two parties. Many of the algorithms based on the single types of cryptographical techniques called as conventional algorithms have been broken down by the hackers. Therefore, the present work is an attempt to recommend the hybrid approach of cryptographical techniques called as LEFD approach of cryptography.

In the nested levels of cryptography, the input message is encrypted by Algorithm A and generated by the cipher text-1. This cipher text-1 has given as input for cryptography of Algorithm B. The cipher text-1 is encrypted by Algorithm B and generates cipher text-2. The cipher text-2 is shared over insecure channel connected through high-speed network. Figure 1 represents the nested levels of cryptography. For decryption, the cipher text-2 is decrypted by Algorithm B and generates cipher text-1. The cipher text-1 is further decrypted by Algorithm A.

In the proposed method, nested levels of hybrid cryptography are proposed with the help of DNA and Paillier cryptographical techniques. A growing percentage of businesses in the information technology, healthcare, and educational

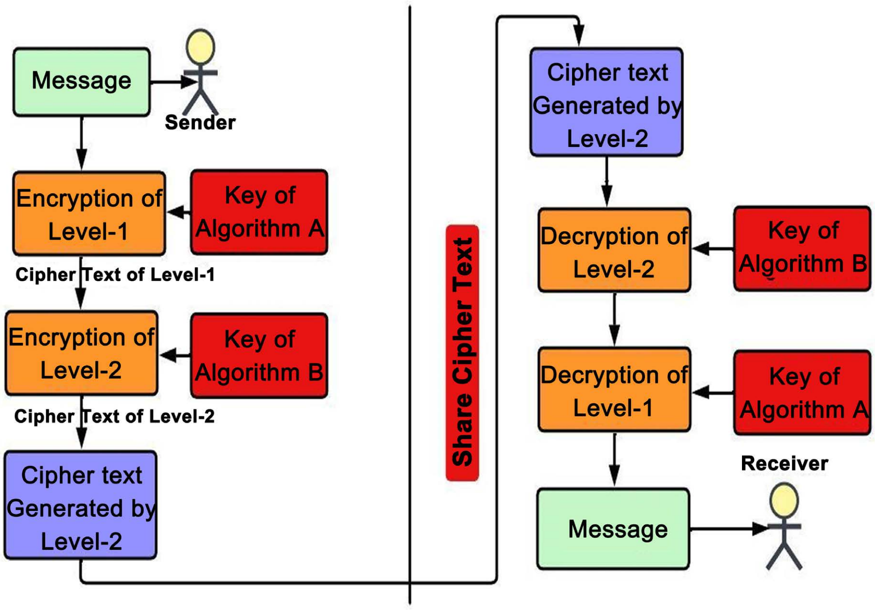

Figure 1. Detailed view of nested levels of cryptography.

sectors currently use cloud-based computing services in daily life. Additionally, there is a rising demand for cloud-based assets, which may be utilised and retrieved whenever one wants. Information security has been transformed by DNA cryptography, which uses strict biological and mathematical concepts to encrypt the original data in the form of the sequence of DNA. The use of related DNA-based keys for encryption is vital when using these approaches. In a particular kind of cryptography called DNA cryptography, private data is securely encrypted and decrypted using the unique features of DNA molecules. It investigates the possible benefits of using DNA as a means of preserving and transmitting encrypted data. The four bases of nucleotide that make up DNA, Adenine (A) represents 00, Cytosine (C) represents 01, Guanine (G) represents 10 and Thymine (T) represents 11. The bases mentioned above serve as the building blocks of DNA sequences, and the order of arrangement affects the information that is encrypted.

Paillier cryptography was introduced by Pascal Paillier in the year 1990. Paillier cryptography is public key cryptography algorithm. Paillier cryptography works on prime number with equal size distinct number. For example, if we choose one prime number with three-digit number as 103 and second prime number will be chosen from any prime number with equal length of three digits *i.e.* 997. With the help of these two prime numbers, we generate public and private keys. Paillier cryptography has three steps such that key generation, encryption and decryption and is described in the following steps [1]:

Key_Generation( )

***Step* 1.** *Choose two large prime numbers that are equal in size and must be distinct numbers and assume as* $Prmno_1$ *and* $Prmno_2$.

***Step* 2.** *Compute* $N = (Prmno_1 * Prmno_2)$ *and Define function* $L(x) = \frac{x-1}{N}$.

***Step* 3.** *Computation for private key,* $Prv\_Key = (LCM\,(Prmno_1 - 1,\ Prmno_2 - 1))$, *and* $\mu = (L(G^{Prv\_Key}\ MOD\ N^2))^{-1}$, *where G is any random number, which is* $G \in \mathbb{Z}^*N$.

***Step* 3.** *Public key is* $Prb\_Key(N, G)$.

Encryption( )

***Step* 1.** *Count the size of message, store in M and to check* $0 \le M \le N$.

***Step* 2.** *Select any random number Rndm_number, which is* $0 < Rndm\_number < N$ *and* $Rndm\_number \in \mathbb{Z}^*N$.

***Step* 3.** *Encrypt the message,* $Cphr\_txt = G^M.Rndm\_number^N\ MOD\ N^2$.

Decryption( )

Step 1. To check $Cphr\_txt < N^2$.

Step 2. Computation for Original Message = $L(Cphr\_txt^{Prv\_Key}\ MOD\ N^2).\ \mu\ MOD\ N$.

The above two algorithms are well-established techniques used for security of the plain text and also for the other kinds of information converted into the ASCII code. DNA generates symmetric keys while Paillier generates the asymmetric keys used for encryption and decryption methods and cracking of any one algorithm is still not reported in the literature hence combination of these two algorithms is taken as a nested level of security during exchange of the information.

2. Related Work

The researchers have developed a wide range of assessment methods for the hybrid cryptography. Let's go through a few of the significant studies that are connected to the hybrid cryptography (nested levels of hybrid cryptography). Kumar and Saxena [1] have also implemented key exchange in hybrid cryptography with the help of AES and Paillier cryptography. In the year 2015, Kumar and Jagan [2] have implemented two-layer security for data security. Public key cryptography was employed at the top layer, whereas steganography was solely utilised at the bottom layer. In the first layer, RSA cryptography is used while in the second layer, steganography is used. Saxena and Dey [3] have implemented the technique for integrity of data verification in cloud computing environment with support of Paillier cryptography and data block (combinational batch code). Each piece of information is given a unique verifiable value using homomorphic tags and the Paillier cryptography system, which enables to perform data processing operations on the block. To allocate and save fundamental data onto several scattered cloud servers, combinatorial batch codes are utilised. Akomolafe and Abodunrin [4] have implemented hybrid cryptography in combination of hash, symmetric and digital signature where hash cryptography is Blake2, symmetric cryptography is AES and digital signature is Schnorr signature. Gandara *et al.* [5] have discussed that hybrid cryptography gradually raise the protection standard and reduce resource consumption in WSN and compared to symmetric and asymmetric algorithms, hybrid cryptography was more effective at escalating security defence levels and reducing utilisation of resources on wireless sensor networks. Kumar and Saxena [6] have implemented nested levels of cryptography with the help of AES, RSA and genetic algorithm. El-Douh *et al.* [7] have discussed classification of hybrid cryptography in respective of model based and domain of application.

In the year 2018, Hazre *et al.* [8] have used DNA cryptography in addition to different cryptography method. The outcomes of the experiments demonstrate that DNA may be used for a variety of biological processes and encoding methods. Abdullah *et al.* [9] have discussed various DNA based cryptography, provided brief information of some DNA based cryptography and compared between conventional types of cryptography and DNA based cryptography. Hammad *et al.* [10] had implemented hybrid cryptography with help of DNA and RSA cryptography. In the first part, DNA cryptography is used with One Time Password (OTP) and in the second part, DNA cryptography is incorporated with RSA cryptography. The current experimental findings demonstrated that DNA symmetric cryptography performed well in time and size evaluations. In the year 2018, Sohal and Sharma [11] had implemented new cryptography algorithm that encrypts information on the client side before it is uploaded to the cloud (network server). The proposed algorithm had compared with some symmetric cryptographic algorithm such that DES, AES and Blowfish. The results of the experiment show that, when measured in terms of cipher text size, encryption time, and throughput, suggested technique performs better than standard algorithms. Khobzaoui *et al.* [12] have implemented DNA cryptography with help of chromosome and it was symmetric type of cryptography. The technique involves encrypting and decrypting the data in blocks of characters while using a symmetric key that was retrieved from a chromosome. Mukherjee *et al.* [13] have implemented DNA cryptography to extract key with help of genetic algorithm approach. The studies presented a function of fitness computation for those weak keys based on the standard deviation. Poriye and Upadhyaya [14] have designed a security framework with help of DNA cryptography for WSN. The structure of the system is divided into stages, including the one involving both the decryption and encryption of data between two sensor nodes in the network. The process used in cryptography is like the framework and functions of DNA. Seth *et al.* [15] have implemented hybrid cryptography with the help of Blowfish and Paillier cryptography. The suggested hybrid cryptography aims to increase the computing efficiency and ciphertext size of cloud storage. This combination of homomorphic and asymmetric cryptography had shown to provide increased security. Utilising compression had aided in reducing both store space and calculation time.

In the year 2021, Koundinya and SK [16] have implemented two-layer encryption with the help of two popular asymmetric cryptography such as Paillier and Elgamal cryptography. The Paillier cryptosystem, which was employed for applications like secure biometrics and electronic voting, makes use of additive homomorphism. Elgamal cryptography makes sure that two-layer encryption is used to protect Paillier encrypted data. Munjal and Bhatia [17] have analyzed and compared between partial homomorphic cryptography RSA and Paillier cryptography and examined based on key generation, encryption time, decryption time, computation time and communicational time. Kumar *et al.* [18] have implemented new homomorphic cryptography with the help of Paillier cryptography and bit shifting. The techniques enable to perform mathematical operations on encrypted data without having to first decode them. Asiedu and MuminSalifu [19] have improved Paillier cryptography with the help of Residue Number System (RNS). In the enhanced traditional system of cryptography, there are two steps of encryption and decryption in the Paillier cryptosystem. In the first step, Paillier cryptography is followed and in the second step, the cipher text is processed by moduli that occurred from Paillier cryptography. Kumar *et al.* [20] have implemented hybrid cryptography with the help of AES, RSA and Elliptic Curve Integrated Scheme (ECIES) cryptography. Saxena and Kumar [21] have implemented new hybrid cryptography for currency transaction with the help of fuzzy, hash cryptography, fingerprint authentication and Elgamal cryptography. Yadav and Kumar [22] have presented a new hybrid cryptography in combination of symmetric, asymmetric and DNA cryptography. The resultant hybrid technique outperformed the AES algorithm in terms of bio complexity for packages larger than 200 kilobytes and was at least 20.7398% quicker than the conventional RSA scheme.

3. Proposed Method

In the proposed method, the nested levels of hybrid cryptography are investigated. Before the information exchange, the key is generated by Paillier cryptography. Paillier cryptography shared public key over insecure channel connected through high-speed networks. Figure 2 represents block diagram of proposed algorithm.

In the proposed algorithm, the level-1 is encrypted by DNA cryptography and the level-2 is encrypted by Paillier cryptography.

The steps of the proposed algorithm are given below:

Key_Generation ( )

Step 1. *Receiver generates public and private key with the help of Paillier Cryptography.*

Step 2. *Shares public key.*

Step 3. *Sender generates private key with help of DNA Cryptography.*

Encryption()

Step 1. *At level*-1 *encryption*, $DNA_{Cipher} = DNA_{priv\_key\_DNA}(Message)$.

Step 2. *At level*-2 *encryption*, $Paillier_{Cipher} = ENC_{Paillier,\, pubkey}(DNA_{Cipher})$.

Step 3. *Shared cipher text of level*-2 *over insecure channels as* $Paillier_{Cipher}$.

Decryption()

Step 1. *At level*-1 *decryption*, $DNA_{Cipher} = DEC_{Paillier},\ priv\_key(Paillier_{Cipher})$.

Step 2. *At level*-2 *decryption*, $Message = DEC_{priv\_key\_DNA}(DNA_{Cipher})$.

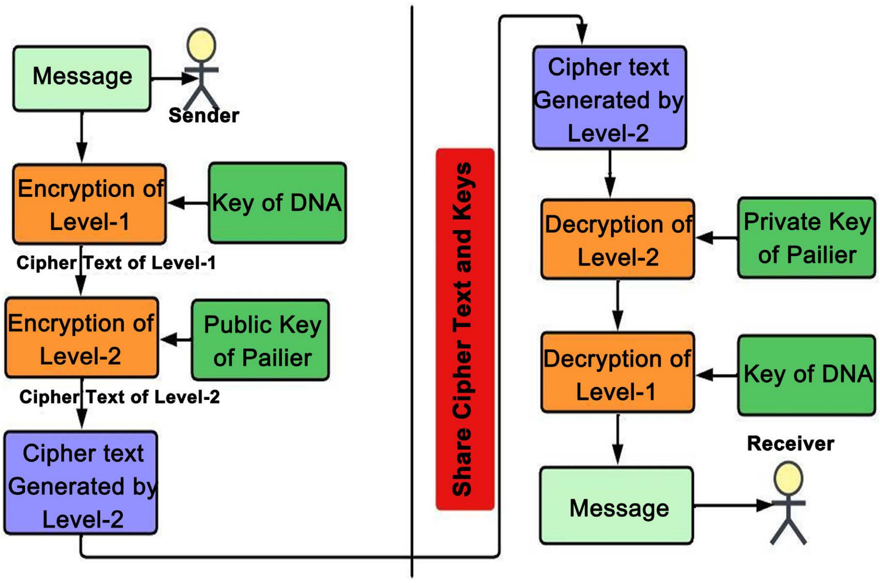

Figure 2. Flow of proposed algorithm.

In the proposed algorithm, the sender receives public key of the receiver which is the public key generated by Paillier cryptography. The sender encrypts the message by DNA cryptography and generates cipher text. Again, this cipher text is encrypted by public key of Paillier cryptography and this cipher text sent over insecure channels. The recipient receives the cipher text and the cipher text is decrypted by private key of Paillier cryptography. In next phase, decrypted value is decrypted by DNA cryptography.

4. Results and Discussion

The nested levels of hybrid cryptography provide more security than other algorithms available in the literature. The proposed algorithm combines DNA cryptography as symmetric and Paillier cryptography as asymmetric cryptography. In the nested levels of cryptography, one cryptography algorithm encrypts the message and generates cipher text, this cipher text gives second cryptography as message. Second cryptography encrypts this cipher text according to the public key and generates cipher text. This cipher text shares over insecure channel. At the receiver end, the cipher text is decrypted by cryptography algorithm which is encrypt in the last which means that it follows the concept of last in first out and denoted as LEFD.

The experiments are computed in Python 3.10.6. Table 1 represents comparison of existing algorithm and proposed algorithm. The first column represents size of input message, the second column represents time taken by existing algorithm and the third column represents time taken by proposed algorithm.

Let's take an example with input a text message like "This is my research algorithm". Table 2 represents level of encryption and decryption of proposed algorithm.

Further, Figure 3 represents comparison between existing algorithm and proposed algorithm. When size of inputs is less then encryption and decryption process take less time.

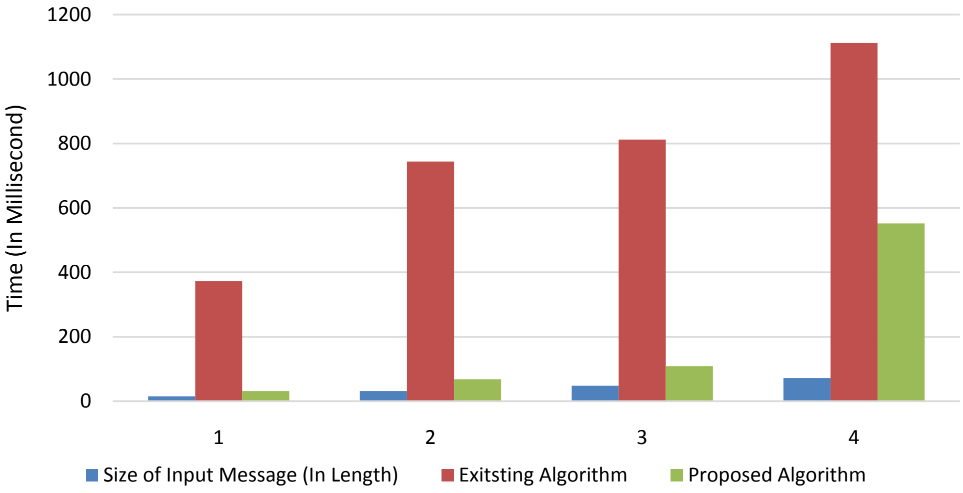

Figure 3. Comparison between existing algorithm and proposed algorithm.

Table 1. Comparison between existing algorithm and proposed algorithm.

Size of Input Message (In Length)	Existing Algorithm [5] (In Millisecond)	Proposed Algorithm (In Millisecond)
15	373	31
32	744	68
48	812	109
72	1112	552

Table 2. Level wise encryption and decryption of the proposed algorithm.

Message	Encryption Level-1	Encryption Level-2	Decryption Level-1	Decryption Level-2	Final Message
This is my research algorithm	CAGTCCAACTCAAGACACAGCATTTCAAGACACAGCATTTCAATACACGACATTTCAGGTCAACACACAGCAACACAAAACACACCAAAGCAACTCATTTCACGGCAAGTCAACGCAATGCACACCAAGACACATCAACTCAATA	15149180436711228097858022352719402357347320940219596186681445669405087229804374521603434935340823900435968565206669721113208408840785170069517370452962426987999847275352443615604524072869502716808975632486948069668075427523825357953802877408647278967733689349537896566345597370225164378781496201599759734459	15149180436711228097858022352719402357347320940219596186681445669405087229804374521603434935340823900435968565206669721113208408840785170069517370452962426987999847275352443615604524072869502716808975632486948069668075427523825357953802877408647278967733689349537896566345597370225164378781496201599759734459	CAGTCCAACTCAAGACACAGCATTTCAAGACACAGCATTTCAATACACGACATTTCAGGTCAACACACAGCAACACAAAACACACCAAAGCAACTCATTTCACGGCAAGTCAACGCAATGCACACCAAGACACATCAACTCAATA	This is my research algorithm

5. Conclusion and Future Scope

From the above work, it is concluded that nested levels of hybrid cryptography provide better security than a single level of cryptography. In the proposed work, the cryptography algorithm uses hybrid cryptography such that DNA cryptography is symmetric cryptography and Paillier cryptography is asymmetric cryptography. DNA cryptography consumes less time in encryption and decryption process than other algorithms. The cipher text-2 has been shared along with the key of DNA cryptography. It used two cryptographies but shared only one cipher text. Hence, the proposed algorithm takes less bandwidth during data transmission over communication channels. In the future, the proposed approach may be extended by considering other prominent algorithms used for encryption and decryption.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Kumar, P. and Saxena, V. (2023) Hybrid Cryptography for Security Exchange through

AES and Paillier. *European Chemical Bulletin*, **12**, 3913-3921.

[2] Kumar, A.A. and Jagan, A. (2015, February) Two-Layer Security for Data Storage in Cloud. 2015 *International Conference on Futuristic Trends on Computational Analysis and Knowledge Management* (*ABLAZE*), Greater Noida, 25-27 February 2015, 471-474. https://doi.org/10.1109/ABLAZE.2015.7155041

[3] Saxena, R. and Dey, S. (2016) Cloud Audit: A Data Integrity Verification Approach for Cloud Computing. *Procedia Computer Science*, **89**, 142-151. https://doi.org/10.1016/j.procs.2016.06.024

[4] Akomolafe, O.P. and Abodunrin, M.O. (2017) A Hybrid Cryptographic Model for Data Storage in Mobile Cloud Computing. *International Journal of Computer Network and Information Security*, **9**, 53-60. https://doi.org/10.5815/ijcnis.2017.06.06

[5] Gandara, R.B., Wang, G. and Utama, D.N. (2018, September) Hybrid Cryptography on Wireless Sensor Network: A Systematic Literature Review. 2018 *International Conference on Information Management and Technology* (*ICIMTech*), Jakarta, 3-5 September 2018, 241-245. https://doi.org/10.1109/ICIMTech.2018.8528147

[6] Kumar, J. and Saxena, V. (2020) Hybridization of Cryptography for Security of Cloud Data. *International Journal of Future Generation Communication and Networking*, **13**, 4007-4014. http://sersc.org/journals/index.php/IJFGCN/article/view/34754

[7] El-Douh, A.A.R., Lu, S.F., Elkony, A. and Amein, A.S. (2022, March) A Systematic Literature Review: The Taxonomy of Hybrid Cryptography Models. In: Arai, K., Ed., *Future of Information and Communication Conference*: *Advances in Information and Communication*, Vol. 439, Springer, Cham, 714-721. https://doi.org/10.1007/978-3-030-98015-3_49

[8] Hazra, A., Ghosh, S. and Jash, S. (2018) A Review on DNA Based Cryptographic Techniques. *International Journal of Network Security*, **20**, 1093-1104.

[9] Abdullah, N.A.N., Zakaria, N.H., Ab Halim, A.H., Ridzuan, F.H.M., Ahmad, A., Seman, K. and Ariffin, S. (2022) A Theoretical Comparative Analysis of DNA Techniques Used in DNA Based Cryptography. *Journal of Sustainability Science and Management*, **17**, 165-178. https://doi.org/10.46754/jssm.2022.05.014

[10] Hammad, B.T., Sagheer, A.M., Ahmed, I.T. and Jamil, N. (2020) A Comparative Review on Symmetric and Asymmetric DNA-Based Cryptography. *Bulletin of Electrical Engineering and Informatics*, **9**, 2484-2491. https://doi.org/10.11591/eei.v9i6.2470

[11] Sohal, M. and Sharma, S. (2022) BDNA-A DNA Inspired Symmetric Key Cryptographic Technique to Secure Cloud Computing. *Journal of King Saud University-Computer and Information Sciences*, **34**, 1417-1425. https://doi.org/10.1016/j.jksuci.2018.09.024

[12] Khobzaoui, A., Benyahia, K., Mansouri, B. and Boukli-Hacene, S. (2022) DNA-Based Cryptographic Method for the Internet of Things. *International Journal of Organizational and Collective Intelligence* (*IJOCI*), **12**, 1-12. https://doi.org/10.4018/IJOCI.2022010101

[13] Mukherjee, P., Garg, H., Pradhan, C., Ghosh, S., Chowdhury, S. and Srivastava, G. (2022) Best Fit DNA-Based Cryptographic Keys: The Genetic Algorithm Approach. *Sensors*, **22**, Article 7332. https://doi.org/10.3390/s22197332

[14] Poriye, M. and Upadhyaya, S. (2023) A DNA Based Framework for Securing Information Using Asymmetric Encryption. *Wireless Personal Communications*, **129**, 1717-1733. https://doi.org/10.1007/s11277-023-10203-y

[15] Seth, B., Dalal, S., Le, D.N., Jaglan, V., Dahiya, N., Agrawal, A., *et al.* (2021) Secure Cloud Data Storage System Using Hybrid Paillier-Blowfish Algorithm. *Computers*,

Materials and Continua, **67**, 779-798. https://doi.org/10.32604/cmc.2021.014466

[16] Koundinya, A.K. and SK, G. (2021) Two-Layer Encryption Based on Paillier and Elgamal Cryptosystem for Privacy Violation. *International Journal of Wireless and Microwave Technologies*, **11**, 9-15. https://doi.org/10.5815/ijwmt.2021.03.02

[17] Munjal, K. and Bhatia, R. (2022) Analysing RSA and PAILLIER Homomorphic Property for Security in Cloud. *Procedia Computer Science*, **215**, 240-246. https://doi.org/10.1016/j.procs.2022.12.027

[18] Kumar, P.S., Nikhil, N.G.S., Vikram, N.R. and Deepa, R. (2022) Improving Security in Cloud Data Using Paillier Homomorphic Encryption System. In Tiwari, S., Trivedi, M.C., Kolhe, M.L. and Singh, B.K., Eds., *Advances in Data and Information Sciences*, Springer, Singapore City, 59-69. https://doi.org/10.1007/978-981-19-5292-0_6

[19] Asiedu, D. and MuminSalifu, A. (2022) Secured Paillier Homomorphic Encryption Scheme Based on the Residue Number System. *International Journal on Cryptography and Information Security* (*IJCIS*), **12**, 1-13. https://doi.org/10.5121/ijcis.2022.12101

[20] Kumar, P., Saxena V. and Singh, K.V. (2023) Analysis of Hybrid Cryptography for Secure Exchange of Information. *International Journal of Computer Applications*, **185**, 37-42. https://doi.org/10.5120/ijca2023922701

[21] Saxena, V. and Kumar, P. (2023) Secure Transaction of Digital Currency through Fuzzy Based Cryptography. *Indian Journal of Science and Technology*, **16**, 3148-3158. https://doi.org/10.17485/IJST/v16i37.1453

[22] Yadav, V. and Kumar, M. (2023, January) A Hybrid Cryptography Approach Using Symmetric, Asymmetric and DNA Based Encryption. *2023 3rd International Conference on Intelligent Communication and Computational Techniques* (*ICCT*), Jaipur, 19-20 January 2023, 1-5. https://doi.org/10.1109/ICCT56969.2023.10076124