# EUDSFDNA: Enhanced User Data Security Framework using DNA Cryptography in Cloud Computing Environment

**L. Leelavathy**
*(Ph.D. Research Scholar), Department of Computer Science,*
*Christhu Raj College, (Affiliated to Bharathidasan University)*
*Tiruchirappalli, Tamil Nadu, India.*
*leelakarthikeyen@gmail.com*
**Dr. Ramalingam Sugumar**
*Professor & Director, Department of Computer Science,*
*Christhu Raj College, Tiruchirappalli, Tamil Nadu, India.*
*rsugusakthi1974@gmail.com*

***Abstract:*** Cloud computing has remained today's fashion due to the growth of the hi-tech improvements and continuous changes of worlds Internet development. The cloud computing environment provide variety of services at the rate of very lower cost and convenience. That is the reason the web users have progressively placed their web resources and information in the cloud data centers. The usage of data volume increasing now a days by the cloud users is giving the bigger task to the data service provider to provide the better quality to the cloud data user. The cloud environment provide everything as a service todays but most of the common people using the storage service it is more dependable and elastic to the cloud users to store and regain their data at anytime and everywhere. Worldwide the cloud users increasing day by day so we think about the security of the users data is the most important one it plays the big role the that environment. As a user we depend on the cloud service provider sometimes it may be insecure. The cloud users are speculating about attacks on the truthfulness and the accessibility of their data in the cloud from hateful insiders and outsiders, and from any collateral impairment of cloud services. Based on this we identify some problems remain very important but then again there is stagnant far possibility for security research in cloud computing environment. In this paper presents an Enhanced User Data Security DNA-Framework in Cloud Computing Environment. The proposed framework EUDSFDNA is envisioned for familiarizing a structure and the framework sanctions the cloud service provider to install a security in dissimilar data centers dynamically though the cloud data user's necessity further security aimed at growing the data storage.

**Keywords:** Cloud computing, Internet, Storage, Security, Framework. Dynamically.

## *I*-Introduction

Now a days cloud services are in well-known [1] outstanding to the progression in networking and high performance computing software and hardware. In accumulation, around is a growing trend from end users to move the load of enormous storage, and wild and difficult computing to [2] cloud servers, which will save space, time and power. So, a developing business of service providing, run by CSPs [3] cloud service providers, has been noticeable just, particularly from large size organizations. Such as Microsoft, Google and Amazon. The customers of a cloud service [4] provider pay for services rendering to the types of service and their service usage. Basically the cloud service are sub divided into three models, Software as a service SaaS [5], Platform as a service PaaS and Infrastructure as a service IaaS. The growing quantity of cloud user's data is at a remarkable speed, outpacing the storage capability of many groups of companies. As a result, subcontracting data to cloud servers is measured a solution to store greater data into efficient cloud data centers. A cloud [6] computing environment suggestions storage as a service under Infrastructure as a service through dissimilar cloud service providers, that allow cloud users or organizations to store data on remote servers, other than organization servers. Database outsourcing bring together an innovative model, named DataBase as a Srvice (DBaaS). Talk about the [7] DBaa service security is the main issues in outsourcing data or databases to cloud servers. The data holder be unable to find control of the data, and the cloud service provider turn out to be the central data manager. By subcontracting the database, the cloud servers and the networks are frequently the target of malicious attacks. Secured cloud computing denotes the fortification of data and process. Ranges of protection are: availability of data, Privacy and Reliability. Cryptography delivers confidentiality of knowledge in cloud computing. Now a days seen that the cryptography seen as merger of three kinds of procedures. [8] They are Symmetric-key procedures, Asymmetric-key procedures and Hashing. Data cryptography function is scrambling the content of the data like script, picture, video, sound and so forth to make the information tangled, impalpable or inconsequential amidst transmission or point of confinement is named Encryption. The significant motivation behind cryptography is to oversee information secure from trespassers. Currently, there is other afresh developing cryptographic technique in the field of cryptography called DNA cryptography. The core fair of this method is to encrypt the plaintext and hide it in the DNA digital form. DNA cryptography allows the confidentiality of data further high then the modern methods with the use of one time pad keys and its size. Also it is believed that in DNA cryptography the key can be made for the huge length of data compared to the

recent methods in which key are generated only for smaller length of the data [9]. The idea of DNA computing acting an authoritative role in the field of computer security which is predictable to be an extra powerful and strong cryptographic algorithm now a days. The DNA cryptography methods supports the management of ciphertext data under privacy protection.

This paper has been prearranged by way of follows. Division I stipulates the introduction on cloud computing environment. Division II stretches the related work of this research effort. Division III originates the framework. Division IV springs the conclusion the proposed work.

## *II- Related Work*

To reduce the malicious user movement in cloud computing environment. The author says the method of DNA cryptography [10] for making a robust key for user and data encryption and decryption process. The Cloud user's info is transformed into human deoxyribonucleic acid form for making sturdy key and data encryption. The execution of the approach is approved out in DOTNET framework and the experimental effects are verified.

In this work presents a strong framework that keeps the copyright property where only the authorized users legally use the data and avoids the prohibited using or copying of end user's data. This [11] framework is created on Digital Right Management and contains two healthy cryptosystems; one is Advanced Encryption Standard algorithm and second one is Elliptic Curve Cryptography algorithm. So the author using the algorithm AES-256 for encrypting the multimedia contents. Here the shared key is encrypted using the ECC algorithm.

This paper offerings a new security framework which offers more data security and confidentiality of user's data. Here a [12] data is fragmented in the blocks of bits. Genetic algorithm is useful on each two blocks of bits. Both ciphertext is stored on cloud at separate place and location of process is a ciphertext which is also two blocks of bits. Every ciphertext is stored on cloud at separate location and setting of the ciphertext is not static. So, it is problematic for an attacker to notice where ciphertext is also genetic algorithm has no key idea due to which security of data increases. The new security framework spread over genetic algorithm on lesser block size which rises the security. The framework too uses the competence slope for secure and fine grain contact of data.

An active security framework [13] is rummage-sale to make available an apparatus through which communication is protected and unauthorized access is restricted. This security framework permits cloud end users to securely handle the privacy and integrity of data it also agree to security, confidentiality, network usage, and storage in the cloud without depending on the credibility of the cloud provider. The application of the AES algorithm delivers a robust basis that defends data stored in the cloud as well as authorizes entrée to data only on positive authentication and verification. The framework improves security, reduces resource utilization, and decreases delay while arranging services of computational clouds.

The cryptography system places a main role to secure the data inside the cloud environment. Therefore, there is a need for standard encryption and decryption mechanism to protect the data stored in the cloud environment, in which key is the required element. Each cloud provider has its own security tools to keep the key. The buyer cannot faith the service provider totally in spite of the fact that, at any instant, the supplier has full access to both data and key. In this paper, [14] a new system which can avoid the contact of the key as well as a framework for distribution a file that will ensure security using asymmetric key and distributing it within the cloud environment using a right-hand third party.

The authors [15] have examined the impacts of the present approaches and techniques to put a systematic study of the current software security issues in the Cloud environment. Based on such viewpoints and survey, a generic framework theoretically is designed to plan the possible current solutions of software security issues in the Cloud and to present a favored software security method to investigate the Cloud research community. As a possible enhancement on the Cloud software security framework, the ideas of fuzzy systems strength to be used to solve a huge numbers of problems in the Cloud security on dissimilar framework levels.

A security mechanism to maintain confidentiality of data. So this method [16] is mixture of multiplicative homomorphic encryption algorithms along with vertical fragmentation of data. It tested our scheme based on communication delays, crypto delays and query processing delays with an existing work. The results gained show that this method out-perform the existing work.

In this article CCAF multi-layered security, was demonstrated. The CCAF security was accessible with the addition of the three-layered security: firewall, identity management, and encryption. Tests were intended to prove CCAF multilayered security as an employed framework for business clouds, whose marks show that it can detect and block viruses and trojans during penetration test. CCAF [17] security policy might work with real-life examples and also bring into line with businesses to protect assets and data. This learning also proved the three major research aids and explained how it could offer profits for volume, velocity, and veracity of big data service in the cloud computing environment.

A framework that considers and assesses security issues in cloud computing environment by a quantifiable approach. This [18] framework is linked in nature that is it reflect the threats individually and seek solution for that. This supports to achieve the cloud system more effectively and provide the administrator to include the specific solution to counter the threat. It predict develop a whole security assessment and management framework as a part of cloud computing services to satisfy the security demands and then organize this framework on really cloud computing environments. Then, it envision control the multi-dimensional Mean Failure Cost model - M2FC by analyzing the cost of various countermeasures.

A novel [19] algorithm is used with the integration of Ciphertext Policy-Identity Attribute-based Encryption and the Rivest–Shamir–Adelman algorithm for securing the cloud. Both the owners and users are provided with the public and distinct secret keys that are generated by the Automated Certificate Authority. The RSA-CP-IDABE algorithm also avoids the Man in the Middle (MITM) attack successfully. The recital of the algorithm is estimated for its time used for encryption, decryption, and execution for variable sizes of data. The developed results are compared with the current framework to show its effectiveness.

In this article to secure the end users data the combination of encryption algorithms is used that is recognized as hybrid encryption algorithm. It is the grouping of symmetric AES and asymmetric RSA encryption algorithms. This [20] hybrid encryption algorithm is to increase the security level to the data. For the encryption of sensitive data, both symmetric and asymmetric encryption techniques are important.

This paper provided the framework for confidentiality of user's data called [21] AROMO. In this framework, user's data are protected in the Cloud Storage location. The AROMO framework has a mechanism which uses two techniques to keep the data that are encryption and obfuscation. The data are encrypted and obfuscated earlier it is uploaded to CS. Based on the enquiry from the client, essential data is procured out from the CS; it could be decrypted and deobfuscated in client side founded on the metadata details.

HLDNS – A Hypervisor Level Distributed Network Security framework [22] which is deployed on each processing server of cloud computing environment. At each server, it monitors the underlying VMs related network traffic to the virtual network or from the virtual network, internal network and external network for intrusion detection. It extended a Binary Bat Algorithm with two new fitness functions for originating the feasible features from cloud network traffic. The derived features are practical to the Random Forest classifier for detecting the intrusions in cloud network traffic and intrusion alerts are generated. This security framework is tested on the cloud network tested at NIT Goa and using recent UNSW-NB15 and CICIDS-2017 intrusion datasets.

This paper intentions to grow the secure framework which limits the insider attacks. The [23] framework covers slicing, data uploading, indexing, encryption, distribution, decryption, retrieval and merging process. The hybrid encryption algorithm was industrialized to deliver the security to the big data before storing it in to the multi cloud. The Simulation analysis is carried with real time cloud storage environments. This algorithm recorded about 2630 KB/S for the encryption method. The results show the superiority of the algorithm associated to the bench mark algorithms.

## III. DNA Security Algorithms.

### Ensure Data Security and Privacy using DNA Symmetric Encryption Method in Cloud Algorithm

The ensure data security and privacy DNA symmetric encryption algorithm follow same technique by integrating, substitution & transposition cipher. This two techniques have used character as a plain text value. First the cipher text character is converted to ascii value and the next stage the converted value that is the first stage value is converted as a DNA code. The DNA base algorithm is described below. [9].

The given steps are the encryption algorithm steps.

**Algorithm: 1-Encryption**

Step 1: Count the No. of character (N) in the plain text Without space.
Step 2: Convert the plain text into equivalent ASCII code. And form a matrix.
Step 3: Apply the converted HEXA code value form the Matrix.
Step 4: Take the even column (2, 4) vales Rewrite and odd column values (1,3)values rewire to form the following order wise
Step 5: Take the key values (DNAC) 44,4E, 41, 43 and Ex-Or with the each row of the matrix.
Step 6: convert the HEXA code into encrypted DNA code and the value into the matrix in the same order.
Step 7: Read the message by column by column. Using the key values (key values 3,1,4, 2)
Step 8: The Converted DNA value as the Cipher Text.

The given steps are the decryption algorithm steps.

**Algorithm: 1-Decryption**

Step 1: The encrypted DNA text is to form the matrix column by column. Using the key values (key values 3,1, 4, 2)
Step 2: The same matrix again to form by use the key (2,4,1,1)
Step 3: Take the key values (DNAC) 44,4E, 41, 43 and Ex-Or with the each row of the matrix.
Step 4: Take the even column (2,4) vales Rewrite and odd column values (1,3)values rewire to form the following order wise and arrange the data in proper matrix order (1,2,3,4)
Step5: Apply the converted DNA code to HEXA code and form the Matrix
Step 6: Convert the ASCII code into equivalent character

**SNDDNA- Algorithm**

The SNDDNA algorithm is used the standard encryption techniques by mixing selected mathematical operation on the given numerical input plaintext. This systems have used DNA code for cipher text. In this algorithm, 1st stage the plain text is merged with the key value and it produced some results and the 2nd stage of this algorithm procedure using DNA code which is used for this algorithm. The planned DNA code base algorithm is described below. [24]

The algorithm is given below

**Algorithm: 2- Encryption**

Step 1: Count the No. of character (N) in the plain text (Numerical value) without space.
Step 2: The plain text value is multiply with K1 (K1=N, K1is the key1) the each value of the PT that is MV.
Step 3: The MV value is arrange in reverse order RO1.
Step 4: The value of the RO1 is take as a cube root CR.
Step 5: The RO2 is multiplied with K2.
Step 6: The RO2 value is again arranged in reverse order it stores in MV1
Step7: The RO2 is modulus with 256 and get the Mod value. MODV.
Step 7: The Mod value is convert the binary code value.
Step 8: Finally the binary value is converted in to the DNA code as the Cipher Text.

**Algorithm: 2 -Decryption**

Step 1: covert the DNA cipher text to binary value.

Step 2: The binary code value is converted to equivalent
Step 3: The MODV is convert in to RO2

Step 4 : RO2 value is shift right to left one shift then we

Step 5: The value MV1 is divide by K2= 3 we get the

Step 6: the reverse CR value we get the value RO1=864.
Step 7: The RO1 value is shift right to left one position

Step 8: the MV value is divide by K1

By end of all these steps in the decryption algorithm the original text is retrieved by the user.

## III. Proposed DNA Based Framework in cloud Environment.

This DNA based security framework is provide the data security mechanism for the cloud end users in cloud system. The proposed EUDSFDNA framework is to answer the old-style security problems. The EUDSFDNA framework is expending cloud computing skills as shown in the given fig.1, the first part this EUDSFDNA framework is user request that provides system interaction with users using web services. The request comes from users through the internet. This user's request move on the cloud service provider. The availability (Character, Non-numeric and character numeric data) of the services forwarded to requester and the storage user select kind of service that is required. Once the service selected by the user the concern service assigned to the requester. Then, the security algorithm is used to deliver finest security mechanisms. The inspiration after this EUDSFDNA framework is to assign data on the particular security methods. Depending on the user request the following algorithm will be executed DNA Symmetric Encryption algorithm, SNDDNA and EUDSDNA algorithm.

The algorithm is given below

**EUDSDNA algorithm**

Plaintext – cloud 78 81 65 89 70

**Algorithm:3- Encryption**

Step 1: Count the No. of character (N) in the plain text (character and Numerical value) without space.
Step 2: Convert the plain text numeric value into equivalent ASCII code and character value as it's as.
Step 3: The converted numeric value plus the original plain text merged.
cloudNQAYF
Step 4: Add the key value, each plain text value is added with its corresponding position value with two characters KV1
(cde lmn opu uvx def NMO QRSABC YZA FGH)
Step 5: Each value of KV1 converted to equivalent binary value.
C=01100011 d= 01100100 e =01100101 ……..
Step 6: The binary value is converted to equivalent DNA code. TGAC TGTA TGTT ……..
Step 7: DNA code as the Cipher Text.

**Algorithm: 3-Decryption**

Cipher Text: TGAC TGTA TGTT ……..

Step 1: The cipher text is converted to binary equivalent
C=01100011 d= 01100100 e =01100101 ……..

Step 2: the Binary value is converted to hex value that is K=2,KV1 (cde lmn opu uvx def NMO QRS ABC YZA FGH)

Step 3: remove the key value with two positions (cloudNQAYF)

Step 4: separate the character value small case and upper case letters.
Character : cloud Numeric : NQAYG

Step 5: convert the upper case value into its numeric value.
NQAYG : 78 81 65 89 70

Step 6: merge the small case letters and upper case letters cloud 78 81 65 89 70

Step 7: Finally collect the original plain text.

Plain Text: cloud 78 81 65 89 70

This EUDSFDNA framework shows the data security algorithms under the DNA based data security algorithms. The data are stored in the cloud data servers based on their data either character, numerical and character numeric data. In this framework before getting the service from the CSP the user must register and gets the authorization. The user follows the authorization procedure.

**User Registration Procedure:**

Step 1: user registration process.

Step 2: set the password

Conditions

i: All letters in toggle case alphabets

ii: At least one numeric character with in that

iii: At least one special character it also in between the toggle letters

Iv: Password must minimum 10 characters at the maximum 18 characters.

Condition satisfied

Step 3: Proceed EUDSFDNA framework ( ) other wise

Step 4: Write (“incorrect password”) return

Step 5: Stop the Process

Step 6: End

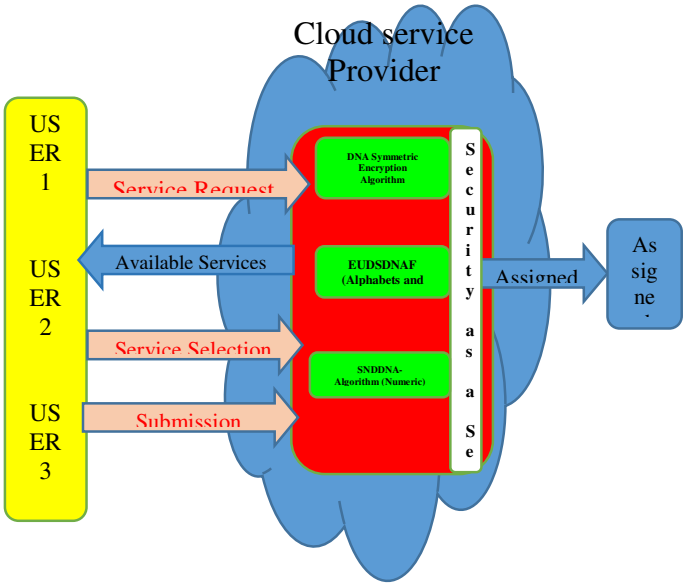


**Fig: EUDSFDNA framework for Cloud Environment.**

## VI. CONCLUSION

The proposed EUDSFDNA framework provide the cloud data security mechanisms in cloud computing environment. The Security and Privacy are important role in storing of data in that location. EUDSFDNA security framework allows cloud users to securely handle the privacy and integrity of data. Thus various scholars are work in that zone. DNA cryptographic systems are used to offer secure communication between the user and the cloud. This EUDSFDNA proposed framework based on encryption and decryption algorithm for secure data storage in cloud storage environment. The produced key performances as the key verification for the user. By means of applying this encryption and decryption algorithm, user guarantees that the data is put in storage only on secured storage and it cannot be retrieved by others.

## IV- References

[1] Mai Rady, Tamer Abdelkader, Rasha Ismail, “Integrity and Confidentiality in Cloud Outsourced Data”, Ain Shams Engineering Journal 10 (2019) 275–285, Received 2 April 2017, Revised 11 October 2018, Accepted 14 March 2019, Available online 4 April 2019.

[2] Manreet Sohal , Sandeep Sharma, “BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing”, Journal of King Saud University – Computer and Information Sciences journal homepage: www.sciencedirect.com. Received 26 April 2018 , Revised 19 September 2018, Accepted 28 September 2018.

[3] Imad El Ghoubach, Rachid Ben Abbou, Fatiha Mrabti, “A secure and efficient remote data

auditing scheme for cloud storage", Journal of King Saud University –Computer and Information Sciences journal homepage: www.sciencedirect.com, Received 8 October 2018, Revised 12 February 2019, Accepted 27 February 2019.

[4] Mbarek Marwan, Ali Kartit, Hassan Ouahmane, "Security Enhancement in Healthcare Cloud using Machine Learning", Procedia Computer Science 127 (2018) 388–397, Available online at www.sciencedirect.com. 2018.

[5] Ahmed Alrehaili, Aabid Mir, Mir Junaid, "A Retrospect of Prominent Cloud Security Algorithms", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ,ISSN: 2278-3075, Volume-9 Issue-3, January 2020.

[6] Manzamasso Kpelou, Keshav Kishore, "Lightweight Security Framework for Data Outsourcing and Storage in Mobile Cloud Computing", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, July 2019.

[7] B. Muthulakshmi, M.Venkatesulu, "Privacy and Security Aware Cloud Storage using Double Cryptography Method", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4S2, December 2019.

[8] Dr. D. Arivazhagan, R Kirubakaramoorthi, "Develop Cloud Security In Cryptography Techniques Using DES-3L Algorithm Method In Cloud Computing", international journal of scientific & technology research ,issn 2277-8616, volume 9, issue 01, january 2020.

[9] Dr. R. Sugumar, L. Leelavathy, "Ensure Data Security and Privacy using DNA Symmetric Encryption Method in Cloud", Journal of Information and Computational Science, Volume 10 Issue 3 – 2020, ISSN: 1548-7741 , Volume 10 Issue 3 – 2020.

[10] Prasanna Balaji Narasingapuram, M. Ponnavaikko, "DNA Cryptography Based User Level Security for Cloud Computing and Applications", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, January 2020.

[11] Heba El-Rahman Hassan, Mohamed Tahoun, Gh.S.ElTaweel, "A robust computational DRM framework for protecting multimedia contents using AES and ECC", , Alexandria Engineering Journal, www.elsevier.com/ locate/aej, www.sciencedirect.com, Received 8 January 2020; revised 13 February 2020; accepted 19 February 2020, Available online 2 March 2020.

[12] shaluMall , Sushil Kumar Saroj, "A New Security Framework for Cloud Data", Procedia Computer Science 143 (2018) 765–775, Available online at www.sciencedirect.com , 8th International Conference on Advances in Computing and Communication -ICACC-2018.

[13] Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar, and Allah Ditta, "Secure Framework Enhancing AES Algorithm in Cloud Computing", Hindawi Security and Communication Networks Volume 2020, Article ID 8863345, 16 pages https:// doi.org/ 10.1155/2020/ 8863345, Received 17 June 2020; Revised 4 August 2020; Accepted 7 August 2020; Published 1 September 2020.

[14] K. V. Pradeep,V. Vijayakumar,V. Subramaniyaswamy, "An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment", Hindawi Journal of Computer Networks and Communications Volume 2019, Article ID 9852472, 8 pages https://doi.org/10.1155/2019/9852472 , Received 18 February 2019; Revised 29 April 2019; Accepted 19 May 2019; Published 27 June 2019.

[15] Shadi A. Aljawarneh, Muneer Bani Yassein, "A Conceptual Security Framework for Cloud Computing Issues", International Journal of Intelligent Information Technologies Volume 12 • Issue 2 • April-June 2016.

[16] Savita A., Vasanth, "Security Framework for Cloud Computing using Fragmentation and Homomorphic Encryption", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019 .

[17] Victor Changa, Yen-Hung Kuob, Muthu Ramachandrana, "Cloud computing adoption framework: A security framework for business clouds", Contents lists available at Science Direct Future Generation Computer Systems journal homepage: www.elsevier.com/ locate/fgcs, Received 11 July 2015, Received in revised form, 9 September 2015 ,Accepted 27 September 2015 , Available online 19 October 2015 .

[18] Mouna Jouini, Latifa Ben Arfa Rabai, "A Security Framework for Secure Cloud Computing Environments", International Journal of Cloud Applications and Computing ,Volume 6 • Issue 3 • July-September 2016 .

[19] Sonali Chandel 1, Geng Yang , Sumit Chakravarty, "RSA-CP-IDABE: A Secure Framework for Multi-User and Multi-Owner Cloud Environment", Information 2020, 11, 382; doi:10.3390/info11080382 www.mdpi.com /journal/ information, Received: 23 June 2020; Accepted: 20 July 2020; Published: 29 July 2020

[20] Vanaja Malgari, Raman Dugyala, Ashwani Kumar, "A Novel Data Security Framework in Distributed Cloud Computing", 2019 Fifth International Conference on Image Information Processing (ICIIP) , 2019.

[21] L. ArockiamÀ , S. MonikandanḂ, "Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage", 1265 | International Journal of Current Engineering and Technology, Vol.4, No.3 ,June 2014.

[22] Rajendra Patil ∗, Harsha Dudeja , Chirag Modi, "Designing an efficient security framework for detecting intrusions in virtual network of cloud computing", Available online at www.sciencedirect.com, journal home page : www . elsevier . com / locate / cose, computers & security 85, 4 0 2 – 4 2 2 , 2019.

[23] G. Viswanath, P. Venkata Krishna, "Hybrid encryption framework for securing big data storage in multi-cloud environment" , Evolutionary Intelligence, https://doi.org/ 10.1007/s12065-020-00404-w , Received: 13 January 2020 / Revised: 28 February 2020 / Accepted: 6 April 2020, © Springer-Verlag GmbH Germany, part of Springer Nature 2020.

[24] L. Leelavathy, Dr. Ramalingam Sugumar, "SNDDNA: Secure Numerical Data using DNA Cryptography Method in Cloud Computing Environment", Mukt Shabd Journal, ISSN NO : 2347-3150 ,Volume IX, Issue IX, SEPTEMBER/2020.