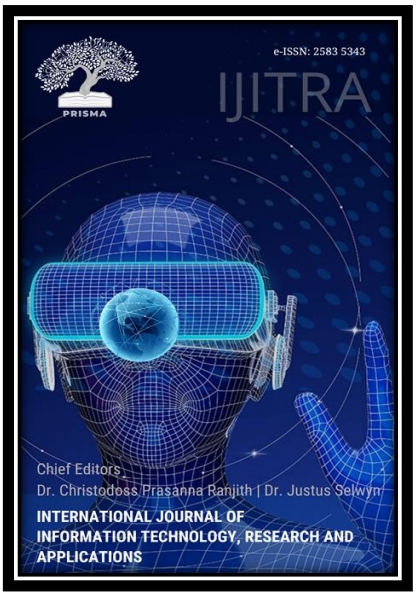

International Journal of Information Technology, Research and Applications (IJITRA)

Kalvikkarasi S, Dr.Saraswathi A.
An Empirical study of Hybrid Cryptographic Algorithms. International Journal of Information Technology, Research and Applications, 2(1), 22-32.

ISSN: 2583-5343

DOI: 10.59461/ijitra.v2i1.50

The online version of this article can be found at:
https://www.ijitra.com/index.php/ijitra/issue/archive

Published by:
PRISMA Publications

International Journal of Information Technology, Research and Applications (IJITRA) is a journal that publishes articles which contribute new theoretical results in all the areas of Computer Science, Communication Network and Information Technology. Research paper and articles on Big Data, Machine Learning, IOT, Blockchain, Network Security, Optical Integrated Circuits, and Artificial Intelligence are in prime position.

PRISMA
PUBLICATIONS

https://www.prismapublications.com/

An Empirical study of Hybrid Cryptographic Algorithms

Kalvikkarasi S[1], Dr.Saraswathi A[2]
[1]PG and Research department of Computer Science, Government Arts College, Trichy-22,India.
[2]PG and Research department of Computer Science, Government Arts College, Karur-5, India.

Article Info

Article history:

Received October 29, 2022
Revised November 15, 2022
Accepted November 17, 2022

Keywords:

Cloud computing
Cloud security
Cryptography
Encryption
Decryption

ABSTRACT

For the last few decades' cloud computing is a blooming word in the field of computer science. Cloud computing is a fast growing technology; it provides various services to the user through internet on demand. Now a days, people in busy move, they use Cloud to store and retrieve data at anywhere, any time without use of any physical storage devices like pen drive, compact disc etc. Enormous features of cloud, most of the small and large scale organizations outsource their data in cloud data storage. With the widespread application of cloud, huge amount of users is incorporated in public cloud, it may lead to vulnerable attacks. So security and privacy is an important factor in cloud environment. This security problem can be solved by various ways. Cryptography is one of the techniques to secure user data in cloud. Researchers can use various cryptographic algorithms to implement the security in cloud storage. This paper focuses the summative analysis of researches, in cloud security from 2018-2022. This survey paper provides solution to researchers who have their work in cloud.

Corresponding Author:

Kalvikkarasi S
PG and Research Department of Computer Science,
Government Arts College,
Trichy-22,
India.
Email: kalvijaya2022@gmail.com

I. INTRODUCTION

Cloud refers to storing the user's data in a remote database instead of storing it in the hard disk of their own computer. Cloud delivers computing resources as a service in a scalable manner to the clients by means of Internet which eliminates the need of setting up company's own data center or server. These resources are offered on demand and customers pay for their level of usage [1]. Cloud computing uses various existing technologies in parallel, distributed, grid and utility computing. It provides different services to the cloud user on demand basis using internet. Cloud service provider offers Infrastructure, software, platform, databases and everything as a service. The advantages of using cloud computing includes on demand service, multi tenancy, rapid elasticity, resource pooling, scalability, virtualization, flexibility, cost saving and availability. Based on the deployment model cloud can be classified as public, private, hybrid and community cloud. Public Cloud can be accessed by any user with an internet connection. Example: Amazon, windows azure. Private Cloud can be accessed by single person or multiple persons in the same organization. Most of the organizations and government sectors prefer private cloud for their usage. Example: windows server hyper-v. Community cloud represents two or more companies in the same policies and procedure to share their infrastructure, resources and other capabilities. Combination of private, public and/or community cloud are referred to as hybrid cloud. Cloud service provider provides various services to the cloud user, that can be modeled as Infrastructure as a service, Platform as a service, Software as a service. Cloud works with

virtualization and distributed network environment; it is very difficult to maintain privacy and confidentiality of user data. Cryptography is one of the solutions to achieve security.

Cryptography

Cryptography technique translates original data into unreadable form [2]. It focuses on securing the user data by applying some encryption and decrypting methods that makes the cryptosystem. It uses mathematical algorithms to provide information security. Cryptographic techniques are mainly classified as (i) Symmetric key (ii) Asymmetric key. Same key used for both encryption and decryption, is referred to as symmetric or secret or private key crypto systems. Asymmetric crypto systems use public key for encryption process, private key for decryption process. It provides high level security but it increases the time to data encode and decode. Both the encryption and decryption in the presence some extra input called as key. Hybrid Cryptography exploits the combination of symmetric and asymmetric cryptosystem. It uses the efficiency of symmetric and simplicity of asymmetric.

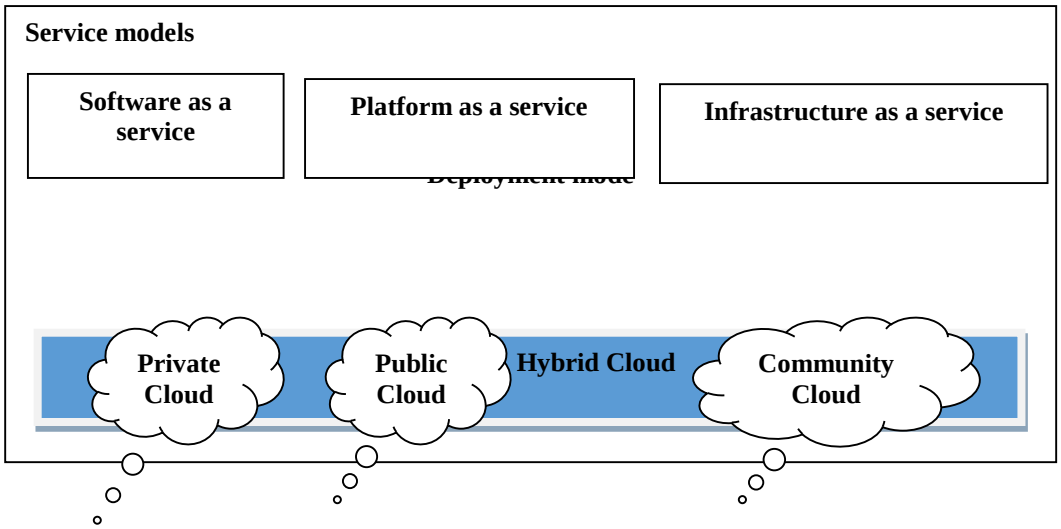

Fig 1 : Cloud Service and Deployment Model Framework

II. RELATED WORKS

To reduce the malicious attacks in cloud, several researches have focused for various algorithms; out of these, few outcomes are presented here.

Neenu Garg,Seema Bawa,Neeraj Kumar[2020] Discussed Bilinear pairings, BLS-based homomorphic verifiable authenticator and the computational Diffie Hellman Problem. Performing various experiments to implement the protocol and the results have been compared with state of the art protocol, and high efficiency by clients with limited resources.

Anil Gupta,Dr.Meghna Dubey,Dr.Durgesh Kumar Mishra[2021] presented a hybrid secure framework for health care application. Patient information is divided in to odd chunks and even chunks, even chunks are decrypted using ECC. Blowfish are used to decrypt odd chunks. Confidentiality can be achieved by using combination of Role based Access control and Attribute Based Access Control.

Roshan Jahan, Preetam Suman, Deepak Kumar Sin gh[2021] introduced an Algorithm to Secure Data for Cloud Storage, in this, it takes plaintext as 1024 bits. Divided into 8 sub blocks of 128 bits, added to key block, generate random key AES Process. Bit positions are changed by using Replacement table, it is stored in 2D Matrix to calculate the step key value, perform 10 iterations to get cipher text.

Deepika Bhatia and Meenu Dave [2021] build Elliptic Curve Layered: A Secure Polyalphabetic Vignere Cryptographic Algorithm for Textual Data, Combination of Vignere cipher and ECC is used. Double layer security is provided. It is cost Effective, implemented in smart IoT and wireless devices.

Dr.M.Navaneetha Krishnan, Mr.T.Tamilarasan[2021] depicted a hybrid approach to Secure File Storage on Cloud. Blowfish algorithms are used to encrypt a files, and key generation done by using DES Algorithm. This System is implemented using JAVA and mySql.

Md. Abdullah Al Hasan and Md. Alamgir Hossain presented a new user verification model to prevent data access by unauthorized user in cloud framework . It uses finger print for biometric authentication and AES algorithm for encryption. It mainly focused by unapproved clients.

Kulsum subiya and others [2022] build a biometric authentication method to secure data in cloud server. It generates a session key that communicates between two biometric templates. In this model implemented with Moodle e-learning platform. Several analyses can be applied to the model to prove the effectiveness of the system.

III. METHODOLOGY

There are 2 ways of implementing hybrid cryptographic schemes.

- Using Symmetric key to encrypt the plaintext and using Asymmetric key to encrypt the secret key value.
- Double layer encryption – plaintext is encrypted by symmetric key, and then the resulted text is once again encrypted by asymmetric key.

  Many researchers apply hybrid cryptography to achieve security in cloud. We have listed the different models with merits and demerits.

Table 1. Techniques and its Advantages & Disadvantages of several survey papers

Auth.Name& Year	TITLE	ALGORITHMS USED	MERITS	DEMERITS
1.Smitha Nisha Mendonca [2018]	Data Security in Cloud using AES	Symmetric - AES Algorithm used	A Physical key management server is installed in the user's location to provide key security	Server takes extra cost

2. BinduBala,Lovejeet Kamboj, Paean Luthra [2018]	Secure File Storage on Cloud using Hybrid Cryptography Algorithms	Block wise data security is provided by using AES,Blowfish,RC6 and BRA Algorithm, and also LSB Stenography technique is introduced for storing key information	It concentrates on text files only.	It uses algebraic structure, the block is encrypted in the same method
3. Joseph Selvanayagam,AkashSingh,Joansmichael, Jaya Jeswani [2018]	Secure File Storage on Cloud using Cryptography	DES, AES, and RC4 Algorithms are used.	In DES plaintext is divided into two parts before the main algorithm begins whereas, in AES the entire block is processed. RC4 uses a little amount of RAM and is extremely fast.	*RC4* stream ciphers support large data streams only.
4. SwarnaC,MarrynalS.Eastaff [2018]	Secure File Storage in Cloud computing using Hybrid Cryptography Algorithm	Blowfish and modified RSA (SRNN) were used.	The proposed system is tested with various types of file audio, image,text, word,PDF files. And also modified RSA algorithm increased security	This model provides security on data as a service model only
5. Bin-hwaang Lee [2018]	Data Security in Cloud Computing using HEROKU Cloud	AES algorithm is used under HEROKU Cloud	The result of the encrypted data is in the form of symbols we cannot normally interpret.	Large file size, it takes more time, to encrypt.

6.Vartika Kulshrestha, Prof.SeemaVerma,Prof.C.Rama Krishna [2018]	Security Concerns & cryptography in Cloud Computing	Combine Double asymmetric encryption with hash technique. 4 prime numbers can be used.MD5 is used to hash the generated keys. The proposed system is tested in Ubuntu.	Achieve key accountability and information confidentiality	File size increases, it also increases the encryption and decryption time.
7.Salma,Rashidah FunkeOlanrewaju,Khaizuran Abdullah and more [2018]	Enhancing Cloud Data Security using Hybrid of AES and Blowfish Encryption Algorithm	DAES algorithm followed by Blowfish	The proposed method slightly changes the s-box structure to obtain more security does not break by brute force and algebraic attack.	Practical implementation and results are not shown
8. Mehulbatra,PrayasDixit,LalitRawat,RohiniKhalkar [2018]	Secure File Storage in Cloud computing using Hybrid encryption algorithm	RC4, AES, DES, and Steganography Algorithms used.	The Algorithm takes less time for encryption and decryption because algorithms can be executed concurrently. (ii) Confidentiality, Data Integrity, and authentication are achieved.	RC4 is vulnerable, non-random/related keys are used.
9. S Lei [2018]	Research and design of Cryptography cloud framework	Virtual cryptographic machineframework used	VCM does not have much loss on transfer mechanism, and can achieve the cryptography service which is bytes are	The aspect of virtual network transmission mechanism, there is still issues to improve.

			encrypted by AES, the encryption speed of VCM would be little slower than that of Host, but the quality of service can't be reduced	
10. Rohini,Tejindersharma [2018]	Proposed Hybrid RSA algorithm for cloud computing	Encrypt and decrypt the data by using RSA with HMAC.	Encrypt and decrypt the data by using RSA with HMAC.	Adequate security - MD5
11. Mr.RohitBarvekar,Mr.ShrajalBehere,Ms. AnushkaGulhane [2018]	An Approach to Hybrid Cryptography on Cloud Environment	Using the upload module the encrypted file is stored in the cloud as well as download module helps to download the decrypted file from the server.	Prevent Confidential data misuse.	It is an abstract model, so it does not provide implementation details.
12. Smita Sharma, R.P. Singh [2019]	The Cryptography Based Security Algorithm For Protecting Sensitive Information in Cloud Environment	Symmetric Algorithm takes 128 bits of plain text, arranged in the form of the matrix. After arranging data matrix operations such as transpose, column mixing, and row mixing are performed. Key values are taken and again matrix operation is performed. Different key values are used at different levels to produce secure cipher text.	(i)Proposed key is 128 bits which is larger; this will enhance the security aspect of this algorithm and make them more secure than other encryption Algorithms. ii)There is no constraint that only one key which is providing	Encryption and Decryption focus on text files only.

			simple structures. (iii) Key having 16 rounds it is also increasing security.	
13. Aditya Poduval,AbhijeetDoke,HiteshNemade,RohanNikam [2019]	Secure File Storage on Cloud using Hybrid Cryptography	Rc6, 3DES, and AES are used to provide data security. Key information is stored by using LSB Steganography.	Key information is stored in image steganography, it is more secure, difficult to break by the intruder.	Sometimes image steganography distortion of the image produces little changes in the user profile.
14. K.V.PradeepV.Vijayakumar, V. Subramaniyaswamy [2019]	An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment	Modified Diffie–Hellman distribution of keys is used to encrypt and decrypt the data or files which are stored in a cloud in a secured manner.	RSA consumes less time for encryption and ElGamal consumes less time for the decryption process. ElGamal is usually slower than symmetric ones for the same level of security, so it is faster to encrypt the symmetric key with ElGamal.	RSA has limitations while handling the largefile (byte) which consumes more resource utilization.
15. PrasannaBalajiNarasingapuram,M.Ponnavaiko [2020]	DNA Cryptography Based User Level Security for Cloud Computing and Applications	DNA can be used to store and transmit data.Biological information is represented as DNA Molecules and is coded using AGCT (A-Adenine,C-Cytosine,G-	This DNA takes less time complexity compared with elliptic curve cryptography and hyper	A strongly authentic, encrypt, and digitally signed information is very difficult to access

		Gunaninr,T-Thymine letters).	elliptic curve cryptosystem is more secure.	legitimate users.
16.Ahmed Alrehaili, AabidMir,Mir Junaid [2020]	A Retrospect of Prominent Cloud Security Algorithms	AES, RSA and Triple DES Algorithms are used separately.	The Efficiency of different algorithms is tested locally as well as the google app engine cloud. Cloud encryption takes less time in AES, and 3DES Algorithms.	When the file size increases the execution time of the RSA algorithm takes more.
17.Dr.D.Arivazhagan,R.Kirubakaramoorthi [2020]	Develop Cloud Security in Cryptography Techniques using DES-3L Algorithm Method in Cloud Computing	DES(Three Level Algorithm) - Byte Insertion Encryption Method is used.	Byte insertion Encryption in DES is more secure and reliable.	The 56-bit key is too short. Using brute-force search it is vulnerable.
18. NeenuGarg,SeemaBawa,Neeraj Kumar [2020]	An efficient data integrity auditing protocol for cloud computing	Discussed Bilinear pairings, BLS-based homomorphic verifiable authenticator, and the computational Diffie- Hellman Problem. The Protocol is executed in two phases. Setup phase and Verification phase.	This protocol performs better where the size of the outsourced data is very big.	The challenged block number increases, it also increases the communication overhead in the challenge phase.

19. Punam S Patil, Mohini R Chaudhari, Sagar U More [2021]	Cloud based Secure File Storage using Hybrid Cryptography Algorithms	Provides block-wise data security by using AES,DES and RC2 Algorithms. By securing Key information Steganographytechnique is used.	AES supports 112 or 168 bits.AES algorithms faster in both hardware and software.	Sometimes image steganography distortion of the image is produced
20. Reece B.D.Souza,Dr.D.Ruby [2021]	Secure File Storage on Cloud using Enhanced Hybrid Cryptography	AES algorithm is enhanced by using threads.RSA Algorithms are used for signing and verification purposes	Enhanced AES runs faster than traditional AES.	There are still many issues to improve
21. Anil Gupta,Dr.MeghnaDubey,Dr.Durgesh Kumar Mishra [2021]	Design & Implementation of Enhanced Security Architecture to Improve Performance of Cloud Computing	RC6 And Bowfish as Symmetric cryptography, ECC and RSA Asymmetric Cryptography used.	By implementing this approach, security parameters 3A'S are achieved.	It takes little computation time, it is suited for the applications like Military, Health care, and banking sector.
22. Roshan Jahan, Preetam Suman, Deepak Kumar Singh [2021]	An Algorithm to Secure Data for Cloud Storage	The plaintext is converted into ASCII code by using the vignere cipher. The cipher text is once again encrypted by using ECC.	It takes less time compared to other RSA,AES and Blowfish	File size increases, Execution time also increases.
23. Deepika Bhatia and Meenu Dave [2021]	Elliptic Curve Layered : A Secure Polyalphabetic Vignere Cryptographic Algorithm for Textual Data	The proposed approach is tested by using the fried man test and index of coincidence.	Data authentication, Integrity, and Confidentiality.	Cost-Effective, implemented in smart IoT and wireless devices.

24. Md. Abdullah Al Hasan and Md. Alamgir Hossain[2022]	Improving cloud data security through hybrid verification technique based on biometrics and encryption system	It uses the minutiae extraction algorithm to extract cloud user biometric samples. And also authentication server generate OTP , send to the authorized user.	It takes less time and get more security	Cryptanalytic attack happens when AES key not employed properly.

IV. CONCLUSION

Cloud computing is an emerging technology for IT enterprise. With significant popularization of cloud, most of the business organizations that utilizes the cloud. It eliminates the requirements for infrastructure set up cost. It provides easy access with the help of internet or web services. But still now, vulnerable attacks happen day to day. This paper explores various risk associated in cloud security are discussed and also provide solutions for the various researcher aspect. Each algorithm has some merits and demerits. In future we aim to overcome the drawback of the existing algorithms to enhance the performance of the cloud in security aspects.

V. REFERENCES

[1] Smitha Nisha Mendonca (2018), "Data Security in Cloud using AES" *International Journal of Engineering Research & Technology (IJERT)* Volume 7,Issue 1 .

[2] Bindu Bala,Lovejeet Kamboj, Paean Luthra (2018) "Secure File Storage on Cloud using Hybrid Cryptography Algorithms" *International Journal of Advanced Research in Computer Science* Vol9,No.2.

[3] Joseph Selvanayagam etc (2018) "Secure File Storage on Cloud using Cryptography" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03

[4] Swarna C,Marrynal S.Eastaff (2018) "Secure File Storage in Cloud computing using Hybrid Cryptography Algorithm" IAETSD *Journal for Advanced Research in Applied Sciences* ISSN NO:2394-8442.

[5] Bin-hwaang Lee (2018) Data Security in Cloud Computing using HEROKU Cloud *The 27th Wireless and Optical Communications Conference* (WOCC2018) 978-1-5386-4959-6/18 IEEE

[6] Vartika Kulshrestha, Prof.Seema Verma,Prof.C.Rama Krishna, "Security Concerns & Cryptography in Cloud Computing" *IJRECE* Vol.6 Issue 3,ISSN:2393-9028

[7] Salma,Rashidah Funke Olanrewaju,Khaizuran Abdullah and more (2018), Enhancing Cloud Data Security using Hybrid of AES and Blowfish Encryption Algorithm *2nd East Indonesia Conference on Computer and Information Technology*.

[8] Mehul batra,Prayas Dixit,Lalit Rawat,Rohini Khalkar (2018) " Secure File Storage in Cloud computing using Hybrid encryption algorithm" *International Journal of Computer Engineering and Applications,*Volume XII,Issue VI,June 2018,www.ijcea.com ISSN 2321-3469.

[9] Lei(2018) Research and design of Cryptography cloud framework *IEEE 3rd International Conference on Cloud Computing and Big Data Analysis* .

[10] Rohini,Tejinder Sharma (2018) Proposed Hybrid RSA algorithm for cloud computing Proceedings of the second *International Conference on Inventive Systems and Control (ICISC 2018)* IEEE Xplore,ISBN:9781-1-5386-0807-4.

[11] Mr.Rohit Barvekar,Mr.Shrajal Behere,Ms.Anushka Gulhane (2018) "An Approach to Hybrid Cryptography on Cloud Environment" *IJARIIE*-ISSN(O)-2395-4396 Vol-4 Issue-2 2018.

[12] Smita Sharma, R.P. Singh (2019) " The Cryptography Based Security Algorithm For Protecting Sensitive Information in Cloud Environment" *International Journal of Scientific & Technology Research* Volume 8, Issue 11,Nov 2019 ISSN 2277-8616.
[13] Aditya Poduval,Abhijeet Doke,Hitesh Nemade,Rohan Nikam (2019) " Secure File Storage on Cloud using Hybrid Cryptography" *International Journal of Computer Science and Engineering*
[14] Prasanna Balaji Narasingapuram,M.Ponnavaiko (2020) "DNA Cryptography Based User Level Security for Cloud Computing *and Applications*" *IJRTE*, ISSN:2277-3878,Volume-8 Issue-5.
[15] Ahmed Alrehaili, Aabid Mir,Mir Junaid (2020) "A Retrospect of Prominent Cloud Security Algorithms" *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* ISSN:2278-3075,Volume-9 Issue-3.
[16] Dr.D.Arivazhagan,R.Kirubakaramoorthi (2020) "Develop Cloud Security in Cryptography Techniques using DES-3L Algorithm Method in Cloud Computing" *International Journal of Scientific and Technology Research* Volume 9,Issue 01.
[17] Neenu Garg,Seema Bawa,Neeraj Kumar (2020) " An efficient data integrity auditing protocol for cloud computing" *Future Generation Computer Systems* Elsevier .
[18] Anil Gupta,Durgesh Kumar Mishra (2020) "Implementation of Different Cryptographic Strategies in Cloud Environment" *International Journal of Recent Technology and Engineering (IJRTE)* ISSN:2277-3878, Volume-8 Issue-5, Jan 2020
[19] Nagesh Shenoy H,K.R.Anil Kumar,Suchitra N Shenoy,Abishek S.Rao (2020) "Data Security in Cloud Environment Based on Comparative Performance Evaluation of Cryptographic Algorithms" *IJATCSE* ISSN 2278-3091,Vol 9,No.4,July-August 2020.
[20] Punam S Patil, Mohini R Chaudhari, Sagar U More (2020) " Cloud based Secure File Storage using Hybrid Cryptography Algorithms" *International Research Journal of Modernization in Engineering Technology and Science* Vol.3/Issue:01.
[21] Reece B.D.Souza,Dr.D.Ruby (2021) "Secure File Storage on Cloud using Enhanced Hybrid Cryptography" *International Research Journal of Engineering and Technology (IRJET)* e-ISSN: 2395-0056 Volume: 08 Issue: 03 | Mar 2021
[22] Anil Gupta,Dr.Meghna Dubey,Dr.Durgesh Kumar Mishra (2021) "Design & Implementation of Enhanced Security Architecture to Improve Performance of Cloud Computing" *Journal of University of Shanghai for Science and Technology* ISSN:1007-673, Volume 23,Issue-3, March-2021.
[23] Roshan Jahan, Preetam Suman, Deepak Kumar Singh (2021) "An Algorithm to Secure Data for Cloud Storage" *IT in industry*, Vol.9,No.1,2021
[24] Deepika Bhatia and Meenu Dave (2021) "Elliptic Curve Layered : A Secure Polyalphabetic Vignere Cryptographic Algorithm for Textual Data" *Journal of Scientific Research, Institute of Science* , Banaras Hindu University, Varanasi Volume 65, Issue 1.
[25] Felix Bentil,Isaac Lartey (2021) "Cloud Cryptography - A Security Aspect" *International Journal of Engineering Research & Technology (IJERT)* ISSN: 2278-0181 Vol.10 Issue-05,May-2021.
[26] Md. Abdullah Al Hasan and Md. Alamgir Hossain(2022) "Improving cloud data security through hybrid verification technique based on biometrics and encryption system" International Journal of Computers and Applications Volume 44, 2022 - Issue 5,2022.
[27] Kiran Jain(2022) "An Approach to Biometric Encryption in Cloud Computing" Appl ied Science & Engineering Journal for Advanced Research ISSN (Online): 2583-2468 Volume-1 Issue-4 July 2022.
[28] Kulsum subiya, Dr. MD.Sirajuddin,Dr.Chandramouli Narsingoju, Dr. Gulab Singh " Enhanced Secuirty schemes in Cloud using Biometric based Access" Dogo Rangsang Research Journal ISSN : 2347-7180 Vol-09 Issue-01 No. 01 : 2022