

# 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: <a href="https://www.ijitra.com/index.php/ijitra/issue/archive">https://www.ijitra.com/index.php/ijitra/issue/archive</a>

Published by: PRISMA Publications

IJITRA is an Open Access publication. It may be read, copied, and distributed free of charge according to the conditions of the Creative Commons Attribution 4.0 International license.

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.

https://www.prismapublications.com/

#### ISSN: 2583-5343

# An Empirical study of Hybrid Cryptographic Algorithms

Kalvikkarasi S<sup>1</sup>, Dr.Saraswathi A<sup>2</sup>

<sup>1</sup>PG and Research department of Computer Science, Government Arts College, Trichy-22,India. <sup>2</sup>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.

This is an open access article under the CC BY-SA license.



# 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 ISSN: 2583-5343

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.

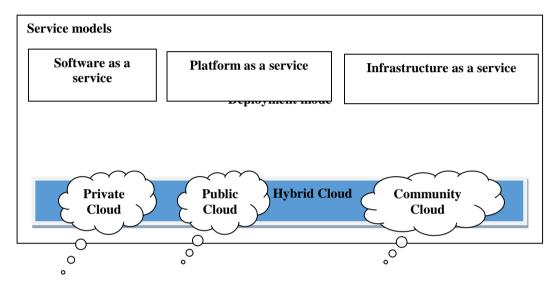


Fig 1: Cloud Service and Deployment Model Framework

# 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.

Auth.Name& Year	TITLE	ALGORITHMS USED	MERITS	DEMERI TS
1.Smitha Nisha Mendonca [2018]	Data Security in Cloud using AES	Symmetric - AES Algorithm used	A Physical key manageme nt 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 Cryptograp hy Algorithms	Block wise data security is provided by using AES,Blowfish,R C6 and BRA Algorithm, and also LSB Stenography technique is introduced for storing key information	It concentrat es 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 Cryptograp hy	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 Cryptograp hy 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.

Prof. Seema Verma, Prof. C. Rama Krishna [2018]   Concerns & encryption with cryptograph by in cloud Computing in the generated keys. The proposed system is tested in Ubuntu.   DatEs algorithm clower of the proposed system is tested in Ubuntu.   The proposed system is tested in Ubuntu.   DatEs algorithm clower of the proposed system is tested in Ubuntu.   The proposed system is tested in Ubuntu.   The proposed system is tested in Ubuntu.   DatEs algorithm clower of the proposed system is tested in Ubuntu.   The proposed method slightly changes the s-box structure to obtain more security does not break by brute force and algebraic attack.   RC4 is Algorithms used.   Al	6.Vartika Kulshrestha,	Security	Combine Double	Achieve	File size
Cryptograp hy in prime numbers Cloud Computing can be used. MD5 is used to hash the generated keys. The proposed system is tested in Ubuntu. DAES algorithm FunkeOlanrewaju, Khaizuran Abdullah and more [2018]   Enhancing Cloud Data Security using Hybrid of AES and Blowfish Encryption Algorithm   Storage in ikhalkar [2018]   Secure File Mehulbatra. Prayas Dixit, LalitRawat, Rohin ikhalkar [2018]   Secure File Mehulbatra. Prayas Dixit, LalitRawat, Rohin algorithm   Storage in ikhalkar [2018]   Secure File Mehulbatra. Prayas Dixit, LalitRawat, Rohin algorithm   Storage in ikhalkar [2018]   Secure File Storage in ikhalkar [2018]   Secure File Mehulbatra. Prayas Dixit, LalitRawat, Rohin algorithm   Storage in ikhalkar [2018]   Secure File Storage in Cloud algebraic attack.   Storage in Cloud algorithm sused.   Secure File Algorithms used.   Secure Fil	The state of the s				
Ny in   Cloud Computing   Security using Hybrid of AES and Blowfish using Hybrid encryption algorithm   Security using Hybrid encryption algorithm   Stepanography Algorithms used.   Majorithm   Stepanography Algorithms used.   Majorithm   Stepanography Algorithms used.   Majorithm   Stepanography   Algorithms used.   Majorithm   Stepanography   Algorithms used.   Majorithm   Stepanography   Algorithms used.   Majorithm	[2018]				
Cloud Computing is used to hash the generated keys. The proposed system is tested in Ubuntu.  7.Salma,Rashidah FunkeOlamewaju,Khaizuran Abdullah and more [2018]  8. Security using Hybrid of AES and Blowfish Encryption Algorithm  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm  8. Secure File Storage in Cloud Computing using Hybrid encryption algorithm  9. S Lei [2018]  8. Research and design of Cryptograph by Cloud framework Physical and authenticat in a rachieved.  9. S Lei [2018]  8. Research and design of cryptograph by cloud framework Physical and authenticat in a rachieved.  9. S Lei [2018]  8. Research and design of cryptograph by cloud framework Physical and active the cryptograph by cloud framework Physical and active the cryptograph by service which is still issues by still issues to improve.					
7.Salma,Rashidah FunkeOlanrewaju,Khaizuran Abdullah and more [2018]  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iRhalkar [2018]  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin algorithm  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin algorithm  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iRhalkar [2018]  8. Secure File Month algorithm  9. S Lei [2018]  8. Secure File Month algorithm  8. Secure File Month algorithm  9. S Lei [2018]  8. Secure File Month algorithm  1. The proposed method slightly changes the s-box structure to obtain more security does not break by brute force and algebraic tack.  8. RC4, AES, DES, algorithms used. using Hybrid encryption algorithms used. using Hybrid encryption algorithm  1. The proposed method slightly changes the s-box structure to obtain more security does not break by brute force and algebraic time for encryption and decryption algorithm falses less time for encryption and decryption algorithm takes less time for encryption and decryption and authentel inity algorithm takes less time for encryption and decryption and decryption and decryption and authentel in the served implement action and results in proposed implement action and results reach reach of encryption and decryption and decryption and decryption and authentel in proposed in pro					
7.Salma,Rashidah FunkeOlamewaju,Khaizuran Abdullah and more [2018]  8.					
7.Salma,Rashidah FunkcOlanrewaju,Khaizuran Abdullah and more [2018]  8.		Companing			
7.Salma,Rashidah FunkcOlamewaju,Khaizuran Abdullah and more [2018]  8. Security using Hybrid of AES and Blowfish Encryption Algorithm  Security does not break by brute force and algebraic attack.  8. Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Menulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm  9. S Lei [2018]  8. Research and design of Cryptograp hy cloud framework  8. Witual authenticat ion are achieved.  9. S Lei [2018]  9. S Lei [2018]  8. Research and design of framework  8. RC4. AES, DES, Algorithm Steganography Algorithms used. decryption and decryption and authenticat ion are achieved.  9. S Lei [2018]  8. RC4. AES, DES, Algorithm Steganography Algorithms used. decryption and decrypt			keys. The		
Salma,Rashidah   Enhancing FunkcOlanrewaju,Khaizuran Abdullah and more [2018]   Enhancing FunkcOlanrewaju,Khaizuran Abdullah and more [2018]   Enhancing FunkcOlanrewaju,Khaizuran Abdullah and more [2018]   Enhancing FunkcOlanrewaju,Khaizuran Abdullah Security using Hybrid of AES and Blowfish Encryption Algorithm   Encryption   Encryption algorithm   Encryption   Encryption   Encryption   Encryption   Encrypt					
7.Salma,Rashidah FunkoOlanrewaju,Khaizuran Abdullah and more [2018]  8.					
FunkeOlanrewaju,Khaizuran Abdullah and more [2018]  Security using Hybrid of AES and Blowfish Encryption Algorithm  8.  Mehulbatra,PrayasDixit,LalitRawat,Rohini iKhalkar [2018]  Secure File Cloud Compute and algorithm algorithm  Secure File Storage in iCloud computing using Hybrid encryption algorithm  Secure File Storage in iCloud computing using encryption algorithm  Storage in Cloud computing using encryption algorithm  Storage in Cloud computing using encryption algorithm  Storage in Cloud Computing using encryption algorithm ality, Data Integrity, and authenticat ion are achieved. The and design of cryptography of computing of framework encryption and design of framework encryption and design of cryptography by cloud framework encryption and design of cryptographic machiner mechanism in the cryptography by service which is still issues to improve.	7 Colmo Doshidah	Enhancina		The	Descriped
and more [2018]  Security using Hybrid of AES and Blowfish Encryption Algorithm  8.  Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin algorithm  Storage in Cloud computing using Hybrid encryption algorithm  Storage in Cloud computing using Hybrid encryption algorithm  Steganography can be executed concurrently, (ii) Confidentia ality, Data Intregrity, and authenticat ion are achieved.  Secure File Storage in Cloud computing using Hybrid encryption algorithm  Steganography can be executed concurrently, (ii) Confidentia ality, Data Intregrity, and authenticat ion are achieved.  Secure File Storage in Cloud computing using Hybrid encryption algorithms can be executed concurrently, (ii) Confidentia ality, Data Intregrity, and authenticat ion are achieved.  Storage in Cloud computing using Hybrid encryption algorithms can be executed concurrently, (ii) Confidentia ality, Data Intregrity, and authenticat ion are achieved.  Storage in Cloud computing using Hybrid encryption algorithms can be executed concurrently, (ii) Confidentia ality, Data Intregrity, and authenticat ion are achieved.  Storage in Cloud decryption because algorithms can be executed concurrently, (ii) Confidentia ality, Data Intregrity, and authenticat ion are achieved.  Storage in Cloud decryption and decryption and decryption and authenticat ion are achieved.  Storage in Cloud decryption and decryption and decryption and algorithms can be executed concurrently of virtual authentication are achieved.  Storage in Cloud decryption because algorithms can be executed concurrently of virtual authentication are achieved.  Storage in Cloud decryption because algorithms can be executed concurrently of virtual authentication are achieved.  Storage in Cloud decryption because algorithms can be executed concurrently of virtual authentication are achieved.  Storage in Cloud decryption because algorithms can be executed concurrently of					
using Hybrid of AES and Blowfish Encryption Algorithm   Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]   Research and Gencryption algorithm   Steganography (computing using Hybrid encryption algorithm   Algorithm sused.   Algorithm stakes less time for encryption and decryption because algorithms can be executed concurrently, (ii)   Confidential alitty, Data Integrity, and authenticat ion are achieved.   VCM does rot have machineframewo for cryptography cloud framework   VCM does rot have machineframewo for thave machineframewo for thave machineframework rot private the cryptography service which is still issues to improve.   The aspect of virtual mechanism achieve the cryptography service which is still issues to improve.					
AES and Blowfish Encryption Algorithm  8.  8.  Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Cecure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. RC4, AES, DES, and algebraic attack.  8. Cloud Computing using Hybrid encryption algorithm  8. Algorithms used.  9. S Lei [2018]  8. Research and design of Cryptograph of Cryptograph hy cloud framework  9. S Lei [2018]  8. Research and design of Cryptograph hy cloud framework  8. RC4 is vulnerable, and algorithms used.  8. RC4 is Algorithm takes less time for encryption and decryption because algorithms can be executed concurrently. (ii) Confidenti ality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  8. Research and design of Cryptograph hy cloud framework hy cloud framework which is vinner for encryption and authenticat ion are achieved.  9. S Lei [2018]  8. RC4, AES, DES, and Algorithm used.  9. S Lei [2018]  8. RC4 is Vulnerable, and algebraic attack.  8. RC4 is vulnerable, onco-rencryption and authenticat ion are achieved.  9. S Lei [2018]  8. RC4, AES, DES, and Algorithm used.  9. S Lei [2018]  8. RC4 is Vulnerable, and authenticat ion are achieved.  9. S Lei [2018]  8. RC4 is Vulnerable, and algebraic attack.  8. RC4 is Vulnerable, and algerithm takes less time for encryption and authenticat ion are achieved.  9. S Lei [2018]  8. RC4, AES, DES, and Algorithm used.  9. S Lei [2018]  8. RC4 is Vulnerable, and algerithm takes less time for encryption and authenticat ion are achieved.  9. S Lei [2018]  8. RC4 is Vulnerable, and algerithm takes less time for encryption and authenticat ion are achieved.  9. S Lei [2018]  9. S Lei [2018]  1. Integrity, and authenticat ion are achieved.  9. S Lei [2018]  1. Integrity, and authenticat ion are achieved.  9. S Lei [2018]  1. Integrity, and authenticat ion are achieved.  9. S Lei [2018]  1. Integrity, and authenticat ion are achieved.  9. S Lei [2018]  1. Integrity, and authenticat ion are achieved.	,				
Blowfish Encryption Algorithm Algorithm Algorithm Storage in iKhalkar [2018]  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. RC4, AES, DES, and Algorithm Steganography computing using Hybrid encryption algorithm algorithm  8. RC4, AES, DES, and Algorithm sused. Algorithms used. Algorithms used. Algorithms used. Algorithms can be exacuted concurrently, (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  8. RC4, AES, DES, and Algorithms used. Algorithms used. Algorithms can be exacuted concurrently, (ii) Confidentiality, Data Integrity, and authenticat ion are achieved. The aspect of virtual machinest mechanism of machinest mechanism on metwork ransmissi on an achieve the cryptograph hy cloud framework and achieve the cryptograph hy service which is still issues by service which is uniprove.					not shown
8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm algorithm  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm  9. S Lei [2018]  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm algorithm algorithm  8. Secure File Storage in Cloud computing using Hybrid encryption algorithm scan be executed concurrentl y. (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Storage in Cloud computing using Hybrid encryption and decryption because algorithms can be executed concurrentl y. (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Storage in Cloud Storage in Cloud Storage in Cloud Encryption and decryption and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Storage in Cloud Storage in Cloud Storage in Cloud Encryption and decryption and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Storage in Cloud Storage in Cloud Storage in Cloud Storage in Cloud Encryption and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Storage in Cloud Storage in Cloud Storage in Cloud Storage in Cloud Encryption and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Algorithm Steep Storage in Cloud Storage in Cloud Encryption and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Algorithm Steep Storage in Cloud Steep Storage in Cloud Encryption and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Algorithm Steep Storage in Cloud Encryption and authenticat ion are achieved.  9. S Lei [2018]  8. Secure File Algorithm Steep Storage in Cloud Encryption and authenticat ion are achieved.  9. S Lei [2018]  9. S Lei [2018]  8. Secure File Algorithm Steep Storage in Cloud Encryption and authenticat ion are achieved.  9. S Lei [2018]  9. S Lei [201					
8.   Secure File   Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]   Secure File   Cloud computing uhybrid encryption algorithm   Algorithms used.   Mercandom/rel are achieved.   Secure File   Storage in Cloud computing uhybrid encryption algorithm   Cloud encryption algorithm   Secure File   Storage in iKhalkar [2018]   Secure File   Storage in iKhalkar [2018]   Algorithms used.   Mercandom/rel are decryption because algorithms can be executed concurrent y. (ii)   Confidentiality, Data Integrity, and authenticat ion are achieved.   Mercandom/rel are achieved.					
8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  8. Storage in iKhalkar [2018]  Storage in Cloud computing using Hybrid encryption algorithm  Research and design of Cryptograph by cloud framework  9. S Lei [2018]  Research and design of Cryptograph by cloud framework  Research and design of Cryptographic machineframewo on transfer mechanism achieve the cryptograph by service which is improve.					
8. Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Cloud Computing using Hybrid encryption algorithm algorithm  Research and design of Cryptographic of Cryptography cloud framework  Steganography and decryption because algorithms can be executed concurrently, (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  Secure File Storage in Cloud Computing using Hybrid encryption algorithm seal.  Steganography takes less oncryption and decryption because algorithms can be executed concurrently, (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  Secure File Storage in Cloud Computing using Hybrid encryption and decryption and decryption because algorithms can be executed concurrently will be executed concurrently of the secure of virtual authenticat ion are achieved.  Secure File Storage in Cloud Steganography takes less on time for random/rel ated keys are used.  Secure File Mehulbatra, Prayas Dixit, LalitRawat, Rohin is hybrid encryption and decryption because algorithms can be executed concurrently, (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  Secure File Algorithm used.  Steganography takes less on time for encryption and authenticat ion are achieved.  VCM does not have machineframewo riveled the secure of virtual network of virtual network of virtual achieve the cryptography and authenticat ion are achieved.  Secure File Malor Algorithm used.  Steganography and Algorithm used.  VCM does Not have machineframewo riveled to the control of virtual authenticat ion are achieved.  Secure File Algorithm used.  Steganography and authenticat ion are achieved.  VCM does Not have machineframewo riveled to the control of virtual authenticat ion are achieved.  Secure File Algorithm atex less less less less less less less le		711501111111			
8. Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Storage in Cloud computing using Hybrid encryption algorithm  Algorithms used.  Algorithms used.  Steganography takes less time for encryption and decryption because algorithms can be executed concurrently. (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of Cryptograph hy cloud framework  Figure File Storage in Cloud and Gerryption algorithm Steganography takes less time for encryption and decryption and decryption algorithms can be executed concurrently y. (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of cryptographic machineframewo rk used  Prival Algorithm vulnerable, Nakes less time for encryption and decryption and decryption and decryption and decryption and antime for encryption and decryption and decryption and decryption algorithms vulnerable, and decryption and decryption and decryption and decryption and decryption and authenticat ion are achieved.  9. S Lei [2018]  Research and design of cryptographic machineframewo rk used  Prival Algorithm vulnerable, Algorithm Steganography and algorithm and selection and and decryption and decryption and decryption and authenticat ion are achieved.  9. S Lei [2018]  Research and design of cryptographic machineframewo rk used  Prival Algorithm vulnerable, Algorithm Algorithm Algorithm and and decryption and authenticat ion are achieved.  9. S Lei [2018]				does not	
8. Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Storage in Cloud computing using Hybrid encryption algorithm  9. S Lei [2018]  Research and design of Cryptograp hy cloud framework  Research and design of Cryptograp hy cloud framework  P. S Lei [2018]  Research and design of cryptograp hy cloud framework  Research and design of cryptographic machineframewo rk used  Research and algorithm stakes less and Algorithm and algorithm and algorithm sued.  Research and authoricat in takes less and algorithm sued.  Research and algorithm sued.  Re					
8. Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Storage in Cloud computing using Hybrid encryption algorithm  9. S Lei [2018]  Research and design of Cryptography hy cloud framework framework framework image.  9. S Lei [2018]  Research and design of framework framework imachine framework imate at algorithm takes less time for encryption and decryption because algorithm takes less time for encryption and decryption because algorithm takes less time for encryption and and design of encryption and decryption because algorithm ality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of rytual cryptographic machine framewor rk used on transfer mechanism achieve the cryptograp still issues by service which is improve.					
8. Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Cloud computing using Hybrid encryption algorithm  algorithm  Steganography Algorithms used. time for encryption and decryption because algorithms can be executed concurrentl y. (ii)  Confidenti ality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of cryptographic of Cryptography cloud framework  Framework  P. S Lei [2018]  Research and design of machineframewo of the used in the province of virtual network rk used  Framework  Rot4, AES, DES, and Algorithm takes less non-random/rel ated keys are used.  Algorithms used. time for encryption and decryption because algorithms can be executed concurrentl y. (ii)  Confidenti ality, Data Integrity, and authenticat ion are achieved.  P. S Lei [2018]  Research and design of wirtual cryptographic machineframewo rk used  Framework  Fram					
8. Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]  Secure File Storage in Cloud computing using Hybrid encryption algorithm  1 Seganography Algorithms used.  Steganography Algorithms used.  Algorithms used.  Algorithms used.  Secure File Storage in Cloud computing using Hybrid encryption and decryption because algorithms can be executed concurrentl y. (ii) Confidentiality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of Cryptograph hy cloud framework  P. S Lei [2018]  Research and design of Cryptograph hy cloud framework  Research and design of cryptographic machineframework  Research and design of continual to the cryptographic machineframework  Research and design of cryptographic machineframework  Research and design of continual to the continual to the cryptographic machineframework  Research and design of continual to the continual to the cryptographic machineframework  Research and design of continual to the				_	
Mehulbatra,PrayasDixit,LalitRawat,Rohin iKhalkar [2018]    Cloud computing using Hybrid encryption algorithm   Cloud encryption and decryption because algorithms used.   Cloud encryption because algorithms   Cloud encryption and decryption because algorithms   Cloud encryption and algorithm   Cloud encryption and decryption because algorithms   Cloud encryption and decryption because   Cloud encryption and decryption because   Cloud encryption encryption   Confidentiality, Data Integrity, and authenticat ion are achieved.   Cloud encryption encryption   Confidentiality, Data Integrity, and authenticat ion are achieved.   Cloud encryption encryption   Confidentiality, Data Integrity, and authenticat ion are achieved.   Cloud encryption encryption   Confidentiality, Data Integrity, and authenticat ion are achieved.   Cloud encryption   Confidentiality, Data Integrity, and authenticat ion are achieved.   Cloud encryption   Confidentiality, Data Integrity, and authenticat ion are achieved.   Cloud encryption   Confidentiality, Data Integrity, and authenticat ion are achieved.   Cloud encryption   Confidentiality, Data Integrity, and authenticat ion a	8.	Secure File	RC4, AES, DES.		RC4 is
computing using Hybrid encryption algorithm  Research and design of Cryptograph y cloud framework  P. S Lei [2018]  Research and design of cryptographic machineframewo rk used  Research cryptograph hy cloud framework  Research encryption and decryption because algorithms can be executed concurrentl y. (ii) Confidenti ality, Data Integrity, and authenticat ion are achieved.  Virtual cryptographic machineframewo rk used  Virtual cryptographic machineframewo rk used  Virtual cryptographic machineframewo rk used  VCM does not have of virtual network on transfer mechanism , and can achieve the cryptograp hy service which is still issues to improve.	Mehulbatra,PrayasDixit,LalitRawat,Rohin				
using Hybrid encryption algorithm  algorithm  algorithm  encryption algorithm  encryption and decryption because algorithms can be executed concurrentl y. (ii) Confidenti ality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of cryptograph y cloud framework  ramework  ramework  ramework  encryption ated keys are used.  Virtual Confidenti ality, Data Integrity, and authenticat ion are achieved.  VCM does not have much loss on transfer mechanism , and can achieve the cryptograp hy cloud framework  ramework  rame	iKhalkar [2018]	Cloud			non-
Hybrid encryption algorithm  algorithm  Hybrid encryption algorithm  algorithm  and decryption because algorithms can be executed concurrentl y. (ii)  Confidenti ality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of Cryptograp hy cloud framework  Cryptograp hy cloud framework  Research and design of cryptographic machineframewo rk used  Pound of Cryptograp hy cloud framework  Research and design of cryptographic machineframewo rk used  Research and design of cryptographic machineframewo rk used  Research and design of wittual of virtual machineframewo rk used  Research and design of virtual such research and authenticat ion are achieved.			Algorithms used.		
encryption algorithm  encryption algorithm  encryption because algorithms can be executed concurrentl y. (ii)  Confidenti ality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of Cryptograph of Cryptograph hy cloud framework  Research and design of cryptographic machineframewo rk used  Research and design of cryptographic machineframewo not have much loss on transfer mechanism on mechanis achieve the cryptograp hy service which is still issues to improve.					-
algorithm  algorithm  because algorithms can be executed concurrentl y. (ii) Confidenti ality, Data Integrity, and authenticat ion are achieved.  9. S Lei [2018]  Research and design of cryptographic of Cryptograp hy cloud framework  Rused  Research and design of cryptographic machineframewo rk used  Research and design of cryptographic machineframewo rk used  The aspect of virtual network on transfer mechanism on n, and can achieve the cryptograp hy service which is  improve.					are used.
9. S Lei [2018]  Research and design of Cryptograph hy cloud framework  Research and design of Cryptograp hy cloud framework  Research and design of Cryptograp hy service which is  Research and design of Cryptograp hy service which is  Research and design of machineframewo rk used  Research and design of cryptographic machineframewo rk used  Research and design of machineframewo rk used  Research and design of cryptographic machineframewo rk used					
9. S Lei [2018]  Research and design of Cryptograph hy cloud framework  framework  Research and design of Cryptograph hy cloud framework  Framework  Research and design of Cryptograph hy cloud framework  Framework  Research and design of Cryptographic machineframewo rk used  Research and authenticat ion are achieved.  Research and authenticat ion are ach					
9. S Lei [2018]  Research and design of Cryptograp hy cloud framework  Cryptograp hy cloud framework  Research and design of Cryptographic machineframewo rk used  Research and design of virtual cryptographic machineframewo rk used  Research and design of cryptographic machineframewo rk used					
9. S Lei [2018]  Research and design of Cryptograp hy cloud framework  Research and design of Cryptograp hy cloud framework  Research and design of cryptograp hy cloud framework  Research and design of cryptographic machineframewo rk used  Research and design of virtual on thave much loss on transfer mechanism on achieve the cryptograp hy service to which is improve.				_	
9. S Lei [2018]  Research and design of machineframewo rk used  Confidenti ality, Data Integrity, and authenticat ion are achieved.  VCM does not have of virtual much loss on transfer mechanism on network transmissi on machineframework  framework  framework  Research and design of cryptographic machineframewo rk used  framework  framework  Framework  Research authenticat ion are achieved.  VCM does not have of virtual network transmissi on mechanism on mechanism achieve the cryptograp hy service which is improve.					
9. S Lei [2018]  Research and design of machineframewo rk used  Cryptograp hy cloud framework  framework  Research and design of machineframewo rk used  Research and design of machineframewo rk used  Research and design oryptographic mot have of virtual much loss on transfer mechanism on mechanism achieve the cryptograp hy service to which is					
9. S Lei [2018]  Research and design of machineframewo framework  Research and design of machineframewo hy cloud framework  Research and design of machineframewo rk used  Research and design cryptographic machineframewo rk used  Research and design cryptographic mot have of virtual network on transfer mechanism on mechanism on achieve the cryptograp still issues hy service which is improve.					
9. S Lei [2018]  Research and design of machineframewo rk used  Research and design of machineframewo rk used  Research and design of machineframewo rk used  Research and design of cryptographic machineframewo rk used  Research and design oryptographic much loss on transfer transmissi on achieve the cryptograp still issues hy service which is improve.					
9. S Lei [2018]  Research and design of machineframewo Cryptograp hy cloud framework  framework    S Lei [2018]   Research and design of machineframewo rk used   S much loss on transfer mechanism on achieve the cryptograp still issues hy service which is   S methods on transfer mechanis machieve the cryptograp still issues hy service which is   S methods of virtual much loss on transfer mechanism on achieve the cryptograp to mechanis machieve the cryptograp by service which is   S methods of virtual machieved.    S Lei [2018]   VCM does not have of virtual much loss on transfer mechanism on achieve the cryptograp to mechanis machieve the cryptograp by service which is   S methods of virtual machine much loss on transfer mechanism achieve the cryptograp by service to mich is improve.				and	
9. S Lei [2018]  Research and design of machineframewo Cryptograp hy cloud framework  framework  Research and design of machineframewo rk used  Research and design oryptographic machineframewo rk used  Research Virtual veryptographic mot have of virtual much loss on transfer mechanism on and can achieve the cryptograp still issues hy service which is improve.					
P. S Lei [2018]  Research and design of cryptographic machineframewo rk cloud framework  Research and design of cryptographic machineframewo rk used  Research and design cryptographic machineframewo rk used  Research cryptographic mot have much loss on transfer mechanism on achieve the cryptograp hy service to which is improve.					
and design of machineframewo rk used rused much loss on transfer mechanism achieve the cryptograp hy service which is of virtual network on transfer mechanism achieve the cryptograp hy service which is of virtual network on transfer mechanism achieve the cryptograp hy service which is of virtual network of virtual network much loss on transfer mechanism achieve the cryptograp by service to which is of virtual network much loss on transfer mechanism achieve the cryptograp by service to improve.	9. S Lei [2018]	Research	Virtual		The aspect
of Cryptograp hy cloud framework  of Cryptograp hy cloud framework  on transfer mechanism achieve the cryptograp hy service which is improve.	, Lor [2010]				
hy cloud framework  mechanism , and can achieve the cryptograp hy service which is  mechanis m, there is cryptograp to improve.					
framework  framework  , and can achieve the cryptograp by service which is  mechanis m, there is still issues to improve.			rk used		transmissi
achieve the cryptograp hy service which is m, there is still issues to improve.					-
cryptograp still issues hy service to which is improve.		Iramework			
hy service to which is improve.					
which is improve.					
<u> </u>					•

****	2502	E 2 4 2
ISSN	2583-	5344

10. Rohini, Tejindersharma [2018]	Proposed Hybrid RSA algorithm	Encrypt and decrypt the data by using RSA with HMAC.	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 Encrypt and decrypt the data by	Adequate security - MD5
	for cloud computing		using RSA with HMAC.	
11. Mr.RohitBarvekar,Mr.ShrajalBehere,Ms. AnushkaGulhane [2018]	An Approach to Hybrid Cryptograp hy on Cloud Environme nt	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 Confidenti al data misuse.	It is an abstract model, so it does not provide implement ation details.
12. Smita Sharma, R.P. Singh [2019]	The Cryptograp hy Based Security Algorithm For Protecting Sensitive Informatio n in Cloud Environme nt	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)Propose d 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.

	I		1	I
			simple structures. (iii) Key having 16 rounds it is also increasing security.	
13. Aditya Poduval,AbhijeetDoke,HiteshNemade,Ro hanNikam [2019]	Secure File Storage on Cloud using Hybrid Cryptograp hy	Rc6, 3DES, and AES are used to provide data security. Key information is stored by using LSB Steganography.	Key informatio n is stored in image steganogra phy, it is more secure, difficult to break by the intruder.	Sometimes image steganogra phy distortion of the image produces little changes in the user profile.
14. K.V.PradeepV.Vijayakumar, V. Subramaniyaswamy [2019]	An Efficient Framewor k for Sharing a File in a Secure Manner Using Asymmetri c Key Distributio n Manageme nt in Cloud Environme nt	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.Ponnav aiko [2020]	DNA Cryptograp hy Based User Level Security for Cloud Computing and Applicatio ns	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 cryptograp hy and hyper	A strongly authentic, encrypt, and digitally signed informatio n is very difficult to access

		Gunaninr,T- Thymine letters).	elliptic curve cryptosyste m 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.Kirubakaramoort hi [2020]	Develop Cloud Security in Cryptograp hy Technique s 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 communic ation overhead in the challenge phase.

19. Punam S Patil, Mohini R Chaudhari, Sagar U More [2021]	Cloud based Secure File Storage using Hybrid Cryptograp hy Algorithms	Provides block- wise data security by using AES,DES and RC2 Algorithms. By securing Key information Steganographytec hnique is used.	AES supports 112 or 168 bits.AES algorithms faster in both hardware and software.	Sometimes image steganogra phy distortion of the image is produced
20. Reece B.D.Souza,Dr.D.Ruby [2021]	Secure File Storage on Cloud using Enhanced Hybrid Cryptograp hy	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 & Implement ation of Enhanced Security Architectur e to Improve Performan ce 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 computatio n time, it is suited for the application s 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 Polyalphab etic Vignere Cryptograp hic Algorithm for Textual Data	The proposed approach is tested by using the fried man test and index of coincidence.	Data authenticat ion, Integrity, and Confidenti ality.	Cost- Effective, implement ed in smart IoT and wireless devices.

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

# 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 2<sup>nd</sup> 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 3<u>rd International Conference</u>* 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