International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 13, Issue 2 [February. 2024] PP: 111-118

A Comprehensive Review for Issues and Challenges of data Security in a Cloud Computing Environment

Rajan Kumar Yadav[1], Munish Saran[2], Upendra Nath Tripathi[3]
Department of Computer Science, DDUGU, Gorakhpur, Uttar Pradesh, India
Email: rkyd94@rediffmail.com[1], munishsaran@gmail.com[2], untripathi@gmail.com[3]
Corresponding Author : rkyd94@rediffmail.com

ABSTRACT – *Cloud computing has emerged after decades of research in the field of information technology. It is a type of business model that facilitates users to exchange services and information through the internet. If we put it in simple words it provides users the ability to access and share any data stored on the cloud server from anywhere and anytime through the internet. Now it comes to the fact that when users are accessing and sharing their data through the internet, how much confidentiality, authentication and integrity of that data remains intact. This paper mainly focuses on the concept of cloud computing, it's architecture, the security challenges faced in it and some of the security techniques used to protect the data stored on cloud storage.*

KEYWORDS – *Cloud Computing, Security Issues, Attacks , Security Techniques.*

Date of Submission: 11-02-2024 Date of acceptance: 26-02-2024

I. INTRODUCTION

The journey of cloud computing has been very long. After many decades of journey, cloud computing has become a very important and useful technology in today's time. In this, without buying any expensive hardware, servers etc., user's can store their data on cloud service through the internet and can access the data anywhere and at anytime with the help of internet, desktop, laptop or mobile devices [1].

Cloud Computing has emerged as a very widespread area and platform in today's time. It is an On-Demand Services that users or any organizations access it with the help of internet. In the present time, it is being used in every type of person, business, social media and banking etc., Cloud Computing can be explained in simple language that storing any type of data or information at any other place which can be accessed anywhere and anytime with the help of internet and that data the security and all other responsibilities of the cloud providers who provide such facilities [2].

Cloud Computing has emerged as technology that provides a large number of services to any users or organizations and these services are on-demand [3].

Cloud Computing has become a huge platform in the field of Internet Technology, so cloud computing is a technology that provides various types of applications, network, storage and On-Demand services to user's or any organizations and users or any organizations, Internet and devices like laptop, desktop and mobile connect to cloud service providers [4].

The architecture of cloud computing represents connectivity and services from clients devices to cloud data centers. Users devices such as laptop or smart phones are connected to cloud service through the internet. The front end represents the user interface while the back end provides the cloud infrastructure including data centers, servers, storage and networks. Infrastructure as a Service provides servers, storage, and networking resources while platform as a service and software as a service facilitate application development and ready to use applications. Runtime cloud represents the runtime environments where applications are executed. Security management represents measures that protect data and applications against threats. Together these elements create a scalable, flexible, and secure cloud computing environment that provide users with on demand access to computing resources as shown in a figure 1.

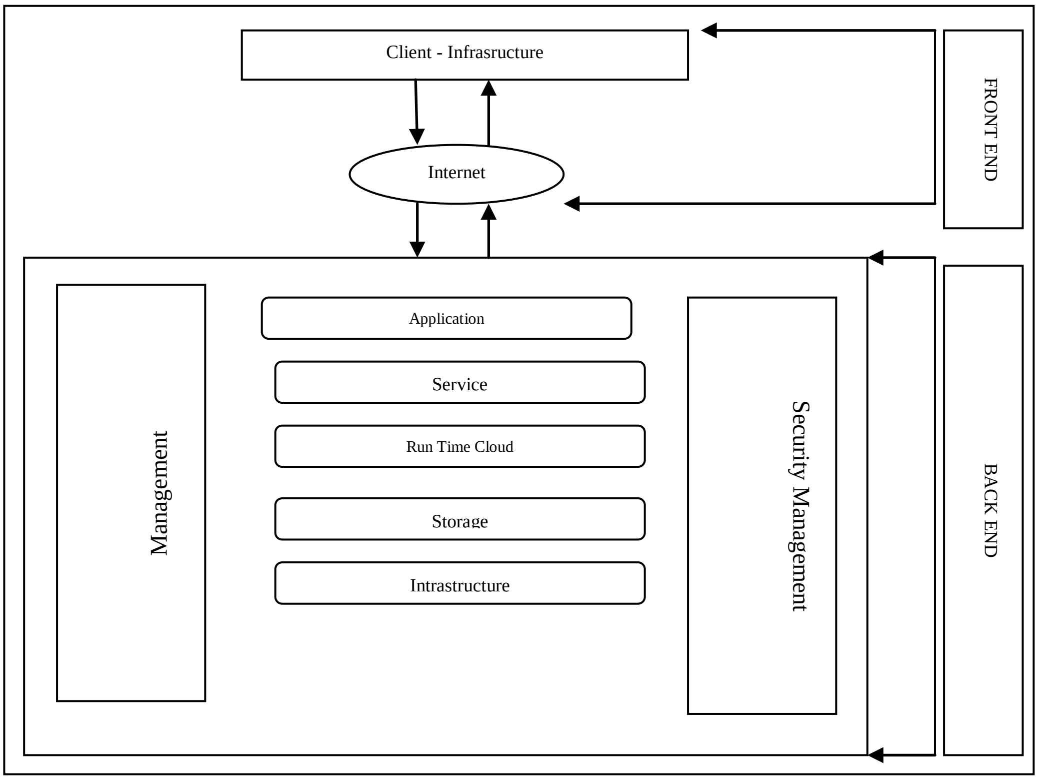


Fig. 1 Architecture of Cloud Computing

1.1. Characteristics of Cloud Computing

According to National Institute of Standards and Technology (NIST) the Characteristics of Cloud Computing are as follows [5].

1.1.1. *On-demand Self Services :* In this, if users or any organizations needs any storage, resources or virtual machine then it can get it directly from the cloud service providers.

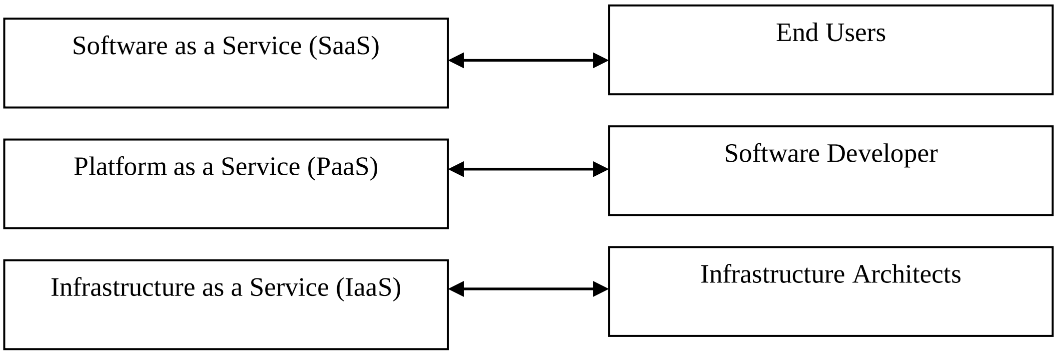
1.1.2. *Resource Pooling :* In this, cloud service providers can make the same type of resource, network and storage available to different users at different times.

1.1.3. *Rapid Elasticity :* In this, the cloud service providers who have provided any kind of storage, network etc., to the users, can increase or decrease it on the request of the users.

1.1.4. *Broad Network Access :* In this, Cloud service providers allow users to access data anywhere and anytime with the help of internet and any devices such as laptop, desktop and mobile etc,.

1.1.5. *Measure Services :* Cloud Service providers provide this facility to the users that for the time they have taken the resources, they have to pay the cost of the same time.

1.2. Service Models of Cloud Computing


Software as a Service (SaaS)
End Users
Platform as a Service (PaaS)
Software Developer
Infrastructure as a Service (IaaS)
Infrastructure Architects

1.2.1. *Infrastructure as a Service (IaaS) :* In this type of service model, storage, servers and network means hardware devices are provided are provided as resources and its maintenance of cloud service providers due to which it is costly [6].
1.2.2. *Platform as a Service (PaaS) :* In this type of service model, software development is done and cloud application is created using different types of technologies and programming languages, users do not have complete control over it, they can only use the developed cloud application.
1.2.3. *Software as a Service (SaaS) :* In this type of service models, cloud service providers provide users with the right to use cloud application with the help of the internet.

1.3. Deployment Models of Cloud Computing

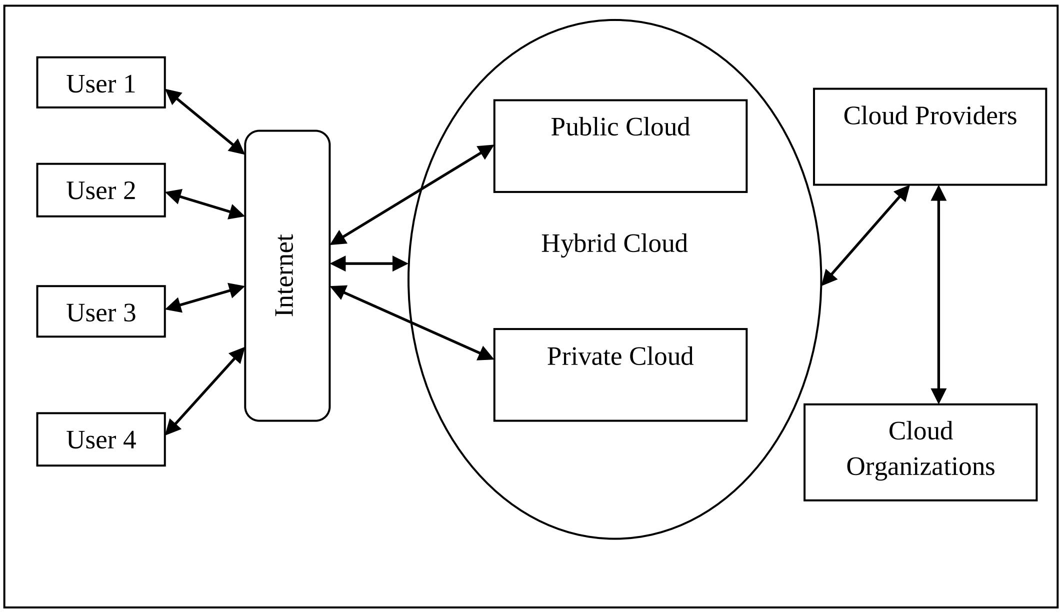


Fig. 2 Deployment Model of Cloud Computing

There are mainly four types of cloud deployment models which are as follow [7].
1.3.1. *Public Cloud :* In public cloud, users only use cloud applications according to their needs, which are provided by a company or third party that provides cloud services.
1.3.2. *Private Cloud :* Private Cloud is used for any particular organization or business, in this it is provided with strong security, in this a private network is also used.
1.3.3. *Community Cloud :* It is a cloud that is used for organizations or businesses with on or more groups.
1.3.4. *Hybrid Cloud :* Hybrid cloud is formed by the combination of different types of cloud, mainly private cloud and public cloud, it mainly provides security and privacy to data centres.

II. LITRATURE REVIEW

In today's time, cloud computing has emerged as a latest technology in which different types of users store their data on cloud storage with the help of internet, desktop, laptop and mobile devices because there are various types of attacks on the data of cloud user's are also seen, regarding which various types of research have been done in the last few years which are as follows :

According to Miss Shakeeba S. Khan et. al.[8] various types of security issues are seen in the cloud environment, to overcome which various types of cryptographic techniques can be used, such as Advanced Encyption Standard (AES), DES, Triple DES and Blowfish in Symmetric techniques and RSA and Diffie-Hellman key exchange in Asymmetric techniques. Cloud security can be improved by using.

According to P. Chinnasay et. al [9] by using cryptographic algorithm, problems related to data security and privacy on cloud storage can be fixed. They have proposed a hybrid model using blowfish in symmetric key algorithms and elliptic curve cryptography in asymmetric key algorithms, in which java platform. They have said that with the help of this hybrid cryptography algorithm, the security and privacy of cloud data storage can be strengthened.

According to Rima Akter et al [10] data security is seen as a big problem in the field of cloud computing. For this, encryption is a secure model at present. Various types of encryption techniques are used in cloud computing in which encryption and decryption algorithm based on AES-128 bit encrypting the original plain text and encrypting its secret key using RSA algorithm. Also the integrity and authenticity of the encrypted plain text message can be checked with the hash based message authentication code, so that the exchange of data of the users can be done in a safe manner.

According to Sanjeev Kumar et al [11] at present, almost every organizations is moving towards cloud storage to store its data, but somewhere the security of data on the cloud of users or organizations remains a major problem. They have proposed a hybrid encryption model in which multi-level encryption is done. Encryption and decryption using hybrid cryptographic techniques, data is encrypted on the client, uploaded to the cloud server and data is exchanged by decrypting it on the receiver side. For this, they have used DES and RSA cryptographic algorithms, which ensures the security of cloud storage or the security of user’s data can be increased. They have used this model for encryption and decryption on text file format buty they have said that this model can be used on other file formats also.

According to Selvaraj Jagadeesh et at [12] Cloud computing is an important in the services of information technology, which benefiting almost everyone in today’s time and people are also using it. Here in cloud computing, cloud service providers (CSPs) update, store, manage and access the data through the internet and provides an easy means of doing this which user can use anytime and from anywhere but an error is seen from the side of cloud service providers (CSPs) that they do not provide a better and stronger security to the user’s data. They have said that key development can be made easier by using Modified Elliptic Curve Cryptography (MECC) and it generates keys of smaller size than other cryptography techniques, hence it is better than them. They have proposed and implemented a hybrid cryptographic model by combining Advanced Encryption Standard (AES) and Modified Elliptic Curve Cryptography, which can significantly improve data optimization and security.

III. CLASSIFICATION OF CLOUD COMPUTING SECURITY ISSUES AND ATTACKS

3.1 Cloud Security Issues

In Cloud Computing, user’s get various types of benefits like on-demand services, low cost, availability everywhere etc., but it also has to face various types of challenges like confidentiality, authentications and integrity of the user’s in which data security is an important aspect [13]. Therefore, it is not so easy to save it because cloud service providers have to deal with various types of security issues. Here the study of various types of security issues has been discussed which are as follows [14].

Table 1. Cloud Computing Security Issues

S. No.	**Security Issues**	**Descryption**
01	Software Application	Software applications have front end and back end on the same platform, due to which it is weak in terms of security because a lot of programming codes are used on both front end and back end, due to which sometimes issues of vulnerabilities arise in it.
02	Cloud Data Storage	The most important part of cloud computing is cloud data storage. In the present times, due to the proliferation of online applications and connected devices, security related to cloud data storage has become a problem and is also becoming important. Establishing a data warehouse requires high security, which reflects the speciality of cloud services.
03	Embedded Security	High quality tools are used in embedded system and the users using it have to connect to the local network to perform the lamp. Here the main problem is seen when using virtual machines. Here the problem is in development. Virtual machines can become a threat when it comes, it can also cause data leakage. Here the cloud service providers have to see when they upload the isolated virtual machine in the cloud infrastructure and here in the monitoring of the virtual machine, the host computer is not connected to any part of the virtual machines. Serves as a controlling point for changing and updating responses.
04	Cluster Computing	A computer cluster is a group of computers, Virtual Machines or servers connected together to work together as a system. In industrial cloud computing, the idea of clustering is used for parallel processing. What are the benefits of this technology, such as improving power distribution and completing tasks faster. But, as the number of users in each cluster increases, some challenges related to security can also arise. This solves the main problems of increasing the number of users, data security and unauthorized access.
05	Client Management	Client management is a security issue in cloud computing environment. Its main objective is to protect the public information present in the client’s system. Client experience in the cloud is very important, because cloud services are growing so fast that the industry is experiencing a growth spurt. This is why some service providers are facing problems because they are implementing weak solutions for users. Only those users with experience in the field of cloud security can face difficulties in choosing a cloud provider. User authentication is also a vital part that helps protect the cloud from serious unethical access.

3.2 Security Attacks Categorization in Cloud Computing

Cloud Service providers face security challenges due to various types of unauthorized access and data bleaching attempts in cloud computing. For this, cloud service providers are continuously increasing security measures to reduce these security risks. Danger is a signal that indicates the possibility of an accident. It can cause harm to any system or organization. In this area, the most important threat has bee highlighted clearly. There are various types of the Attacks mentioned are as follows [2][14].

Table 2. Cloud Computing Security Attacks

Sr. No.	**Categorization of attack**	**Description**	**Name of Attack**	**Affected Cloud Services**	**Effect**	**Solution**
01	Storage Based	Storage bases attack is a type of attack in which a users stores its data on a cloud servers through a devices. In this type of attacks, other users or hackers can cause damage by attacking the stored data.	Data Privacy and Authentication	Software as a service	Service delivery is affected. A fake service can be created.	Using an intrusion detection or intrusion prevention system, using forced authentication and authorization, using a signature based approach.
			Man In The middle	Infrasture as a service, Platform as a service and Software as a service	Data Privacy and Security are affected	Using an encryption and decryption algorithms, Using an intrusion detection system and using a requirement for true secure socket layer (SSL) architecture.
02	Network Based	Cloud servers are connected to various external machines through the network, in which some unsuspecting users or hackers can attack it by entering the cloud setup through the network and break the security and confidentiality of the data.	Port Scanning	Infrastructure as a service, Platform as a service and Software as a service	Unsanitary conduct of service, affects service delivery.	Using packet counts and neural networks, Developing TCP/IP packets and Using Firewalls.
			Spoofing	Infrastructure as a service, Platform as a service and Software as service	Unsanitary conduct of service, this affects the confidentiality of the service.	Require strong authentication to access files and Encrypting information about service functionality and other details.
			Phishing	Infrastructure as a service, Platform as a service and Software as a service	The privacy of user credentials is affected and should not be disclosed.	Do not click on short URLs, Identifying spam e-mails and Using secure web links.
03	Application Based	Many different types of applications are running simultaneously on the cloud platform, in which hackers enter the application by using injection code. These codes trace the path of applications and collect data information.	DDoS Attacks	Infrastructure as a service, Platform as a service and Software as a service	Service delivery is affected, a fake service can be created.	Using a filter based approach, Using an intrusion detection or intrusion prevention system and using a signature based approach.
			SQL Injection	Software as a service	Rogue services are provided to users in lieu of legitimate services. The shape of the service is affected.	Using proxy based architecture to dynamically identify and extract useful input, Do not use dynamically generated SQL in the code.

			Cross Virtual Machine	Infrastructure as a service	This allows an attack that allows an attacker to gain control of a virtual machine by impersonating another user.	Using encryption and decryption and using a virtual firewall.

IV. SECURITY TECHNIQUES

4.1. Security Algorithms used for Cloud Storage

Encryption algorithm plays an important role in the security techniques of cloud. It is mainly divided into two parts in which the first is Symmetric (private) and the second is Asymmetric (public) key encryption. In symmetric key encryption, the same key is used to encrypt and decrypt the data. Such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Blowfish. In asymmetric key encryption, two keys are used, where the public key is used for encryption and the private key is used for decryption, such as Rivest Shamir Adleman (RSA), Digital Signature algorithms (DSA) and Elliptic Curve Cryptography (ECC) [15]. There are various Symmetric and Asymmetric Algorithms mentioned are as follows [16].

Table 3. Cloud Computing Security Algorithms

Algorithm	Description	Key Type	Key Size	Block Size	Structure	Quality
AES	It is a Rijndael block chipher , in which a single key is used for encryption and decryption. This means key sizes of 128, 192 and 256 bits are supported. Operation occurs in three rounds – 10 rounds for 128 bits, 12 rounds for 192 bits and 14 rounds for 256 bits. In every round byte substitution, shift row, mix column and key addition operations take place.	Symmetric	128, 192, 256 bits	128 bits	Substitution Permutation	It provide better encryption and Security
DES	The DES algorithm, a crucial element in cryptography, necessitates a 64-bit configuration for plaintext encryption and a 56-bit setup for decryption into chiphetext. With a block size of 64 bits, DES utilizes 56 bits from a key that is split into two segments of 28 bits each. The key undergoes rotation by one or two bits in accordance with the specific round in the process	Symmetric	64 bits, 54 bits are used	64 bits	Festial	It provides low Strangeness
Blowfish	The blowfish serves the purpose of both encryption and decryption, operating through a 16-round cipher. The F-Function methodology employed within enhance software speed. Notably, this algorithm is capable of encrypting data efficiently even on 32-bit microprocessors.	Symmetric	32 bits to 448 bits	64 bits	Festial	Better Cipher in SSL
RSA	RSA stands as the pioneering public-key cryptosystem designed for secure encryption and decryption during data transmission. The core of its security lies in the challenge of factoring two sizable prime numbers. Despite its somewhat slow operational pace, RSA	Asymmetric	1024 – 4096	128 bits	Public Key Algorithm	It provide better encryption but low speed

	executes its functionality in three distinct steps. The intial phase involves key generation for encryption or decryption data, followed by encryption where plaintext transforms into ciphertext. Lastly, the decryption phase reverses this process, converting encrypted text back into plaintext. RSA key size typically span for 1024 to 4096 bits.					
DSA	DSA is employed to secure digital or electronic data by verifying its authentic source. This ensures the sender's identity is confirmed, preventing unauthorized alteration or theft of data during transmission .	Asymmetric	Variable	Variable	Public Key Algorithm	It Provide better Encryption and fast speed
ECC	ECC is gaining popularity due to its compact key size, swift processing speed, and minimal memory usage. Rooted in the Discrete Logarithmic Problem, ECC presents algorithmic complexity. Functioning as public key cryptography, ECC employs a private key for decryption and a public key for encryption and verification across various services.	Asymmetric	Symmetric and Variable	Variable	Public Key Algorithm	It provide Better Encryption, security and fast speed

V. CONCLUSION

Currently, various users and organizations adopted for cloud storage in the realm of efficient storage solutions provided by cloud computing. However, data faces inherent risks related to sever storage, encompassing authentication, integrity and confidentiality issues. In this paper, mainly cloud computing technology and various types of security issues and security attacks arising in it have been studied. Also, to deal with these security issues and security attacks, encryption techniques have been studied in security techniques because encryption emerge is a dependable safeguard where data is transformed in an encryption format at the source and restored to its original state at the recipient, hence using it to strengthen the security and privacy of cloud data.

REFERENCES

[1]. Nada Alrehaili and Agadeer Mutahar, "Cloud Computing security challenges", International Advanced Research Journal in Science, Engineering and Technology, Vol 7, Issue 8, August 2020.

[2]. Rajan Kumar Yadav, Munish Saran, Upendra Nath Tripathi, "A Comprehensive Review of data Security in Cloud Computing Environment using Cryptographic Algorithms", International Journal for Research Trends and Innovation, Volume 7, Issue 11, ISSN : 2456-3315.

[3]. Munish Saran, Rajan Kumar Yadav, Upendra Nath Tripathi, "Mitigation from DDoS attack in Cloud Computing using Bayesian Hyperparameter Optimization based Machine Learning approach", International Journal for Research Trends and Innovation, Volume 7, Issue 11, ISSN : 2456-3315.

[4]. T. Ashok, K. Suresh, "Review on Cloud Computing Security Solutions against various Issue", International Journal of Innovative Research in Science and Technology, Volume 01, Issue 01, August 2021.

[5]. P. Mell and T. Grance, " The Nist Definition of Cloud Computing", National Institute of Standards and Technology Special Publication, Gaithersburg, 011.

[6]. Munish Saran, Rajan Kumar Yadav, Upendra Nath Tripathi "Machine Learning based Security for Cloud Computing : A Survey", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 17, Number 4 (2022), pp. 332-337.

[7]. Evans Osei – Opoku, Rym Regaieg, Mohamed Koubaa, "Review on Cloud Computing Security Challenges", European Scientific Journal April 2020 edition Vol. 16, No. 12 ISSN : 1857-7881 (print) e – ISSN 1857-7431.

[8]. Miss. Shakeeba S. Khan, Miss Sakshi S. Deshmukh, "Security in Cloud Computing using Cryptographic Algorithm", Internation Journal of Computer Science and Mobile Computing", IJCSMS, Vol. 3, Issue. 9, September 2014, Pg. 517-525.

[9]. P. Chinnasay, S. Padmavathi, R. Swathy and S. Rakesh, "Efficient Data Security using Hybrid Cryptography on Cloud Computing", Inventive Communication and Computational Technologies, Lecture Notes in Networks and System 145, https://doi.ogr/10.1007/978-981-15-7345-3_46.

[10]. Rima Akter, Md. Ashikur Rakman Khan, Fardowsi Rahman, Sultana Jahan Soheli and Nusrat Jahan Suha, "RSA and SEA Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing", International Journal of Computational and Applied Mathematics & Computer Science, Volume 3, 2023, DOI : 10.37394/232028.2023.3.8

[11]. Sanjeev Kumar, Garima Karnani, Madhu Sharma Gaur and Anju Mishra, "Cloud Security using Hybrid Cryptography Algorithms", 2021 2nd International Conference on Intelligent Engineering and management (ICIEM), IEEE.

[12]. Selvaraj Jagadeesh, Sabna Machinchery Ali, Soundara pandian Gnan Selvan, Mohammad Alijanbi, Manimaran Gopianand and John peter Jasmine Hephzipah, "Hybrid AES-Modified ECC Algorithm for Improved Data Security over Cloud Storage", Journal of Advanced Research in Applied Sciences and Engineering Technology, Volume 32, Issue 1 (2023) 46-56.

[13]. Mohammed Fars, Munwar Ali, Reehan Ali Shah, Asif Wagan and Radwan Kharabsheh, "Cloud Computing and data Security threats taxaonomy : Review", Journal of Intelligent & Fuzzy Systems, IOS Press, 2019.

[14]. Lubna Alhenaki, Alaa Alwatban, Bashaer Alamri and Noof Alarifi, "A Survery on the Security of Cloud Computing", 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), IEEE.

[15]. Dr. Prerna Mahajan & Abhishek Sachdeva, " A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Volume 13, Issue 15, Version 1.0, 2013.

[16]. Alabi Orabosade, Thompson Aderonke, Alese Boniface and Arome J. Gabriel, "Cloud Application Security using Hybrid Encryption", Communications on Applied Electronics (CAE) – ISSN : 2394-4714, Foundation of Computer Science FCS, New York, USA, Volume 7 – No. 33, May 2020.