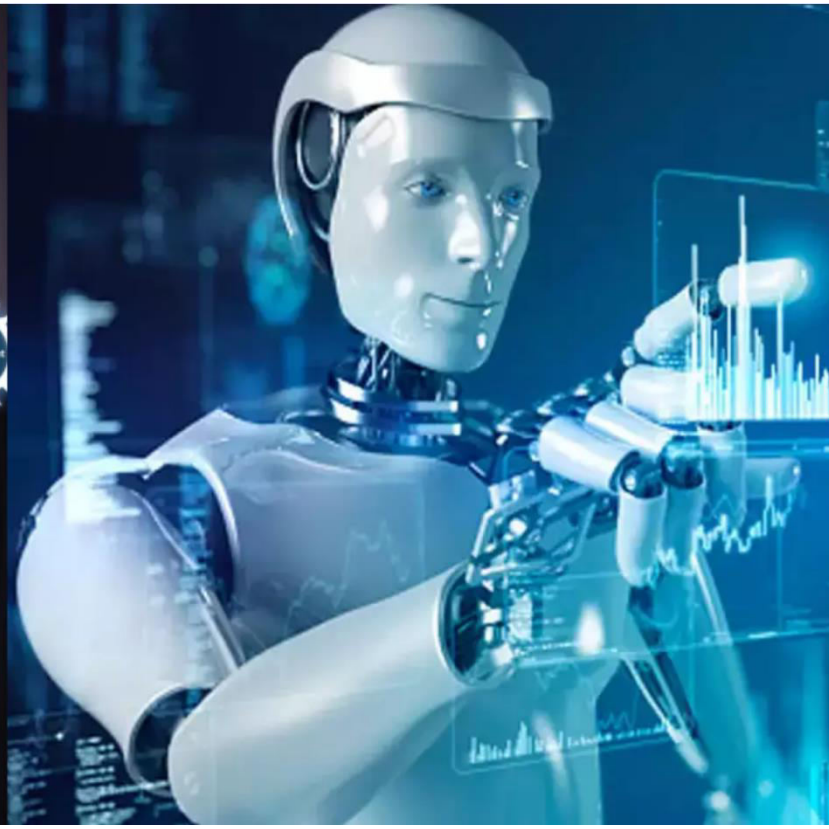
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 9, September 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 9, September 2025

|DOI: 10.15680/IJIRSET.2025.1409032|

Role Based Security for Cloud Based Data with Data Reliability

Kratika Saxena[1], Dr. Bhawana Pillai[2]

M. Tech. Student, Department of Computer Science & Engineering, LNCT's, Bhopal, India[1]

Assistant Professor, Department of Computer Science & Engineering, LNCT's Bhopal, India[2]

ABSTRACT: Cloud information storage has given significant advantages by permitting clients to store huge amount of information in a cost effective way. To ensure the protection of information put away in the cloud, cryptographic part based get to control plans have been created to guarantee that information must be gotten to by the individuals who are permitted by get to arrangements. As cryptographic methodologies don't address the problem of trust, in this paper, we propose a model to reason about there can be more method, enhance the security for put away information in cloud storage frameworks. The security models give a way to deal with the proprietors and parts to decide the dependability of individual parts and clients separately in this framework. The proposed security models consider part legacy and chain of importance in the assessment of reliability. We exhibit an outline of a security-based distributed storage framework which demonstrates can be coordinated into a framework that uses AES algorithm and SHA-2 algorithm to enhance the security of data.

KEYWORDS: Cloud computing, Encryption, AES, SHA- 2

I. INTRODUCTION

Cloud computing is the branch of computing. This is the most recent technology that is using today in each and every field of computer science. Cloud computing environment provide various services. As the name specifies that lots of computing resources provided by CSP (Cloud service provider). There has been a rapid growing trend in the recent times for using online services [1]. Today lots of thing is now putting all the data online. A major benefit of using online service is that the data is more secure than manual shaved data. When data is store in a manual way so if disaster comes the data will lose. However, lots of online service provider does not have capacity to store the large amount of data because these data have to secure in the particular manner. And this is so complex to maintain data of end user with efficiency and provide this service in a cost effective manner.

There is various cloud service that is provided by the cloud service providers. Cloud services can be in term of for academic use or it can be for storing data related to business aspect and it also can be a normal user that can use the cloud computing environment. Cloud computing technology has resources to provide the solutions. The solution can be in term of the software solution, hardware solution and it can be infrastructure solution. The online service provider can outsource data of end user's. There are 3 types of services that are provided by cloud computing environment.

1. IAAS
2. PAAS
3. SAAS

These three services are the major services that are provided by the Cloud computing environment. IaaS, is stands for infrastructure as a services. PaaS is stands for the Platform as a service. SaaS is stands for the software as a service [2]. This layer of cloud computing, which is on top of one another, are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and software as a service. Infrastructure layer is at the bottom, Platform in the middle. These services used to provide solution online to the end user's. The cloud computing provides solution to address the issue with the ability to store and manage the information which is increasing day by day. This has raised several security issues as how to control and prevent unauthorized access to database. There are various cloud types, four types are main: Public cloud, Private cloud, community cloud Hybrid cloud [3].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 9, September 2025

|DOI: 10.15680/IJIRSET.2025.1409032|

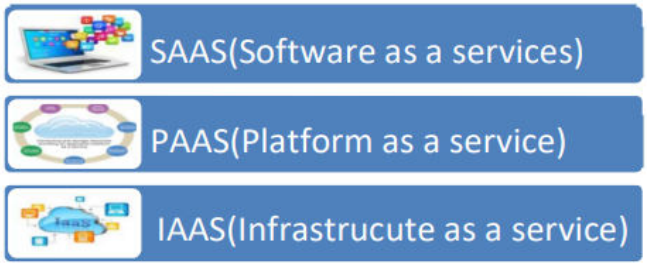


Figure 1: Cloud Computing Services

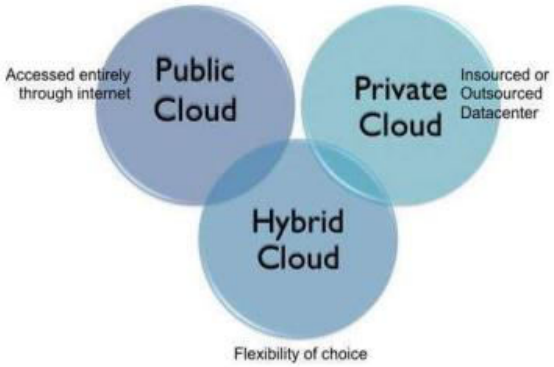


Figure 2: Types of cloud computing

Online service providers can outsource user's data to the public cloud while focusing on the service quality as well. Since public cloud is an open platform for all the users and it can be subjected to the malicious attacks from both insiders and outsider also.

In a cloud data storage system, the data owners would wish to specify the policies as to who can access their data and the cloud providers are required to correctly enforce the policies that the data owners have specified With growing awareness and concerns regards to Cloud Computing and Information Security, there is growing awareness and usage of Security Algorithms into data systems and processes [4].

In this paper we review some encryption algorithms along with some add-ons to such techniques, used by various authors. One approach is to protect the privacy of the data stored in the cloud is using access control. Many access control mechanism have been proposed over the years. The aim of this study is to briefly look into the flaws of the current solutions to the problem in question here. Based on this study, we will work towards finding a solution with better computational costs and overheads.

II. LITERATURE SURVEY

1. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security [5]

In this paper, the author clearly defines the differences among various encryption techniques being used today. It explains what asymmetric and symmetric techniques actually are and how they differ with each other. The speed and security graph clearly defines that AES is better in each aspect being used for testing in this paper, as compared to its counterparts.

2. Flexible Data Access Control based on Trust and Reputation in Cloud Computing [6]

In this paper, the author proposed a scheme so as to control the cloud data access in a cloud, based on trust and reputation. The scheme makes use of a trust management framework and uses Attribute Based Encryption (ABE), Proxy Re-Encryption (PRE) along with a reputation-based revocation mechanism. This scheme supports the fact that

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 9, September 2025

|DOI: 10.15680/IJIRSET.2025.1409032|

the cloud data access can be flexibly supported by making use of these techniques in a certain pattern. With certain testing phases, the scheme proposed by the author comes with low communication costs, low computation costs, auto-generation and management of access keys based on trust, flexible and pretty much secure under the testing environment.

3. Applying Encryption Algorithm to Enhance Data Security in Cloud Storage [7]

The author of this paper defines a way of providing extra security to the cloud data. It defines how asymmetric and symmetric techniques work on their own, and what if, they can be used together to provide an ultimate secure solution? The author makes use of RSA and AES algorithms. Here, the data secret key is encrypted via AES encryption technique. This encrypted key is then further encrypted using the RSA the output is then stored in a secure server as well. This technique, in way provides a two layer security to our data stored in the cloud.

4. A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing [8]

In this paper, the author focuses on the Mobile Cloud Computing (MCC) and its related issues with security. The author defines a custom Ciphertext Policy Attribute Based Encryption (SL-CP-ABE), by exploiting the traditional CP-ABE and ABE techniques and their flaws. This method aims at reducing the computational overheads for the encryption and decryption process in mobile environment, by outsourcing the most of it, to the cloud, making this technique more flexible and more expressive over the policy of data access control. The basis of this technique starts with the use of UCCMA technique for the secret sharing between the authorized parties which basically breaks the whole secret into parts and with even one part less, the secret won't be what it is supposed to be. SL-CP-ABE then reduces all the computational overhead, whatever it can, to the cloud based Encryption Proxy Server (EPS) and Decryption Proxy Server (DPS). These servers are used only during the respective processes only, and help a lot in making the complete system a lightweight with swift and faster response over other techniques.

5. Cloud Based Access Control Model for Selective Encryption of Documents with Traitor Detection [9]

Here, the author used the Fast Access Control Vector Broadcast Group Key (FACV-BGKM) scheme and Aggregate Equality Oblivious Commitment Based Envelope Protocol (EQ-OCBE), followed by a traitor log recorder. OCBE protocol is similar to Diffie Hellman protocol, based on the Pedersen Commitment scheme. It makes sure that the data is transferred only to the legit users. EQ-OCBE, with more and more equality conditions, the complexity of the protocol thickens. And to make sure the protocol stays collision free, the author added hashing to the Aggregate EQ-OCBE Protocol. BGKM is basically a key management, creation and sharing scheme. Fast ACV-BGKM is an extension of ACV-BGKM (used to make the rekeying a one off function) that reduces the computational cost of update operations. Pre- computation can be used to improve the efficiency of this scheme. It uses the baby-step-giant-step (BSGS) rekeying method with no need to run the complete key generation step again for updating new users or policies.
For the traitor log system, the illegal users who try to access data they are unauthorized for will get their ids stored in a traitor record file. This file can be shared with the data owner and other responsible roles regarding such issues.

6. Secure Role based Data Access Control in Cloud Computing [10]

The author of this paper made use of different technologies so as to achieve a fine grain access of data in cloud computing. It uses Key policy Attribute-Based Encryption (KP-ABE) which is used for the data encryption and decryption. This method encrypts the data into a cipher text, based on the message, public key and the set of attributes, used as input. The cipher text is then re-encrypted into another cipher text, using Proxy Re-Encryption, so that it can be accessed by the private key of the required user, without peeking into the actual message. The decryption in KP-ABE is achieved by using the encrypted data, public key, required private key and the set of attributes, as the input.

7. Cryptographic Secure Cloud Storage Model with Anonymous Authentication and Automatic File Recovery [11]

In this paper, the author makes use of a decentralized system with multiple Key Distribution Centre (KDC) structure. This system is implemented using the Role Based Access Control mechanism. And for the anonymous authentication, the author implemented SHA -1 hash function in which, user attributes are hidden from the cloud. User authenticity is based on three levels of cross check. First, the user gets passed by the KDC body. Then comes the assurance of a trusted third party who takes the guarantee of the user being genuine and authorized. Finally, a digest of the User ID is generated and uploaded via SHA-1 using Pallier cryptosystem encryption technique. This homo-morphic technique is being used for the data encryption process as well.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 9, September 2025

|DOI: 10.15680/IJIRSET.2025.1409032|

8. Enhancing Cloud Computing Security using AES Algorithm [12]

In this paper, the author proposes how and what benefits can be reaped from the use of AES algorithm for encryption-decryption purposes. It defines how AES can be a better option than its counterparts. It easily supersedes techniques like DES and Triple DES in terms of key collision, weaker keys and performance tests. It also passed the tests of data encryption-decryption throughput and execution time, when compared to Triple DES, DES and RC2 techniques. When compared to methods RC2, RC6 and Blowfish, it clearly wins them over in terms of time consumption.

III. PROPOSED METHODOLOGY

In cloud computing environments, the usual data transmission and storage mode is shown in Figure3.

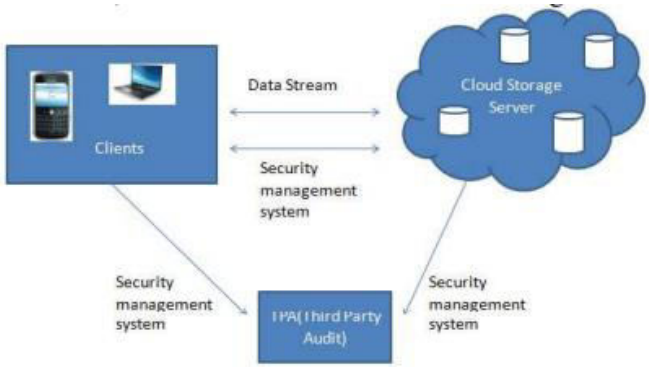


Figure 3: Data storage structure in cloud

The effective protection of user privacy data is the primary problem of cloud security. From the above figure, we can see that cloud computing stores a large number of data files on the distant servers, and users can reduce the burden of storage and computation, then enjoy the flexible and efficient service brought by cloud computing.

In cloud computing security concern is most important thing. To get the security in cloud we proposed a system that is a combined security system. This system used re-encryption technique with SHA-2 algorithm for security. When these two algorithms will performed on the file then third party verification will use to improve the security. The complete flow diagram of proposed model is shown below:

Algorithm Pseudo Code

Input: Data packet, receiver address.
Output: encryption evaluation, access management, result evaluation.
Algorithm Begins:
Receiving user input packets();
RSA();
If(data packet received)
{
Packet transmission ();
Permission access();
Datasecurity ();
SigSha2();
EndIf;
}
If(Access==Allowed)
{
Data permission access;
Rightsmanagement();
Fileshare();

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 9, September 2025

|DOI: 10.15680/IJIRSET.2025.1409032|

}
EndIf;
}

The following flowchart describes process will start first then we upload a file if file is already uploaded to the server then is will show "already uploaded file ", if file is not uploaded then file will upload to server then encryption will perform to the data of file. Here the AES algorithm is used for the encryption process. Then re-encryption is performed secure socket layer and SHA-2 is performed. Then user takes permission to access the file. For this process request will generate then the request will go to the TPA, to verify the request and give the permission to access the file. After getting the permission to access the file, decryption will performed to file and it will show to the authenticated user.

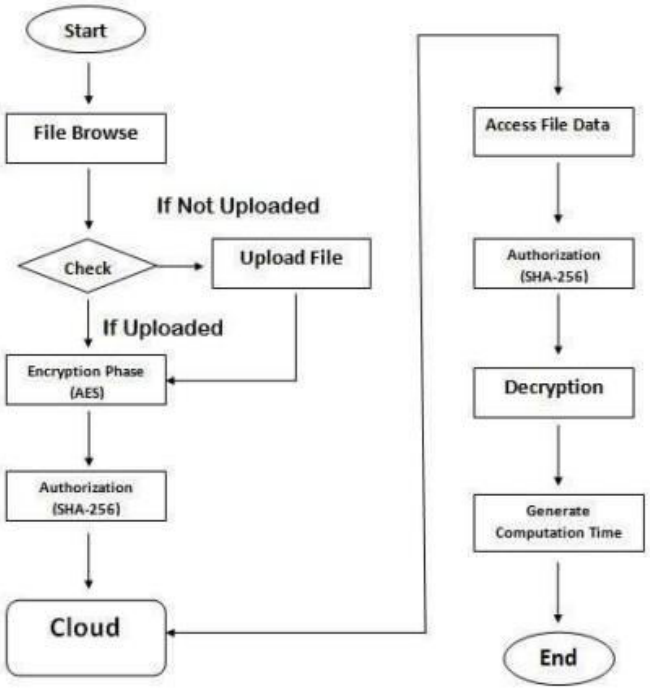


Figure 4: A complete flow diagram of proposed method

IV. RESULTS ANALYSIS

The following figures would clearly define that the use of a single key encryption method, AES is proved to be a faster better and secure alternative to the double key encryption methods like RSA. Also, the use of SHA256 over the traditional SHA-1 proves to be more secure, and complex to the attackers, when used for authentication purposes (Figure 3-4). Limitations, Flaws and Future The study we performed was solely based on how the data is stored in the cloud, with different encryption methods. These techniques were rarely aimed at smaller-mid level firms. Our system is based on how role based cloud data access be performed with lesser implementation and computational costs. So apart from this, any big level firm or any firm with a lot of users and big chunk of data, this system proposed by us isn't tested for. All the findings and funding of this research were solely performed and taken care by the author themselves.

V. CONCLUSION

In cloud computing user's data stored in cloud server, so security of that data is the biggest concern in cloud computing. A secure access and authentication mechanism is required to preserve the security of that data while accessing that data. In this paper a security mechanism over the various files, used to provide access control and authentication in cloud computing is presented. This paper exploits the importance and the flaws of such techniques.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 9, September 2025

|DOI: 10.15680/IJIRSET.2025.1409032|

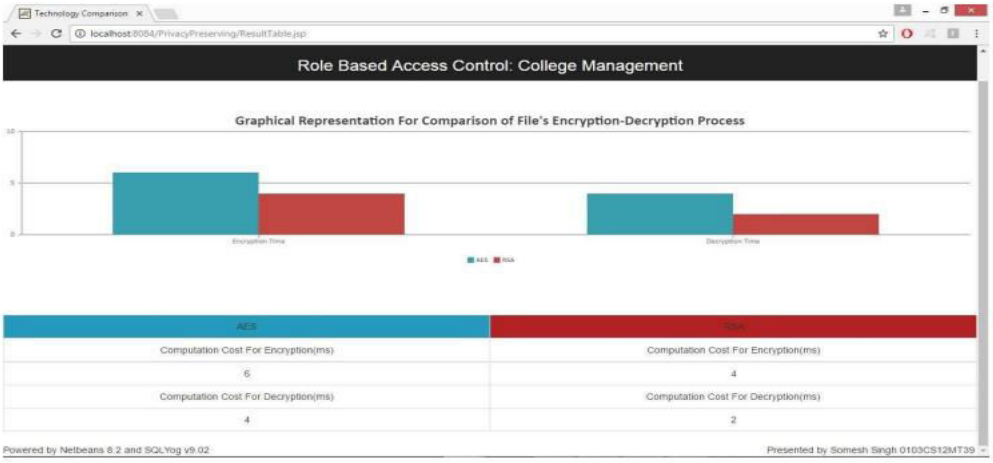


Figure 5: AES vs RSA final computational difference (Graphical Representation)

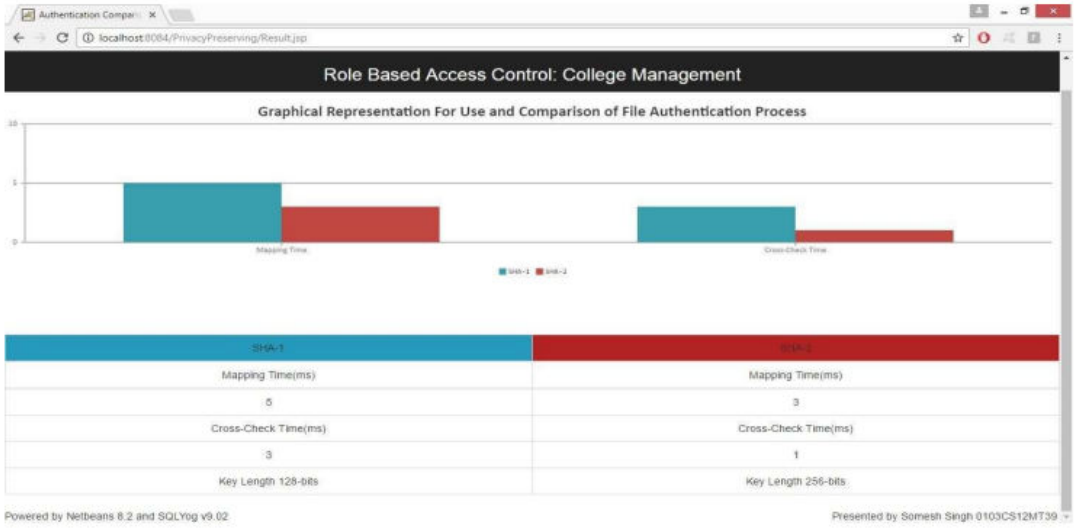


Figure 6: SHA-256 vs SHA-1 (Graphical Representation)

REFERENCES

[1] Grossman, R. L. (March/April 2009). The Case For Cloud Computing. IEEE Itpro, 23–27.
[2] Jens, F. (September 2008). Defining Cloud Services And Cloud Computing.
[3] L. Wang, G. Laszewski, M. Kunze And J. Tao, ―Cloud Computing: A Perspective Study , J New Generation Computing, 2010, Pp 1-11.
[4] Eystein Mathisen. Security Challenges And Solutions In Cloud Computing, In: International Conference On Digital Ecosystems And Technologies (IEEE DEST 2011), 2011.P.208-212.
[5] Gurpreet Singh, Supriya "A Study Of Encryption Algorithms (RSA, DES, 3DES And AES) For Information Security",International Journal Of Computer Applications (0975 – 8887)Volume 67– No.19, April 2013
[6] Zheng Yan,, Xueyun Li, Mingjun Wang And Athanasios V. Vasilakos, "Flexible Data Access Control Based On Trust And Reputation In Cloud Computing", DOI 10.1109/TCC.2015.2469662
[7] Zaid KARTIT, Mohamed EL MARRAKI "Applying Encryption Algorithm To Enhance Data Security In Cloud Storage", Engineering Letters, 23:4, EL_23_4_06 (Advance Online Publication: 17 November 2015)
[8] Yu Jin,Chuan Tian, Heng He & Fan Wang "A Secure And Lightweight Data Access Control Scheme For Mobile Cloud Computing", 2015 IEEE Fifth International Conference On Big Data And Cloud Computing

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 9, September 2025

|DOI: 10.15680/IJIRSET.2025.1409032|

[9] Punya Peethambaran And Dr. Jayasudha J. S. "CLOUD BASED ACCESS CONTROL MODEL FOR SELECTIVE ENCRYPTION OF DOCUMENTS WITH TRAITOR DETECTION", International Journal Of Network Security & Its Applications (IJNSA), Vol.6, No.5, September 2014

[10] V.Sathya Preiya, R.Pavithra & Dr. Joshi "Secure Role Based Data Access Control In Cloud Computing" International Journal Of Computer Trends And Technology- May To June Issue 2011

[11] Sowmiya Murthy "Cryptographic Secure Cloud Storage Model with Anonymous Authentication and Automatic File Recovery" ICTACT Journal on Soft Computing: Special Issue on Distributed Intelligent Systems And Applications, October 2014, Volume: 05, Issue: 01

[12] Abha Sachdev Mohit Bhansali "Enhancing Cloud Computing Security Using AES Algorithm" International Journal Of Computer Applications (0975 – 8887)Volume 67– No.9, April 2013

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details