ISSN 2348 – 8034
Impact Factor-4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ENAHNCEMENT OF SECURITY FOR PRIVACY PRESERVATION IN CLOUD SYSTEM BY ANONYMOUS REQUEST ACCESS

Ashwini Khodwe[*1] and Prof. Dipali Khatwar[2]
[*1]Computer Science & Engineering ,RTMNU University, A.C.E. Wardha, Maharashtra , India
[2]RTMNU University , A.C.E. Wardha , Mahrashtra , India.

ABSTRACT

Distributed computing is a processing innovation or data innovation engineering utilized by association or people. It dispatches information stockpiling and intuitive worldview with some points of interest like on-interest self-administrations, pervasive system access. Because of ubiquity of cloud administrations, security and protection gets to be significant issue.

There is the issue of real obligation regarding data (If a customer stores some data in the cloud, can the cloud supplier advantage from it?). Various Terms of Service assentions are calm on the subject of proprietorship. Physical control of the PC equipment (private cloud) is more secure than having the apparatus off site and under someone else's control (open cloud). This passes on magnificent inspiration to open appropriated figuring organization suppliers to sort out building and keeping up strong organization of secure organization. This paper addresses configuration of proposed framework.

Keywords: *Cloud Computing, Authentication Protocol, Privacy Preservation, Shared Authority, Universal Composability.*

1. INTRODUCTION

1.1 Cloud Computing

Cloud computing is a relatively new business model in the computing world. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

1.2 Cloud Models

There are three types of cloud models.

a. Private Cloud b. Public Cloud c. Hybrid Cloud

Private Cloud

Private cloud give the capacity to all the more specifically oversee assets that oblige a larger amount of control than is typically accessible from people in general cloud. Private cloud are typically utilized for a solitary business.

Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The public cloud is a blending of figuring administrations accessible on the Internet.

Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

A hybrid cloud is for the most part best-of breed. It joins the solace level of a private cloud with the adaptability and flexibility of people in general cloud.

1.3 Security Issues

According to the Cloud Security Alliance, the fundamental three perils in the cloud are "Precarious Interfaces and API's", Data Loss and Leakage", and "Gear Failure" which spoke to 29%, 25% and 10% of all cloud security power outages separately - together these structure shared development vulnerabilities. In a cloud supplier

stage being shared by unmistakable customers there might be a credibility that information having a spot with differing customers harps on same data server. In this way Information spillage may develop by blunder when information for one customer is given to other.[86] Additionally, Eugene Schultz, manager advancement officer at Emagined Security, said that software engineers are contributing extensive vitality and effort scanning for ways to deal with enter the cloud. "There are some certified Achilles' heels in the cloud establishment that are making immense crevices for the unpleasant colleagues to get into". Since data from hundreds or an enormous number of associations can be secured on significant cloud servers, software engineers can theoretically get control of colossal stores of information through a lone strike — a methodology he called "hyperjacking". There is the issue of authentic obligation regarding data (If a customer stores some data in the cloud, can the cloud supplier advantage from it?). Various Terms of Service assentions are calm on the point of proprietorship. Physical control of the PC equipment (private cloud) is more secure than having the rigging off site and under someone else's control (open cloud). This passes on amazing inspiration to open conveyed figuring organization suppliers to arrange building and keeping up strong organization of secure organization.

2. RELATED WORK

Dispersed processing is a decently new arrangement of activity in the figuring scene. As showed by the official NIST definition, "conveyed figuring is a model for engaging general, favorable, on-interest framework access to a shared pool of configurable preparing resources (e.g., frameworks, servers, stockpiling, applications and organizations) that can be immediately provisioned and released with insignificant organization effort or organization supplier correspondence." The NIST definition records five crucial characteristics of circulated registering: on-interest self-organization, wide framework access, resource pooling, quick adaptability or advancement, and measured organization. It in like manner records three "organization models"(software, stage and infrastructure),and four "game plan models" (private, gathering, open and mutt) that together request ways to deal with pass on cloud organizations. [1]

Appropriated processing is a surely understood and comprehensively recognized perspective built thoughts, for instance, on-enthusiasm figuring resources, flexible scaling, transfer of ahead of time capital and operational expenses, and working up a remuneration as-you-use arrangement of activity for enrolling and information advancement organizations. Moreover, the gathering of virtualization, organization masterminded models, and utility figuring there has been a basic progression really taking shape of cloud reinforce structures for IT organizations inside QoS limits, organization level understandings, and security and insurance necessities. The troubles related to the configuration, execution, resolute quality, security, common sense, and virtualization were all inside the degree of this issue. Interfacing contraptions, for instance, Switch , Router , Ethernet are used for making framework and one tradition called as Spanning Tree Protocol(STP) is the trading tradition learns a circle free single-way tree structure for the entire framework. [2]

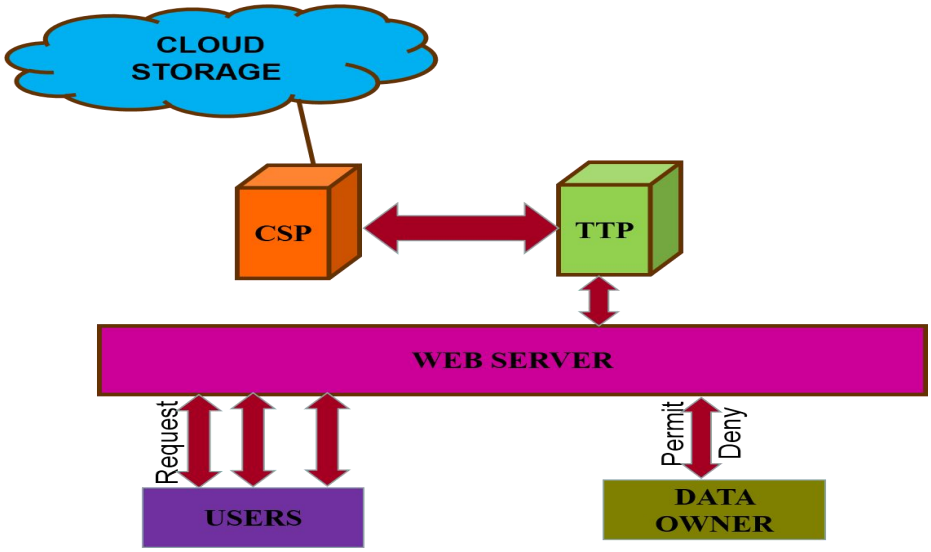
The virtualize stage decreases cost and suitable gear and programming utilize and cloud is in like manner used for data stockpiling anyway it moreover go with security challenges and customer continually pushed over data set away on cloud. The troubles take after Snooping , Cloud Authentication, Key Management, Data Leakage, Performance. To beat this troubles there are two estimations named as KeyGen computation used for delivering set of keys and TagGen count used for making emanate name key to each data part. Using this assessing structure is made in two phases, Audit and Key period. [3]

Shared force based security ensuring affirmation tradition (SAPA) is another tradition which oversees security issue for dispersed stockpiling. It gives check and endorsement without exchanging off a customer's near and dear data. In the SAPA, 1) shared access force is expert by obscure access request organizing instrument with security and insurance considerations (e.g., confirmation, data lack of definition, customer security, and forward security); 2) property based access control is gotten to comprehend that the customer can simply get to its own specific data fields; 3) middle person re-encryption is associated with give data sharing among the various customers. Meanwhile, across the board compos ability (UC) model is set up to exhibit that the SAPA speculatively has the arrangement rightness. [4]

ISSN 2348 – 8034
Impact Factor-4.022

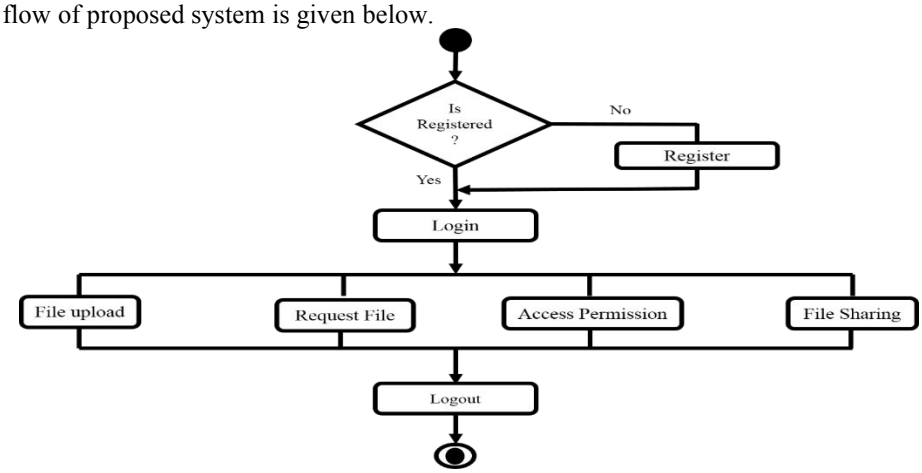
3. PROPOSED WORK

The proposed system plan is carried out in following manner.



This project solves the security issues related to cloud access as well as cloud storage. This project mainly includes securing data by encrypting it and the data access permission is totally depend on data owner that is data owner will permit or deny the access permission. So that the privacy of data owner will be preserved.

The basic flow of proposed system is given below.



4. MODULES

a. Registration and Login:

In this module an owner has to upload its files in a cloud server, he/she should register first. And a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

b. Database Connectivity:

In this module file uploading and file downloading to the database, these to actions will performed.

ISSN 2348 – 8034
Impact Factor-4.022

File Upload:

In this module Owner uploads the file(along with meta data) into database. The uploaded file was in encrypted form, only registered user can decrypt it.

File Download:

The Authorized users can download the file from database.

Uploading to cloud:

In this module, all the files present in the database will be uploaded on cloud.

Timestamp and Approvals:

Owner can permit access or deny access for accessing the data. So users can able to access his/her account by the corresponding data owner. If owner does not allow, user can't able to get the data.

5. DESIGN WORK

In this paper, we are going to show whole execution of proposed system.

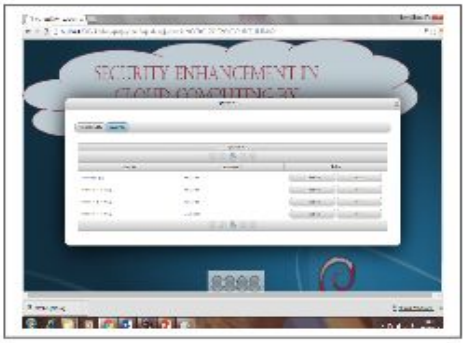
Main Page

Registration

File Uploading

ISSN 2348 – 8034
Impact Factor-4.022

File Sharing



File Downloading

6. COMPARATIVE RESULT ANALYSIS

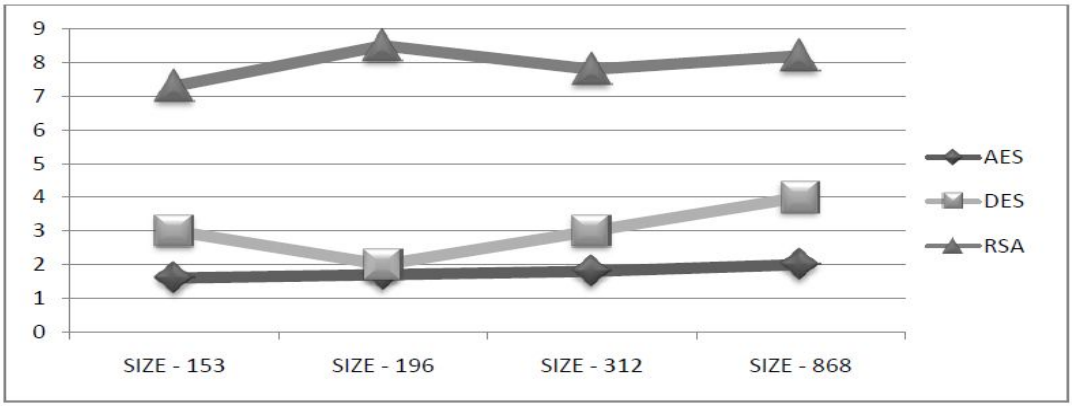
6.1Comparison between Symmetric Algorithms (Existing System)

Table 6.1 Comparison between Symmetric Algorithms

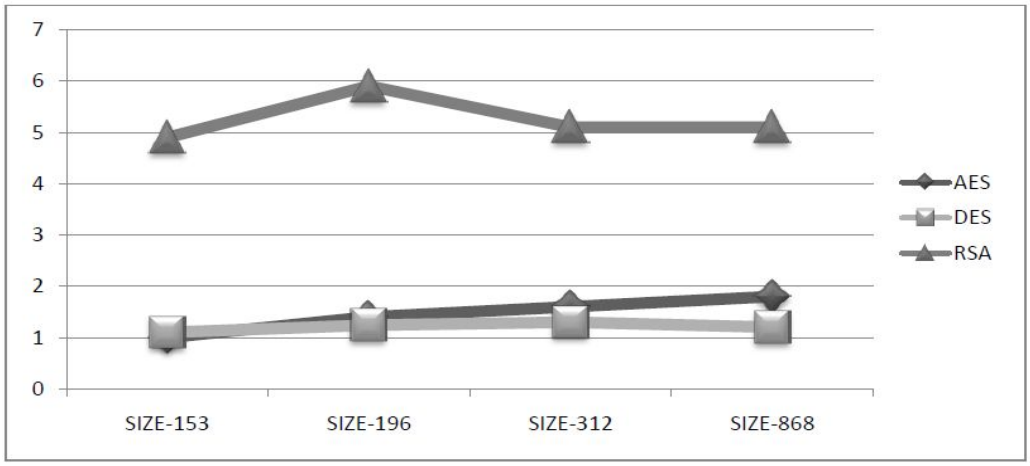
Input	AES	AES Cloud	DES	DES Cloud	BLOWFISH	Desede	Desede Cloud
10 Kb	11.5	1.5	7.5	2	4	12	4.5
13 Kb	14.7	2	10	2.5	4.7	15.5	5.25
39 Kb	21	3	31.5	6.5	8.25	47.25	10.25
56 Kb	24.5	3.75	50.25	9.25	15.7	70.5	14.5

ISSN 2348 – 8034
Impact Factor-4.022

Graph based Comparison of AES DES and RSA

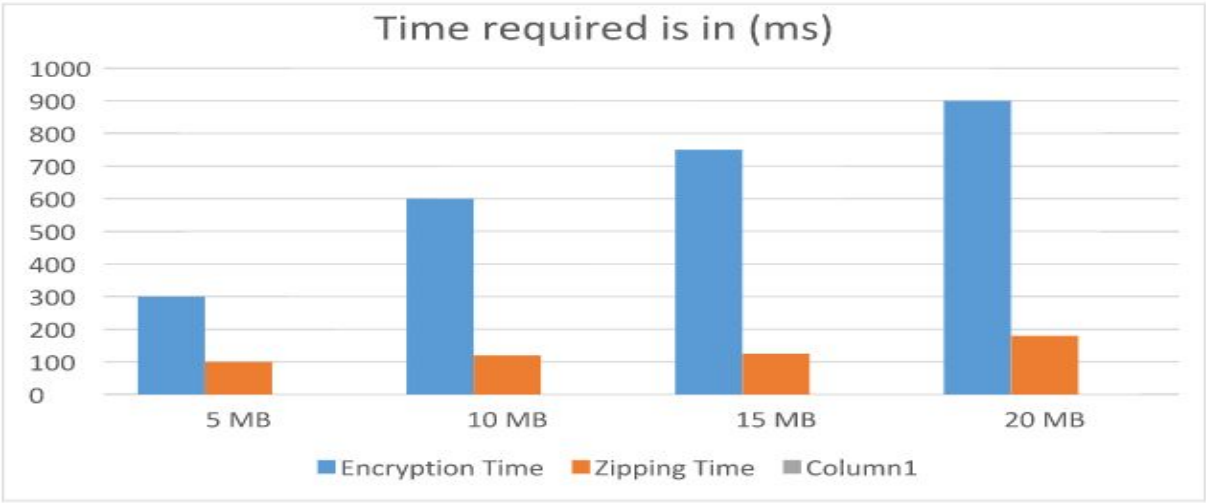


Encryption Time (in milliseconds)



Decryption Time (in milliseconds)

6.2Graph based analysis of proposed system



7. FUTURE WORK

In future we can extend following functionalities in this project:

- Use of multiple encryption algorithms for better security.
- Extending project to multi-cloud.
- Real time data sharing like audio and video conferencing.
- Strong Compression algorithm for less cloud data storage.
- Making it more user friendly.

8. CONCLUSION

The proposed framework gives security utilizing Key Aggregation and AES encryption calculation. This anticipate servers a contrasting option to key administration frameworks. The security gave is extemporize utilizing an irregular key generator which utilizes a key accumulation capacity. The proposed framework can be utilized as a part of any application which incorporates information sharing between clients (it is possible that coordinated or numerous to numerous) methodology.

REFERENCES

1. *P. Mell and T. Grance, "Draft NIST Working Definition of CloudComputing," National Institute of Standards and Technology, USA, 2009.*
2. *A.Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," IEEE Communications Magazine, vol. 50, no. 9, pp, 24-25, 2012.*
3. *K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, 2012.*
4. *A.Gomathi P.Mohanavalli ,"Anonymous Access Control by SAPA in Cloud Computing" IJCSEC, Vol.3, Issue 2, 2015, Page.848-853, ISSN: 2347–8586.*
5. *L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.*
6. *X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.*
7. *M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.*
8. *C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, 2012.*
9. *S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.*
10. *S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, 2011.*
11. *N.Vaitheeka, V.Rajeswari, D.Mahendran," Preserving Privacy by Enhancing Security in Cloud" ,IJIRCEC,* ***Vol. 3, Issue 3, March 2015.***
12. *Kopparthi Lakshmi Narayana, M.Purushotham Reddy, G.Rama Subba Reddy," Privacy Preserving Authentication With Shared Authority In Cloud", International Journal of Science Technology and Management, Vol. No.4, issue 07, july 2015.*

13. *Yerragunta Harshada , K.Janardhan," Ranking Based Shared Authority Privacy Preserving Authentication Protocol in Cloud Computing"IJIRCCE,* ***Vol. 3, Issue 5, May 2015.***
14. *R. Moreno-Vozmediano, R. S. Montero, and I.M. Llorente,"key challenges in cloud computing to enable the future internet of services",IEEEinternet computing,Vol.17,no.4,pp.18-25.*
15. *R. Sanchez, F.Almenares, P. Arias, D. Diaz-Savchez and A. Marn,"Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing" IEEE Trans. Consumer Electronics, Vol. 58. No. 1,pp.95-103,Feb.2013.*
16. *K. Yang, X. Jia. "an efficient and secure dynamic auditing protocol for data storage in cloud computing", IEEE Trans. Parallel and Distributed Systens, vol. 24, no.9,pp.1717-1726,Sept 2013.*
17. *S. Ruj, M. Stomenovic, and A. Nayak, "decentralized access control with anonymous authentication for securing data in cloud", IEEE Trans. Parallel and Distributed Systems, Vol. 25, no. 2, pp.384-394,Feb.2014.*
18. *K. W. Park, J. W. Chung, and K. H. Park,"THEMIS:A mutually verifiable billing system for the cloud computing environment", IEEE Trans. Services computing, vol. 6, no. 3, pp.300-313,July-Sept 2013.*
19. *Ashwini Khodwe, Prof. V.R. Wadhankar "A Survey Paper on security Enhancement for Privacy Preservation in Cloud Computing by Anonymous Request Access" International Journal of Research (IJR) e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015.*
20. *Ashwini Khodwe, Prof. V.R. Wadhankar "Security Enhancement for Privacy Preservation in Cloud Computing by Anonymous Request Access" IJRITCC Journal, Volume 4, Issue 1, January 2016.*