International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

SECURE CLOUD ACCESS USING AES ENCRYPTION AND DECRYPTION ALGORITHM

Rohith S[1],Ms. Varsha Pawar[2]
[1]*Student, Masters of Computer Applications, CMR Institute of Technology, Bangalore*
[2]*Assistant Professor, Department of MCA, CMR Institute of Technology, Bangalore*

Abstract - Distributed resources are shared in an open environment through network in cloud computing. As aresult, users may simply access their data from any location. Security and privacy concerns are present at the same time for a variety of reasons. First, there has been a significant advancement in network technology. Anotheris the rising need for processing power, which forces many businesses to outsource their data storage. Therefore,in an unrestricted cloud environment where the earner is unreliable, there is a necessity for protected cloud packing services. In a cloud computing context, this article discusses several data safety and confidentiality protection concerns and suggests a technique for delivering security services including authentication, authorisation, and confidentiality as well as monitoring in real time. Using the 128 bit Advanced Encryption Standard (AES), data security and confidentiality are improved. In the suggested method, information is encodedusing AES before being uploaded to the cloud. The suggested model prevents unwanted access to user data by using the Mail Service warning mechanism.

Keywords – Cloud-Computing; Cloud Security; AES; DES; Encryption; Decryption; QoS**.**

1. INTRODUCTION

Cloud-Computing is one of the utmost popular new tools, cloud computing offers a number of ways to buy and manage massive amounts of IT resources. The provision of various services by cloud computing includes foundation as-a-administration (IaaS), otherwise called equipment as-a-administration (HaaS), stage as-a- administration (PaaS), and programming as-a-administration (SaaS). Making arrangements for Cloud Computingempowers asset partaking in an unadulterated fitting and offers a methodology that fundamentally lessens foundation intricacy.

As distributed computing exists another new innovation notwithstanding having numerous advantageous elements, it faces numerous dangers in different ways. To give the security with corrupting the presentation. In this undertaking we propose an entrance control model highlighted with the effective key update capability in information rethinking climate. Our entrance control depends on the mix of Encryption text strategy - Attribute based Encryption (CP-ABE) and job based admittance control (RBAC).

Compared to the current CP-ABE based systems, this considerably lowers the overheads of updating and delivering keys to all users concurrently. Decentralized Multi-Authority ABE (DMA-ABE), a variant of CP-ABEthat is resistant to this sort of bad behaviour, is derived from CP-ABE. Our approach makes a distinction betweenan information proprietor (DO) head and quality specialists (AAs). The DO claims the information, however AAsare given the power to referee access by giving clients admittance to the suitable quality marks. Over these properties, policy encryption safeguards the data.

Cloud computing will be figuring idea where an extraordinary pool of systems associated each other in isolated or exposed systems. They give increasingly multipurpose base to application, gen and file storing. The thought behind Cloud computing is major main of 'reusability of IT assets'. In Cloud

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

computing the applications and administrations keep running on scattered system utilizing virtualized assets and got to by regular web conventions and system models. Cloud computing has two elements. Abstraction: The system implementation information is hidden from the users and data is stored in locations that are unknown to the user. Virtualization: All the IT related resources, network and applications are virtualized to provide the implementation independent infrastructure.
A cloud conveys programming, storage, and system or oversaw administrations to client customers by means of a system, for example, Internet. Cloud computing or cloud is conveyed on system (Internet or private intranet). Clients can get to administrations on gadget, for example, desktop or cell telephone or web programs.

1. **Hybrid cloud:** This is combination of atleast double clouds, where cloud comprised remain sharedof private cloud, open cloud and pubic cloud. Community cloud: This is designed for some organization. This cloud may share among two or more associations that have comparative cloud prerequisites.

Service Model
These are cloud service owners that users can subscribe. These three representations differ in the quantity ofcontrol that consumers have their information and purpose of service provide.

- **Software as a Service:** This service model provides both resources and applications. Sales forces,Google and Microsoft etc. companies offer SaaS.
- **Platform as a Service:** This administration model gives access to the parts that they require creatingand working application over web. It provides system development and runtime environment. Google's App Engine is PaaS example
- **Infrastructure as a Service:** This service model provides hardware properties such as servers, datacenter space, storage interacting services with virtualization. Some examples are Amazon, 3tera etc.

2. LITERATURE REVIEW

M.Armbrust, A. Fox, et.al [1], have proposed to give the hindrances are conquer, the cloud computing can perhaps change a vast part of IT industry, building programming more alluring as a management and decorationthe way. Its equipment is composed and obtained. Engineers have innovative ideas for new,

DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

user-friendly websitesthat don't require them to invest a lot of money in expensive machinery to put their management or their employees to work.
The economies of size significant scale server ranches merged with "pay more only as costs arise" resource use has broadcasted the rising of distributed computing, it is right now charming to send an imaginative new organization access on the outcast web server ranch rather than your own framework, and to easily scale its resources as it creates or diminishes in reputation and pay.
Developing and contracting every day in contrast with run of the mill diurnal occurrences could additionallysave costs. With dispersed registering, the risks of over or under provisioning are moved to the disseminated figuring give, who diminishes that bet by really multiplexing over significantly greater clients and who offers reasonably unassuming rates due to better use and the economies of scale.

M. Green, S. Hohenberger and B. Water, et.al, have proposed to trademark based encryption is one more ideaaimed at open key encryption that grants client to encode also translate communications considering client characteristics, the new perspective for ABE that generally abstains from this above for clients.
Accept that ABE figure works are taken care of in the cloud. It exhibits the way that the user be able to outfitthe cloud with single tranformation key that permits the cloud to unravel any ABE consider content fulfilled by those client's characteristics close by an expected size lacking the cloud taking the option to review any section of the client's communications.
To portray & show the potential gains of this methodology thy give fresh security meanings to both CPA and repayable CCA security without-getting a few now upgrades a usage of our estimations and straightforward execution assessments. The normal course of action the client saves basically on both exchange speed and unscrambling time, without creating how much transmissions.
As the fundamental responsibility of our work they set up an indispensable and relationship between irrefutable estimation and properties-based encryption, a crude that has been comprehensively inspected. They are unquestionable nature computation plan with open arrangement and open conspicuousness from any ABE plan.
The VC plan checks any limit in the class of limits encased by the sensible ABE approaches. This plan valuesa very compelling affirmation computation that relies just upon the yield size. Building up this affiliation, it exhibits the improvement of multicapacity confirmable estimation plan from an ABE with re-evaluated unscrambling an out of date portrayed lately.
J. Han, W. Susilo, have proposed the accelerating of apportionment of distributed computing among tries. Inany case, moving the base and sensitive data from solid region of the data owner to open cloud act outrageous security and assurance risks. Property based encryption-(ABE) is one more cryptographic which gives a guaranteeto watching out for the issue of protected and fine-grained data dispersion and decentralized right of section control.
Key strategy normal based encryption (KP-ABE) is a basic kind of ABE, engages despatchers to scramble messages under game plan of characteristics and isolated keys are connected with access models that demonstratewhich figure messages the key compartment will be reasonable to unscramble. In KP-ABE plan, the figure contentdegree becomes straight with amount of properties embedded in figure content. They propose another KP-ABE advancement with steady figure content extension.
In this model, the entrance procedure can be enunciated as any robot access model. The code text extension is free of how much code text credits and the quantity of bilinear blend evaluations is consolidated to a consistent.Our plan is semantically protected in the set model in view of the Daffier-Hellman type presumption
They have made another KP-ABE plan supporting any monotonic access improvement with consistent

DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

size figure message and exhibited that the organized arrangement is semantically secure specifically set model thinking about the overall Daffier-Hellman model declaration. The deterrent of the proposed KP-ABE plan is thatprivate keys have various size improvements in the amount of characteristics in the entry structure.

One charming open issue is foster a KP-ABE plan with consistent size figure messages that is secure under amore standard doubt or which achieves a more grounded full security thought. Another testing issue is to constructa KP-ABE plan with reliable figure content size and consistent confidential key size.

They show ABE plan for courses of any abstract polynomial degree, where the overall boundaries and the figure content become straight with the significance of the course. The advancement is protected under the regularlearning with botches notion. Past advancements of idiosyncrasy made encryption were for Boolean conditions gotten by the versatile quality class NC.

3. System Model

We must understand the security problems in the cloud environment and the significance of AES between extra encryption algorithms before debating the suggested system in depth.

A. Cloud Computing Safety Problems

Cloud Security: A growing area within the larger fields of data security, network security, and computer securityis cloud computing security. It describes a broad range of measures put in place to safeguard information, programmes, and the interconnected architecture of cloud computing.

Security Problems Linked with the Cloud: There are several security problems that arise with cloud computing.Users should inquire about seven security issues when choosing a cloud vendor: limited user access, monitoringcompliance, data location, data separation, rescue, research maintenance, and long-term sustainability. The CloudSecurity Alliance (CSA) takes recognised security problems in various cloud regions and also provides safety recommendations. An overview of security problems in cloud service provision replicas with detailed analyses of each issue. Data Centre Information, a top source of current events online, examined issues with data centre security. They say that there have been cloud outages, data losses, and security flaws.

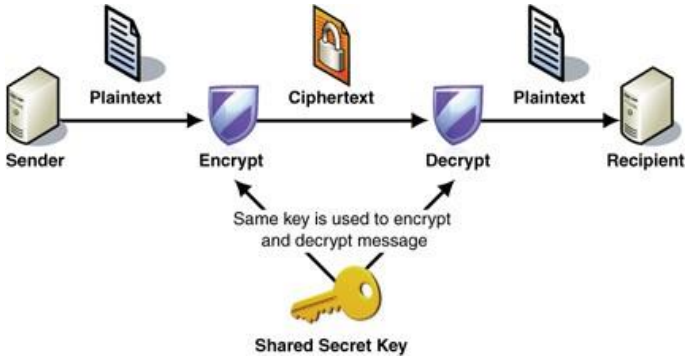
B. Encryption algorithms

The two primary categories of encryption algorithms are symmetric key encryptions and asymmetric key encryptions. A single secret key is utilised in symmetric key encryption for both encryption and decryption. Withan asymmetric key, the secret key is used for decryption while the public key is used for encryption. AES is a kind of symmetric key encryption.

AES: The best encryption method has been replaced by NIST with AES (Advanced Encryption Standard). A block cypher algorithm with symmetric keys is used. The 3 fixed 128-bit block cyphers used by the AES algorithmhave cryptographic keys of 128 bits, 192 bits, and 256 bits. Keys can be any size, but blocks can only be a maximum of 256 bits. It is quickest, most adaptable, and secure to use AES encryption. It is supported on a varietyof platforms, including tiny devices. The National Institute of Standards and Technology (NIST) released this method in 2001. AES is a symmetric block encryption designed to take the role of DES. The plaintext input sizefor the encryption is 18 bits. The maximum key length is 128.192.256 bits. Depending on the length of the key, the algorithm is known as AES-128, AES-192, or AES-256. Depending on the key length, the cypher has N rounds: 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key. Four transformation functions are used in the first N-1 round: one permutation (Shift Rows), three replacements, and (Substitute bytes, Mix Columns, AddRoundKey). There are just 3 phases in the final encryption and decryption procedures. Byte by byte replacement is done using the S box. Math over GF is used by Mix Columns Simple bit-

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

wise XOR of the current block and a piece of the extended key is what AddRoundKey does.



C. Why AES Encryption?

Comparative evaluation of the security, ease of h/w and s/w operation, speed of encryption and decryption, and other factors of the encryption algorithms DES and AES. Built on the period for encryption and decryption, a comparison of three distinct encryption techniques AES has been conducted. Manuscript files of various sizes are used as the input to test the encryption and decryption times. RSA takes the longest to encrypt data, accordingto their testing, whereas AES takes the least time. They came to the conclusion that the AES algorithm is far superior to the DES and RSA algorithms based on their findings. AES is the fastest and safest. The fastest and safest delivery of services to the clients is currently a major issue that all organisations and suppliers confront. The degree of user happiness affects a system's security as well. Thus, before uploading to the cloud, the suggestedmethod secured user data using encryption. Since the AES algorithm is quicker and more secure than other methods, it is utilised for data encryption and decryption.

D. Problem Statement

In turn, cloud computing offers a variety of services, including infrastructure-as-a-service (IaaS), often referred to as hardware-as-a-service (HaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Public, Private, and Hybrid Cloud are the three main types of deployment methods that the cloud offers. Exceptionally believed cloud clients might be conceded full access honours while different clients are given restricted admittance freedoms to the re-appropriated information to keep up with the security of the cloud's information. To deliver better security features in cloud-computing environment and for fast accessing our systemprovides hybrid encryption using CP-ABE and RBAC generating token as key in distributed system. This ensurehigh security among the cloud users and has full access to all the users very securely.

E. Existing System

The present method in cloud is centralized and only limited users with partial rights and only for few full rights to access the data is provided to ensure the security. The encryption takes place using only ABE attribute-based encryption and the same key is distributed through web service. As the user increases it falls down with security and performance wise.

Disadvantages

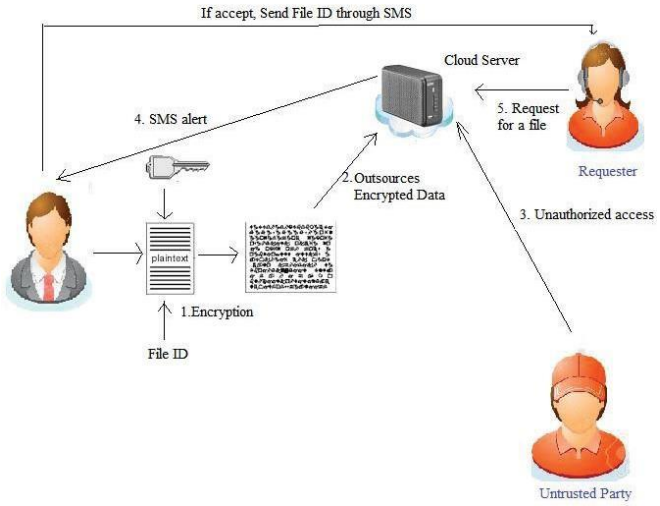
- The System is less secure
- Only partial rights and few full rights to access the data is provided
- Key sharing through we service is not that safe

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

- As it is centralized performance is low
- Overloaded with memory.

F. System Module

Three elements make up the suggested system: a customer, one cloud controller, and other nodes. Created onthe appeal and reply times during file upload, delays were measured. The complete system architecture is depictedin Fig. below.



Administrator

Administrator is in charge for providing the authentication access to the users in order to upload or access the files.

Data Owner

Data Owner would register for the account at first and then the secure authentication code will be sent to him through the registered mail ID. After login he will upload the file which has to be sent to the consumer by adding a public key which further goes to the admin for approval. Once the admin approves the file the consumerwill be able to download or view the file.

Data Consumer

Data Owner would register for the account at first and then the secure authentication code will be sent to himthrough the registered mail ID. Then the consumer can login with his username and password after that he will be able to download or view the file.

G. Software Requirement Specification Cipher Text Attribute based Encryption

The definition and the security model of our CPABEs. In such a framework, a route figure content approach property-based encryption plot, a symmetric encryption plan and an encryption system are applying toguarantee the secrecy, the fine-grained control and the unquestionable appointment.

CA-CPABE defined by a data of algorithm. The explanation of each algorithm is as follows:

- **Setup:** Executed by the key Distributer, this calculation takes as info a safety parameter S, the quantity of traits n, the preeminent depth1 of the circuit. It yields people in general parameters PKsand master key MKs which is kept private.
- **Hybrid-Encryption:** The algorithm is performed by the data owner. It might be suitably divided to dual parts. They are:

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

- **Key wrapping mechanisms-(KWMs):** The KWMs takes as response the public key PK. Itcomputes the accompaniment route f and selects a random word RW.
- **Authentication symmetric encryption-(AE):** This receipt as input a key MKs, the randomword R, the symmetric key

Access Control Model AC-CP-RBAC

At centre of the model, RABE is coordinated into CP-ABE to improve the expressiveness of CP-ABE strategy particular and deal with a gathering credits in the CP-ABE component.

Digital Token Generating

To sustain the security of the outsourced data, key structures were created. Key structures are derived from user properties like roles that are common to all users. The creation of key structures grants a group of common user's access rights to the data that has been outsourced. Using Pseudo Random algorithm produces unique big length keys using 256 characters

Pseudo Random Key Generation algorithm

Stage 1: Generate 32-pseudo arbitrary byte with the seed key generator, adding the client provided seed, U, ifany.

Stage 2: Set the 192-digit Triple DES key- K, as the initial 24-bytes produced in sync 1, and set the seed, S, asthe last 8-bytes.

Stage 3: A 64-cycle portrayal of the ongoing dot and time ought to be set as D.

Stage 4: Create the 64---bit block X0 = G ---- (S, K, D), where G is the ANSI X9.17 RNG calculation indicated in

Appendix C/Appendix A, and where S is refreshed utilizing that calculation.

Stage 5: a framework for running tests on an irregular number generator consistently:

Quit testing the consistent irregular number generator if either X0 rises to L or X0 approaches P.For the following call, set L = X0 and store it in string safe memory.

Set P = X0.

Stage 6: up until R approaches zero, for R = N, perform:

Make a 64-bit block with the equation X = G (S, K, D), refreshing S as you go.

Assuming X is identical to the recently delivered block, P, the consistent arbitrary number generator test comesup short, and it is halted.

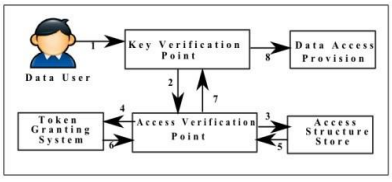
The more modest of R and 8 is set B.From X, yield B bytes.

Set R = R - B.

Set P = X.

Stage 7: Create a last block with the equation Xf = G (S, K, D), then, at that point, set P = Xf.

Stage 8: zero out all inner cushions that were used, including K, S, D, X. Keep L and P around for some timelater.



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

Email Authentication

Email verification is a social affair of methodologies went for planning messages of the email transport structure with clear data. It is a coarse-grained insistence, for the most part at Administrator Management Domain-(ADMD) level, and proposes kind of support.

That is, support for email certification is to recognize the characters of the social gatherings who looked at exchanging a note, as thy can change the message. The results of such affirmation can then be utilized as a pieceof transport choices, which are past the level of email certification fitting, and are very specific in nature Receiving E-mail: Receivers can use affirmation to really look at the wellspring of a received message and swear off phishing stunts. For example, in case you get mails ensuring to be since google.com then again are not genuinely genuine as starting from google.com, these are pushing messages. You would not arrive or guide somewhat singular info. Recollect, Google won't ever demand that you send individual gen.

4. System Design

Social affair of methodologies went for planning mails of the email transport structure with clear data. It is acoarse-grained insistence, for the most part at Administrator Management Domain-(ADMD) level, and proposeskind of support.

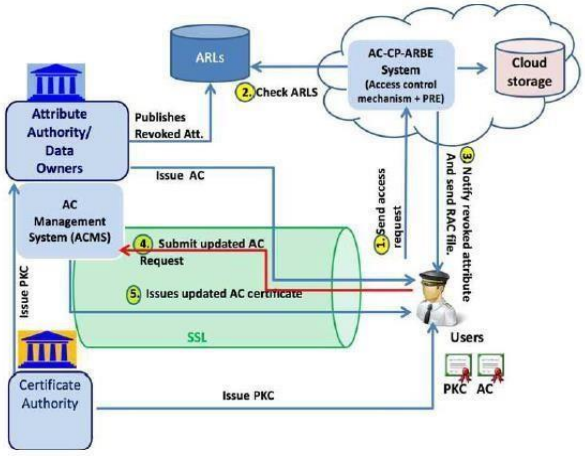
That is, support for email certification is to recognize the characters of the social gatherings who looked at exchanging a message, as thy can change the message. The results of such affirmation can then be utilized as a piece of transport choices, which are past the level of email certification fitting, and are very specific in nature-- Receiving E-mail: Receivers can usage affirmation to really look at the wellspring of a received message and swear off phishing stunts. For example, in case you see mails ensuring towards be since google.com, but then again are not genuinely genuine as starting from google.com, these remain phasing messages. You would not entry or direct any singular data. Evoke, Google won't ever demand that you send individual gen.

The model contains of following separate level:

✓ Requirement and Definition: In this level the reprobate is indicated alongside the needed administrationtargets and the imperatives are distinguished

✓ System and Software Designing: In this level the plan details are deciphered into a product depiction. The product engineer at this level is on edge with information structure, programming design,calculation subtle elements and interface depictions.

✓ Implementation: In this level the outlines are deciphered into the product space.



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 Aug-Sept – 2022
DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

✓ Component, Integration and System Testing: Testing at this level concentrates on ensuring that any mistakes are perceived and that the product meets its required necessity. After this stage the product is conveyed to the client

✓ Processes and Maintenances: In this level the product is effective to meet the changing client needs, acclimated to oblige assortments in the external climate, right slip-ups and rejections in advance undetected in the testing stages, updating the efficiency of the item.

5. RESULT

One system serves as the controller in this architecture. Anyone with internet connection can use the programme at any time and from any location. The programming languages utilised to create this application areJAVA and JSP. HTML was used to construct graphic user interfaces (GUI). Displays the proposed model's activities and overall system design. This system's safe exchange of private information, such as medical records,personal identifiers, and financial data, is one of its key applications. If a user wishes to utilise our programme tosubmit their sensitive data, they must first register with a working email address and cell phone number. Their account's username and password are user-defined, not structure clear. They can log in as a user after a successfulregistration. The user can then utilise the file upload module to upload the sensitive file. The user is given a window to encrypt their file as discrete blocks before sending it to the cloud. After creating a secret file ID for later access and sharing, press the "Save" button. The file will upload to the database on the server. Medical records may be shared with a doctor at any time, from any location, thus there is no need for the patient to carry about a paper copy or a digital copy of their records at all times. All they need to do is keep their top-secret folderID in mind. The folder ID can be any combination of integers, alphanumeric characters, different characters, or everything else the user chooses. The length of the file id is unlimited. The user may examine the amount of timeit took to upload their material.

6. CONCLUSION

This it to guarantee the information secrecy, the Fine-grained access control similar approval in cloud. In thehybrid encryption there are several keys namely, random encryption, symmetric, one time verified key for different purpose enhance the security of the system. The key distribution for accessing the file on the cloud andto decrypt that we use the Gmail service to distribute the generated key among the data consumer.

Therefore, as this system is highly secured with data uploading and downloading. The system is more securedagainst malicious attacks.

Compared to the current CP-ABE based systems, this considerably lowers the overheads associated with concurrently updating and distributing keys to all users. Decentralized Multi-Authority ABE (DMA), a variant ofCP-ABE that is resistant to this sort of bad behaviour, was developed. Our approach makes a distinction betweena data owner principal and attribute authorities. The data owner owns the data, but attribute authorities are given the authority to arbitrate access by giving users access to the appropriate attribute labels. Over these properties, policy encryption safeguards the data.

Finally, our system is highly secured as hybrid encryption on CP-ABE and RBAC to secure the data and keyto decrypt is token generated and shared in the distributed system. The decentralized system helps in the parallelcomputing the secure transaction between the users efficiently with high performance in cloud.

DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

7. FUTURE ENHANCEMENT

This study examined current security concerns in the cloud computing environment and suggested a fresh approach to safeguarding cloud data in practical settings. Access control, authenticity, and secrecy are all provided via 128 bit AES encryption. Then, depending on delay, the performance of the suggested technique was examined.From this data, we deduced that the latency dramatically increases as the file size increases. Future research suggests a brand-new approach to smart data storing in which the storage nodes are valued according to the pastof prior attacks.

Stronger security features must be included in the cloud computing environment and for fast accessing our system provides hybrid encryption using CP-ABE and RBAC generating token as key in distributed system. Thisensure high security among the cloud users and has full access to all the users very securely. Our system is highly secured as hybrid encryption on CP-ABE and RBAC to secure the data and key to decrypt is token generated and shared in the distributed system. The decentralized system helps in the parallel computing the secure transaction between the users efficiently with high performance in cloud.

We have completed with collecting the base papers and analysis on the methodologies to be used. Prepared the designs containing in this report. Next phase we would be starting with implementation of the methodologiesto provide security to our medical system and test the system using test cases.

8. REFERENCES

1. P. Mell, Grance, “The NIST definition of cloud computing”, Natl. Inst. Standards Technol.(NIST), U.S.Dept. of Commerce, Gaithersburg, MD,USA, NIST Special Publication; Sep.2011, pp. 800-145.
2. Hyun-Suk Yu, Yvette E. Gelogo, K J Kim, “Securing Data Storage in Cloud Computing”, J. of SecurityEngineering, June 2012, pp.252-259.
3. C.W. Hsu, C.W. Wang, Shiuhpyng Shieh, “Reliability and Security of Large Scale Data Storage in Cloud Computing”, part of the Reliability Society Annual Technical Report 2010.
4. Qian Wang, Cong Wang, Jin Li, Kui Ren, Wenjing Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing”, IEEE Systems Journal, Vol.9, No.1, August 2015.
5. http://www.datacenterknowledge.com/archives/2015/03/16/securitybreaches-data-loss-outages-the-bad-side-of-cloud/
6. Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Ensuring data storage security in Cloud Computing",IEEE 17th International Workshop on Quality of Service (IWQoS) 2009, pp. 1 - 9
7. 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, Vol.13, Iss. 15, Vol. 1, 2013.
8. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing”, V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, retrieved on 19th November 2015.
9. Wentao Liu, "Research on cloud computing security problem and strategy", IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 1216-1219.
10. “Gartner: Seven cloud-computing security risks”. InfoWorld. 2008-07-02.
http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853, retrieved on 6th March 2016.
11. Deyan Chen, Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, IEEE International Conference on Computer Science and Electronics Engineering, 2012, pp 647-651.

DOI:10.46647/ijetms.2022.v06i05.072 ISSN: 2581-4621

12. Ateniese, Giuseppe, “Provable data possession at untrusted stores”.ACM Conference on Computer andCommunications Security. ACM Press; 2007, pp. 598-609.
13. Ashalatha R, Vaidehi M, “The Significance of Data Security in Cloud: A Survey on Challenges And Solutions on Data Security”, International Journal of Internet Computing, Vol, 1, Iss. 3, 2012, pp.15- 18.
14. S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”,Journal of Network and Computer Applications, Vol. 34, Iss. 1, Jan 2011, pp.1–11.
15. Paul C. H., S Rao, C B. Silio, A Narayan, “System of Systems for Quality-of-Service Observation andResponse inCloud Computing Environments”, IEEE Systems Journal. Vol.9, No.1, March 2015, pp. 212-222.
16. D Ardagna, G Casale, M Ciavotta, J F Perez, W Wang, "Quality-ofservice in cloud computing: modeling techniques and their applications", Journal of Internet Services and Applications, 5:11, 2014, pp. 1-17.
17. S.Lee, D.Tang, T.Chen, W.C.Chu, “A QoS assurance middleware model for enterprise cloud computing”, IEEE 36th Int. Conf. on Computer Software and Application Workshops, 2012, pp. 322-327.