Encrypted Data Sharing in Cloud data storage using Cloud Computing

JAMPANA POOJA SRI MANI
Student of M.Tech (CSE), Department of Computer Science & Engineering, Kakinada Institute Of Engineering And Technology, KORANGI, AP, India.

SATTI VIJAYA KRISHHNA REDDY
Asst. Professor, Department of Computer Science & Engineering, Kakinada Institute Of Engineering And Technology, KORANGI, AP, India.

Abstract: **To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, Ciphertext-Policy Attribute-based Encryption (CP-ABE) can be utilized to conduct fine-grained and owner-centric access control. But this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provider the capability to verify whether a downloader can decrypt. Therefore, these files should be available to everyone accessible to the cloud storage. which will largely consume the cloud resource. The payer of the cloud service bears the expense. Besides, the cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners. These concerns should be resolved in real-world public cloud storage. In this paper, we propose a solution to secure encrypted cloud storages and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE. We present two protocols for different settings, followed by performance and security analysis.**

Keywords: **Cloud Service Provider; Cp-Abe; Access Strategy; Cloud Storage;**

I. INTRODUCTION

Cloud computing is a rising innovation with lower cost, shared assets and depend based on the shopper request. Because of various qualities, it has impact on IT spending plan and effect on security, protection, and security issues. Every one of those CSPs who wish to appreciate this new inclination should take great care of the issues. Client not comprehend where the data is put away, who handle different vulnerabilities that can happen and data. Following are a couple of issues which can be stood up to by CSP while executing cloud services. Cloud computing is innovation that enables client to get to programming application, store data, create and test new programming, make virtual server, draw on unique IT assets, and all the more everywhere throughout the web. Cloud computing is model driven technique that gives configurable computing assets, for example, server, system, storage, and application as and when required with least endeavors over the web services. Cloud additionally demonstrates fundamental attributes, conveyance model, and arrangement model. Cloud are require data focus however the point of cloud computing is to wipe out the need to consider data focus. A data focus is an office used to house PC framework and related segment, for example, media transmission and storage framework. It incorporates repetitive reinforcement control supplies, excess data correspondence associations, natural control (e.g. aerating and cooling, fire concealment), and security gadgets. Data focus are fixing to territory with particular segment including excess power supplies, repetitive correspondence, condition control, security gadgets, and so on. Cloud are area free, giving disconnected form of data focus part that are not fixing to a particular data focus: virtual server, virtual storage, virtual systems administration, and so forth. Unwavering quality and repetition originates from cloud supplier utilizing numerous data focus, so cloud more likely than not traverse at least one data focus, however themselves are not data focus. Cloud computing is a tremendous idea. Huge numbers of the calculations for stack adjusting in cloud computing have been proposed. A portion of those calculations have been outlined in this postulation. The entire Internet can be considered as a cloud of numerous associations less and association arranged services. So the detachable load booking hypothesis for remote systems depicted in [9] can likewise be connected for clouds. The execution of different calculations have been considered and looked at. Cloud computing is developing as another worldview of vast scale circulated computing. It has moved computing and data from work area and compact PCs, into vast data focuses. As a piece of its services it gives adaptable and simple approach to keep and recover data and files particularly to make extensive data sets and files accessible for the spreading no. of clients around the globe. Cloud computing gives the distinctive kinds of services that are based in pay-as-go model. Client can take services on cloud running from web application to logical application. These services are conveyed to the client over the web.

II. RELATED WORK

[1] J.K.Liu-"Fine-grained two factor get to controls for electronic cloud computing services":Fine-grainedtwofactor access control convention for online cloud figure services, it is generally utilized as a part of online application. The two elements are Secret key and Light weight security gadget.The client can be conceded get to just in the event that he utilizes those two components. Something else, the client can't utilize his mystery key with another gadget have a place with others for the entrance. At a similar minute, the security of the client is preserved[4]. The cloud framework just realizes that the client has some required attribute, however not the first character of the client. Touchy data might be put away in the cloud for helpful access and qualified clients may likewise get to the cloud framework for different applications and services, client verification is a basic segment in cloud framework for that client is required to login before utilizing the cloud services or getting to the delicate data put away in the cloud[5]. [2]X.Xie-"An Efficient Cipher PolicyAttributeBased Access Control towards Revocation in Cloud Computing":In this paper the data proprietor (DO) scrambling the data previously distributing in to the cloud, and after that circulates the mystery keys to every single approved datum clients (DUs). In this acheive data confidentiality and access control through after ways: (1) DO scramble a record F with an at irregular private key k1 and sends the ciphertext C1 to the cloud; (2) If a DU needs to get to E (F), he/she initially sends the demand to DO, thenDO reaction the k1 and access allow by means of a safe channel; (3) DU recovers E (F) from the cloud storage by the allow and after that utilizations k1 to unscramble it.This framework can ensure the data security in a manner by which neither unapproved clients nor the untrusted CSP could get the plaintext.The get to arrangement renouncement is expensive, in light of the fact that DO needs to recover the data, and re-encode and re-distribute it[13]. [3]T.H.Yuen-"K times attribute-based unknown access control for cloud computing": In this paper, a client can approve itself in the cloud. The server just knows the client secure some fundamental attribute, yet it doesn't be regular with the distinction of this client. In k-times is essentially point of convergence in the individual from staff serving at table may restrain a careful arrangement of client to get to the framework for a greatest k-times inside a period or an event.Userscan not get to if login check surpasses given k limits[6]. We additionally demonstrate the confidentiality of our instantiation. It can be utilized to give boundless circumstances unspecified validation. In any case, in the cloud computing condition, boundless circumstances get to control is at times unattractive[7]. Give us a chance to take Netflix has its service in the cloud by empowers its client to get to the motion pictures online[8].

III. PROBLEM STATEMENT

In the Existing framework the entrance code will be sent to the versatile utilizing that client login to the site. Access code security isn't there.it display a secret key insurance plot. That includes a little measure of human computing in an Internet-based condition, which will be impervious to phishing tricks, Trojan stallions, and shoulder surfing assaults. As touchy data might be put away in the cloud for sharing reason or helpful access; and qualified clients may likewise get to the cloud framework for different applications and services, client verification has turned into a basic segment for any cloud framework. A client is required to login before utilizing the cloud services or getting to the touchy data put away in the cloud.

IV. RISKS IN CLOUD COMPUTING

Risk in Cloud Computing:

Much worry in cloud computing which can't be all around ensured by customary security approaches. Cryptography is best practice for securing information very still at the cloud supplier. Luckily hard drive makers are currently conveying self-encoding drives construct encryption. Encryption ought to likewise be utilized for information in collapsible verification and uprightness assurance guarantees that information just goes where the client needs. Cloud suppliers has solid that address legitimate issues every client must have its lawful specialists examine cloud supplier policy's guarantee their sufficiency.

Similar Study:

Contrast with past investigation progressive model have various proprietors who may scramble as per their own specific manners, every client acquire keys from each proprietor whose records needs to peruse would constrain the availability are not generally online process. Option is to utilize a focal specialist to do the key management in the interest of all record yet require to trust on a solitary expert may bring about issues. Looking at above investigation our work demonstrates secure sharing of progressive characteristic construct encryption put away with respect to semi-trusted servers and concentrate on tending to the confounded and testing key management issue. Accomplishes adaptability because of its various leveled structure additionally acquires adaptability and fine grained get to control in supporting compound characteristics of different esteem assignments for get to close time to manage client denial more productively than existing plan. Utilizing property based encryption approaches are communicated in view of the traits of clients or information which empowers patient to specifically share records among policy of clients by encoding the document under a policy of credits without the need to know an entire rundown of clients.

V. METHODOLOGY

Supported by the necessities in the cloud, we change the interpretation of CP-ABE with evident distribution and there a physical structure to comprehend circuit's figure content strategy standard half breed encryption with undeniable assignment (CPABE). To keep up information classified and achieve fine grain right of passage control, our preparatory point is a circuit key policy property based encryption. We give the counter impact circuit CP-ABE structure in this archive for the premise that CPABE is hypothetically prior to the regular right of passage control strategies. For the fundamental ability issues of ABE, going before structures gave a ready system to outsource the lion's share straightforwardness of decoding to the cloud. In any case, there is no affirmation that the proposed result returned to by the cloud is constantly exact. The cloud server may fake figure content or cheat the qualified client that despite everything he doesn't have assentions to unscrambling. To validate the rightness, we make greater the CP-ABE figure content into the quality based figure content for two relating approaches and put in a MAC for each figure content, so that whether the client has understandings he/she could pick up a secretly settled key to check the precision of the distribution and keep from impersonation of the figure content. Trying at extra enhancing the capability and giving unconstrained clarification of the asylum confirmation, the idea of cross breed encryption is excessively presented in this work. Plus, asylum of the CPABE framework ensures that the sad cloud won't be sharp to study whatever thing about the scrambled message and fake the special figure content. From that point forward, the proposed plan is recreated in the GMP library. At last; the framework is refined to be sensible in the cloud.

A. System Overview

The client registers himself at server and afterward login with legitimate username and secret key into framework. After login, client ask for keys to CP-ABE [1]. The client/proprietor scramble the records utilizing the keys and transferred these documents at cloud server for particular time interim and turn out to be free from the weight. At the point when any client leave the gathering ,the rundown of outstanding client is send to CP-ABE, where the CP-ABE create the new key or refresh the keys to keep up the security of the framework and send the new keys to the key asked for client. At cloud server if the predetermined time for the document is end then the record is destructed/erase from the server and it is no longer accessible for clients. This expands the storage room at cloud server.

In past work the framework stores the information at cloud server and the client itself has erase the information put away at cloud in the event that he no longer required the information, it builds overhead of client and furthermore utilizes more space at cloud server, to conquer the disadvantage of past framework, the framework genius postures information self-distractive plan, In this client transfer the information at cloud server for particular time duration.at cloud server information is substantial for just a single year i.e. from begin date to end date determined by client after finish of day and age information is self-destructed from the cloud and it liberates the space at cloud server.

B. Key policy Scheme

The Scheme called key-policy attribute based encryption with time determined traits plot, which depends on investigation that, in sensible cloud application circumstance, each information thing can be connected with an policy of properties and each property is connected with a particular of time interim, showing that the encoded information thing must be unscrambled between on a predetermined date and it won't be recoverable that day. In which each client’s key is related with a get to tree and each leaf hub is related with a period moment the information proprietor scrambles his/her information to impart to clients in the framework. As the coherent articulation of the get to tree can connote any coveted informational collection with at whatever time interim, it can achieve fine-grained get to control. On the off risk that the time moment is not in the predefined time interim, the ciphertext can't be decoded, i.e., this ciphertext will act naturally destructed and nobody can unscramble it on account of the close of the protected key. Along these lines, secure information implosion with fine-grained get to control is accomplished. So as to decode the ciphertext successfully, the legitimate characteristics ought to satisfy the get to tree where the time moment of each leaf in the clients key ought to have a place with the in the coordinating quality in the ciphertext.

VI. PROPOSED WORK

We go for usage of cloud based framework which manages the key escrow issue in information security and make coordinate correspondence occurs between the distinctive clients utilizing cloud specialist co-ops and additionally attempt to diminish the server side load. Get to control is a standout amongst the most imperative security components in cloud computing. In this propose Attribute based get to control conspire we gives an adaptable approach that enables information proprietors to incorporate information get to strategies inside the scrambled information. Additionally in propose framework we will develop the framework to manage the significant drawbacks of existing framework like key escrow issue in information sharing and execution corruption issue.

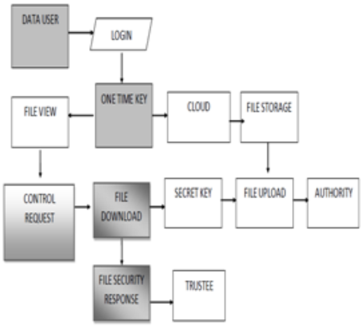

Fig. Proposed Architecture

The proposed scheme is being analyzed for the characteristics of security

Authentication and Authorization

The user is authenticated and authorized by a multi – factor and multi-step approach at the cloud service center. All the interactions of the owner of the data and cloud service is also authenticated, the mechanism followed is, the owner uses his private key for the encryption of the scrambled data file, and the Cloud Services uses his public key to authenticate the owner of data. The authentication user of the data is performed with owner private key when adding a new client, while the owner authentication is performed at cloud service by the private encryption at cloud service with owner private key.

Data Confidentiality and Integrity

In order to perform the analyses of the data confidentiality for this proposed approach, it is compared with the already existing encryption techniques that use the symmetric keys. The provider of cloud service is unable to visualize the original data and digest of the owner as the key is symmetric and only shared among the user and data owner. The data after encryption with symmetric keys is once again encrypted with the private key of the data owner, and public key of the provider of cloud services. To wrap up the discussion that data is not available to be decrypted in to its original form by the cloud services. The integrity is ensured for the data under consideration by employing the MD5 hash algorithm. The user of the data computes a fresh has and then match it up to the one already appended to the original data file. The integrity violation will be reported and the owner of the data will be informed accordingly, if the hash calculated by the user does not match to the original hash present in the message.

Access Control Based on Attribute Certificates

The authentication and authorization is based on a multistep process including the biometric data, other than that, in our proposed model, the access is further control on the bases of a second type of digital certificate i.e. the attribute certificate. The identity and attribute certificate can be created by owner of the data in certificate issuing authority center. The clients are issued certificates according to the nature of their request after successful login to the cloud service provide. The reason of using the attribute certificate is that, the earlier models were using access control lists, which may not be practicable for cloud computing environment [22, 23, 24]. Because the user needs are different, if one access one data file may not necessary accessed by other client so, creating of access control list for any data object is apparently difficult. In our approach we use attribute certificate which contain the necessary data structure of the data files for the access control.

Algorithm Description

ATTRIBUTE-BASED ENCRYPTION (ABE)

Attribute-based encryption (ABE) is a recent method that uses the concept of public key cryptography. In public-key cryptography, a message is encrypted for a specific user using the user's public-key. Identity based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g. the email address of the user. To keep up information classified and achieve fine grain right of passage control, our preparatory point is a circuit key policy property based encryption. The key issue is that someone should only one who is able to decrypt a cipher text if the person holds a key for "matching attributes" where user keys are always issued by some trusted party.

Cipher text-Policy ABE (With Triple DES algorithm)

Supported by the necessities in the cloud, we change the interpretation of CP-ABE with evident distribution and there a physical structure to comprehend circuit's figure content strategy standard half breed encryption with undeniable assignment (CPABE). To keep up information classified and achieve fine grain right of passage control, our preparatory point is a circuit key policy property based encryption. We give the counter impact circuit CP-ABE structure in this archive for the premise that CPABE is hypothetically prior to the regular right of passage control strategies. For the fundamental ability issues of ABE, going before structures gave a ready system to outsource the lion's share straightforwardness of decoding to the cloud. In any case, there is no affirmation that the proposed result returned to by the cloud is constantly exact.

Trying at extra enhancing the capability and giving unconstrained clarification of the asylum confirmation, the idea of cross breed encryption is excessively presented in this work. Plus, asylum of the CPABE framework ensures that the sad cloud won't be sharp to study whatever thing about the scrambled message and fake the special figure content. From that point forward, the proposed plan is recreated in the GMP library. At last; the framework is refined to be sensible in the cloud.

VII. CONCLUSION

Encryption scheme describes the amount of time and computational resource required for the evaluation. Analysis shows the attribute set-based encrypted data stores on cloud and protects from the unauthorization users mainly usefully for banking services. To prevent server from learning the file content of each segment searched by monitoring the users search patterns. Future direction of our analysis is to avoid the intrusion objects without user presence.Here we proposed the Hierarchical Attribute-based Encryption algorithm in an efficient manner to achieve the more security in cloud environment. Existing system a chance to loss the information for that we proposed the replication concept to protect the data and save the storage space in cloud environment.

REFERENCES

[1] C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou, "Securityconcerns in popular cloud storage services,"vol. 12, no. 4, pp. 50–57, October-December 2013.

[2] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. K. Liu, "TIMER: secureand reliable cloud storage against data re-outsourcing," vol. 8434, pp. 346–358, May 2014.

[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbasedrevocable identity-based proxy re-encryption scheme for public clouds data sharing," vol. 8712,September 2014.

[4] T. H. Yuen, Y. Zhang, S. Yiu, and J. K. Liu, "Identity-based encryptionwith post-challenge auxiliary inputs for secure cloud applications andsensor networks," vol. 8712, pp.130–147, September 2014.

[5] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X.Phuong, and Q. Xie, "A DFA-based functional proxy reencryptionscheme for secure public cloud data sharing," vol. 9, no. 10, pp. 1667–1680,October 2014

[6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "ktimesattribute-based anonymous access control for cloud computing," vol. 64, no. 9, pp. 2595–2608,September 2015.

[7] S.Saravanan, Arivarasan."An efficient ranked keyword search for effective utilization of outsourced cloud data" Journal of Global Research in Computer Science, Vol4(4), pp:8-12

[8] S Saravanan, V Venkatachalam ," Improving map reduce task scheduling and micro-partitioning mechanism for mobile cloud multimedia services" International Journal of Advanced Intelligence Paradigms ,Vol 8(2),pp157- 167,2016.

[9] S Saravanan, V Venkatachalam ," Advance Map Reduce Task Scheduling algorithm using mobile cloud multimedia services architecture" IEEE Digital Explore,pp21-25,2014.

[10] S.Swathi "Preemptive Virtual Machine Scheduling Using CLOUDSIM Tool", International Journal of Advances in Engineering, 2015, 1(3), 323 -327 ISSN: 2394-9260, pp:323-327.

AUTHOR's PROFILE

Ms.**JAMPANA POOJA SRI MANI** is a student of Kakinada Institute Of Engineering And Technology For Women, KORANGI, Kakinada, E.G,A.P. Presently she is pursuing her M.Tech[Computer Science and Engineering] from this college and she received her B.Tech from Kakinada Institute Of Engineering And Technology For Women, KORANGI, affiliated to JNT University, Kakinada in the year 2019.

Mr. **SATTI VIJAYA KRISHHNA REDDY** is a excellent teacher Received M.Tech(Computer Science and Engineering)from Kakinada Institute Of Engineering And Technology, Kornagi, affiliated to JNT University, Kakinada. He is working as Asst. Professor in Kakinada Institute Of Engineering And Technology For Women. He has 3years of teaching experience in engineering colleges. His area of Interest includes Data Warehouse and Data Mining, information Security and other advances in Computer Applications.