GROUP DATA SHARING USING MULTIPLE SECURITY IN CLOUD

Sri Hari. T, Sangeetha. D, Suraj. A, Mr. Anwar Basha
Student, Student, Student, Faculty
Computer Science and Engineering
SRM Institute of Science and Technology, Chennai, India

Abstract: The main objective of Cloud Computing is sharing of System resources and services via the Internet. Another mode of cloud is Storage where we can store documents, multimedia contents, files, etc., To avoid problem with syncing the system should be always connected to the Internet. The maintenance of information in cloud computing permits various subscriber to uninhibitedly allowance the associated documentation information's then they enhance the productivity of tasks in helpful conditioned and for reaching prospective end user programs. Notwithstanding, how to guarantee the reliability of information allocating inside a gathering and how to productively share the re-appropriated information in a gathering way are imposing difficulties. The Lead understanding conventions have assured an essential job in protected and collection gathering in cloud computing. Cloud Storage can also be used as a group where many members or participants can be joined together in the group and they can share the data between the members of the group. Even though, there are many vulnerability from within or outside the group. This issue can be handled by implementing Multiple Security to the group such as Identity, Public Key or Search file key, Private Key or Limited time OTP, Encryption and Decryption.

Index terms **– Keyword Guessing Attack (KGA), Public Key Encryption System (PKEKS), Semantic Security (SS), Indistinguishability opposing KGA**

I. INTRODUCTION

Cloud computing and cloud storage have wind up trending points in ongoing decagon. Extraordinarily developing the creation effectiveness in a few territories. Nowadays, because of restricted file assets and the prerequisite of helpful approach, so we have to store every kinds of information in cloud storages and server set-ups, so that likewise a decent alternative for organization's as well as associations has to maintain a strategic distance from the overhead of conveying and keeping up hardware when information are put away confined. The server cloud gives a wide-open access and helpful capacity stage for people and associations, however it likewise presents security issues, for e.g. A cloud framework might be exposed to assaults from both pernicious clients and cloud suppliers. The above plan as it were considered security issues of a solitary information proprietor. However, in certain applications, various proprietors might want to safety share their information in a gathering way. Thus, a convention that underpins secure gathering information distributing in mist storage is required. A path understanding convention is utilized to create a typical meeting key for different members to guarantee the security of their late correspondences, and this convention can be connected in cloud storage to be helpfully protected and proficient information distributing.

II. LITERATURE REVIEW

Mohammad Aazam, Eui-Nam Huh [1] suggested that benchmark mechanism is demanded to allow interoperability between clouds and transcoding media contents. Ambition of this cloud is to define this problem and to compose a cloud and handle media contents transparently, even if it is determined outside the user's domain. Administrating multimedia does not mean only transcoding media contents into interoperable form but also to communicate multimedia file according to quality and types. Multimedia is sent to the cloud according to the quality poll done on the stream. Inter-Cloud architecture, Media Cloud storage design considerations and some key findings on storage heterogeneity. They face some key challenges like handling multimedia contents. Maintaining the cloud space between the clouds and the also keeping in mind the heterogeneity.

B.Manishkumar, R.Rajasekar, D.Deepa, P.Veeralakshmi [3] used a public cloud to share the data to the users which makes the accessing operation much easier. A public cloud mainly supports the simultaneous data uploading/downloading. To provide security to the cloud, key agreement protocol has played a very major role in an efficient manner. Based on the advanced group data sharing model, we present general formulas for generating the random group key for multiple users, once the group is made the data will be made into clusters and secured within the cloud using general and advanced algorithms. The users can securely

obtain their private keys from group manager. User sends request to group manager for accessing the wanted group, at that time our system provide personal secure key to user without activation. Then group manager see's the request and activate the keys after confirming them. After user's private key gets activated, then only user can access the group. Our device has fine-grained access control, any user in the group can use the origin in the cloud and revoke users cannot access the cloud again after they are revoking. These methods generally mathematically bind the agreed keys to other agreed upon data, such as the followings: 1) Public/private key pairs 2) Shared secret keys 3) Password 4) Fault Detection Phase.

Shengmin Xu, Guomin Yang [4] gave a fine-grained access control and data sharing system for on-demand services with vigorous user groups in cloud. The experimental data shows that our proposed device is more efficient and scalable than the state-of-the-art solution. The solution offered in made of dynamic group sharing between many same groups which will be confronted based on the input of the access control system posed on the system produced.1) defining and enforcing access policies based on the attributes of the data 2) permitting key generation center (KGC) to efficiently update user credentials for dynamic user groups and 3) allowing some expensive computation tasks to be performed by untrusted CSPs without requiring any delegation key. Sharing cloud data among authorized users at a fine-grained level is still a challenging issue, especially when dealing with dynamic user groups. The dynamic user groups are very vast which makes the scalability of the group to be another challenging concern as well.

III. RESEARCH METHODOLOGY

3.1 Tools and Models

3.1.1 Cloud Computing

It is the use of remote servers on the internet to store, manage and process data rather than a local server or your personal computer. Generally, cloud frameworks put your data on cloud servers and voila. Cloud computing has more stability when server capability will vary according to traffic and your cloud provider will manage your servers, hence no worries about the underlying infrastructure. There are two types of different cloud models they are service models and deployment models. Each cloud models sector has their own operations and platform services. Deployment models contains 3 platforms public, hybrid and private. As well as Services models contains Infrastructure as a service, Software as a services and Platform as a service. Mists might be restricted to a solitary association be accessible to numerous associations or mix of both. Presently, the biggest open cloud is **AMAZON AWS.**

3.1.2 Cryptography

Cryptography is a practice and a study of techniques, communication in the presence of data and adversaries. It is essentially important, it allows to secure data and classified information. The goal here is to make the communication secure. It refers to a set of techniques which is used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. Before crypto was adequately synonyms founded on numerical hypothesis and software engineering testing. Cryptography is classified into two different types they are: 1. Symmetric and 2. Asymmetric cryptography.

3.1.3 File Storage

Cloud record is based on the service information through shared document frameworks. A cloud service is any service made available to users on demand via the internet from a cloud computing provider's server. All the files will be stored according to the service sectors. A record framework in the cloud is a progressive storing database framework that gives shared access to document information. Clients can make, erase, study, alter and compose and sort out them consistently in registry trees for natural access. Cloud record sharing can be characterized as an administration that gives concurrent access to different clients to a typical arrangement of document information in the cloud. Security for record database in the cloud is made do with client and gathering authorizations empowering heads to firmly control access to the mutual document information.

3.2 Initial System

3.2.1 Generic Construction of Integrated PKE and PEKS

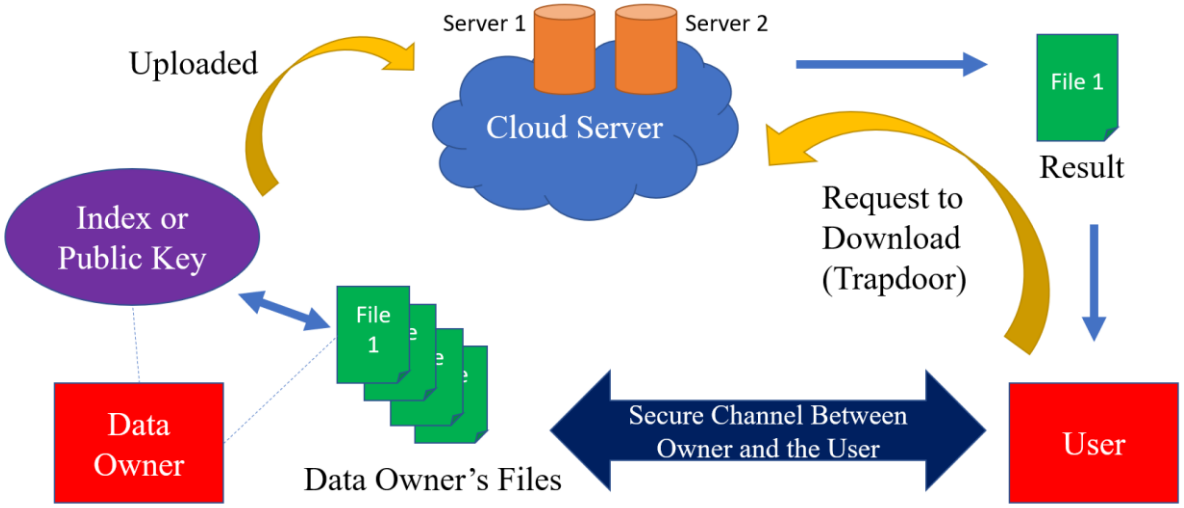
The PEKS scheme actually helps the third party to search through without impacting the security. Thus, the risk of the security breach is minimized and the data encrypted is saved also the search can be made based on the public key. The public key itself will be the search quadrant which identifies the actual data under the encryption. The data encryption will take place when the email travel through the server and the encryption takes place assigning the public key. The assigned public key will made as

the cypher key text which will be the entry code for the user to enter. Since the PEK is generated the search can be easily carried over through the whole set of data and the attacker won't have the clearance required.

3.2.2 Free Channel PEKS

The trapdoor between the data with the encryption is made to be under the SCF. Therefore, the data searched within the use of the actual algorithm will be considered as SCF-PEKS so the entitled data will be shown. The KEY will be generated only by the server thus the server can only make the search through the trapdoor. Thus, the attacker will not have the access to the original secured cypher keys and therefore the data will be kept under encryption and the attacker will meet the trapdoor and the duplicate rather than the servers key due to the use of SCF-PEKS. The secure channel will be created by the server therefore the trapdoor will be set as well having a duplicate case on for the attacker and the PEK encryption will also delay the search of data in the upper hand. The data with the cypher key will have advanced security model-based access recognition which will have the SCF-PEK scheme of search.

3.3 Theoretical Framework



Architecture Diagram

3.4 Security Modules

3.4.1 Opposing Keyword Guessing Attack

Keyword Guessing Attack is a type of unauthorised access to our data done by the person who can be inside or outside of the organization. This problem was faced by many of the previously developed Group Data Sharing System because we can't identify the user who access the data. The Attacker can be one of the Group members or the person other than the Group who knows about the Keyword to access the data. Many of them developed solutions for the issue but still the adversarial effect is more. This issue cannot be stopped but it can be controlled by the solution we propose. Since there are more securities applied, the attacker requires more time to overcome the system. First, the user will be registered with the group where the identity of the user will be recorded and stored in the database which can be accessed by the organization owner. Second, we implemented double server where one acts as a normal security but other one acts as a trapdoor for the inside users. And the File attached with the index or public key will be the increased security because the user knows the public key, he/she can tell the key only to the most trusted person so that no one access the File. This problem is just for the person inside the group and not for the owner of the group.

Every condition should apply to everyone especially the owner because the owner sends the private key to the group members and they know the key to access data. No one knows who are trusted, that's y we proposed double server, if one goes down without the other one the data can't be retrieved. This person acts as an Outside adversary. In this System, the trapdoor server knows only the ½ of the private key where the other half will be kept private. The key generation will be done by the RSA algorithm which is modified according to the system implemented.

3.4.2 Adversarial First Owner

Here, we're characterizing the dependability opposed to an ill-disposed first network. So here we're initializing present duplet recreations to be specific semantic security against picked catchphrase assault and lack of definition against defend to catch the protection of trapdoor and PEKS Cipher text, separately.

3.4.2.1 Connotation Security

Here we're characterize the Connotation protection against picked watchword assault which ensures that no adversary is capable to recognize a watchword from the given PKEKS. (i.e.) PKEKS cipher text will not uncover any data about the hidden catchphrase to any enemy. Formally we present an analysis for the SS-CKA security definition against the ill-disposed front server.in the analysis the enemy is given general society/private key pair of the first server and the open of the back server .in the discover stage A can test any match of PEKS figure content and watchword by questioning the prophet OT and in the end. Yield two testing watchwords (kw0, kw1) with the indication data state "with an irregular piece b £ {0, 1} as information, the analysis creates and afterward sends the PKEKS cipher text CT". The B is a substantial yield of the examination if and just if that A has never questioned OT with the test watchwords. We allude to such an ill-disposed first server an in the above experience.

3.4.2.2 Indistinguishability opposing KGA

The Trapdoor catches and shows the uncover Zero information about the basic catchphrase to the antagonistic first owner. Thus, we are characterizing that the security tries as appeared .so the investigation is like that of SS-CKA explore then again, in the test stage, the foe is stated trap door is rather than the cipher text. We allude to such an antagonistic first owner in the overhead analysis as an IND-KGA enemy and characterize its favourable position.

3.4.3 Adversarial Second Owner

The security reliable models of SS-CKA and IND-KGA as far as antagonistic second owner are like those who argue as an antagonist first owner.

3.4.3.1 Connotation Security

Here the SS-CKA test against an antagonist second owner is equivalent and an antagonist first owner aside from that the enemy is given the private key of the second owner rather than that of the first owner. We preclude the subtleties here for straight forwardness. We allude to the ill-disposed second owner an in the SS-CKA explore as a SS-CKA foe and characterize its preference as Adv SS-CKA.

3.4.3.2 Indistinguishability opposing KGA

Also, this security show means to catch that the trapdoor does not uncover any data to the back sever and henceforth is equivalent to that against the first owner with the exception of that the foe claims the private key of the second owner of that of the first owner. Thus, we likewise overlook the subtleties here. We allude to the ill-disposed second owner in the IND-KGA test as an IND-KGA foe and characterize its favourable position.

3.4.4 Hashing Function

The cryptographic hash function indeed little changes in the source contribution radically change the subsequent yield, by the purported torrential slide impact. A cryptographic hash work is a functional hash work which takes an information and returns a fixed-measure alpha numeric string. The string is known as the 'hash esteem', 'message digest', 'computerized unique mark', 'condensation' or 'checksum'. The perfect hash work has 3 fundamental properties:

i. It is very simple to compute a hash for some random information.
ii. It is very computationally hard to ascertain an alphanumeric content that has a given hash.
iii. It is incredibly improbable that two marginally extraordinary message will have a similar hash.

A focal component of development for double owner open index encryption with watchword is smooth projective hash work, a thought presented by the tool Cramer and shoup. We begin with the first definition of a SPHF.AS SPHF have been presented by Cramer and shoup under the name hash verification frameworks. A SPHF for a language L permits to hash a word in two distinctive ways, either with some mystery key, hashing key or with the related open. It must fulfil 2 properties:

i. On the off chance that the word x is in the Language, both methods for hashing will restore a similar hash esteem
ii. On the off chance that word x is outside the Language, the hash got with the mystery key is factually vague from irregular, even the open key.

Instinctively, this can be utilized as a sort of assigned verifier zero-information confirmation (in spite of the fact that it doesn't full the traditional zero-learning property):to demonstrate the x belongs L, the prover gets the projection key hp from the verifier, and

hashes the word as for Utilizing hp, and sends back the outcome. The verifier contracts It to the hash got and the mystery key acknowledges the verification if the two hashes are the equivalent.

3.4.5 RSA Cryptosystem

RSA stands for Rivest Shemir Adlemen. It requires the encryption pair of numbers which acts a pair of lock which will be handed over to everyone. The pair or numbers will be published to the other users and the user should use the pair of number to lock the file before sending and the user who publishes the numbers can only decipher the file from the lock. For example, the sender wants to send a text file to the receiver. The receiver sends a pair of numbers or lock to the sender. The sender should use the locks to secure the file which is known as encryption. If the pair of locks are (5, 14), then the sender wants to send a file, he should first consider the text as a random number and use a formula (File Number^Lock1(mod Lock2)).

The result from the formula outputs a value which acts a ciphertext. The receiver uses a different pair of numbers to decipher the text but the both the pair of numbers are related. We should pick two prime numbers P and Q which should be large enough so that the key will be larger. The product of the number N=PQ which will be public in both encryption and decipher of the file. Then, the number which doesn't share the coprime with N are taken and listed and counted which can be done by ((P-1) (Q-1)). Choose E which satisfies the condition of 1. 1<E<(P-1) (Q-1) 2. Coprime with N, ((P-1) (Q-1)) which will be given to the sender. Formulate D by using the formula (D*E (mod ((P-1) (Q-1))) which gives the decipher key.

IV.RESULTS AND DISCUSSION

4.1 Result

The proposed Group Sharing System is more secured and stable for an Organization, Hospital Management System, Between Students and Teacher, Police Crime Records, etc. The number of Participants in the group is unlimited and the user with access rights can modify the Data. We researched many identical papers for Data Sniffing and we proposed a system where malicious attack will be controlled.

V.ACKNOWLEDGMENT

This project was guided by Mr. Anwar Basha, SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, Chennai

REFERENES

[1] Mohammad Aazam, Eui-Nam, Inter-Cloud Architecture and Media Cloud Storage Design Considerations Huh Computer Engineering Department Kyung Hee University, Suwon, South Korea aazam@ieee.org, johnhuh@khu.ac.kr

[2] S.Simla Mercy, Dr.G.Umarani Srikanth, An Efficient Data Security System for Group Data Sharing in Cloud System Environment, simlamercy@gmail.com & gmurani@yahoo.com

[3] B.Manish kumar,R.Raja sekar,D.Deepa,P.Veeralakshmi, Framework for Secure Data Sharing in Dynamic Group Using Public Cloud

[4] Shengmin Xu, Guomin Yang∗, Senior Member, IEEE, Yi Mu, Senior Member, IEEE, and Robert H. Deng Fellow, IEEE, Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud