ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Key Aggregate Policies for Secure Data Sharing in Cloud Storage

Sneha A.Jaswante[1], Prof. Nitin R.Chopde[2]

PG Scholar, Department of Computer Science & Engineering, SGBAU, India[1]

Head of Department, Department of Computer Science & Engineering, SGBAU, India[2]

ABSTRACT: Sensitive information modified should be firmly done to verify the integrity of cloud information, to stop it from being disclosed to or modified by unauthorized parties. Many enterprises supply information storage to the cloud mere a member of a company or information owner can merely share information with completely different members or users with confidentiality. The new public key aggregate policies that prove constant-size ciphertext wherever mere ciphertext unit labeled with sets of attributes and private keys unit associated with structures that management that user is able to decrypt. In several words, the key holder can unleash a constant-size aggregate key for versatile preferences of ciphertext set in cloud storage, but the other encrypted files outside the set keep secret to boot to authentication and privacy preservation this theme tries to satisfy all completely different security wants with key management and achieves higher quantifiability once the quantity of access levels can increase.

KEYWORDS: Cloud storage, data sharing, key-aggregate encryption,decryption.

I. INTRODUCTION

Cloud computing is a vigorous analysis topic reaching to produce safe spoken communication environments on-line. It's net primarily based computing technology wherever virtual shared servers offer computer code, platform, infrastructure, and different resources that delivers the resources as a service to the users over the web. Internet-based on-line services do offer large amounts of space for storing and customizable computing resources, this computing platform is eliminating the responsibility of native machines for information maintenance at constant time. whereas in a very cloud, most information and computer code that users use reside on the web, that bring some new challenges for the system, concerning to security and privacy. On the one hand, though the cloud infrastructures square measure rather more powerful and reliable than personal computing devices, broad vary of each internal and external threats for information integrity still exist.

Cloud computing have several benefits in resource sharing, value reduction, and time saving for brand spanking new services. Since every application could use resource from multiple servers. The servers could settled at multiple locations and also the cloud could use totally different infrastructures across organizations. of these characteristics of cloud computing create it difficult to supply security in cloud computing. To confirm adequate security in cloud computing, numerous security problems, like authentication, information confidentiality and integrity, and non-repudiation, all got to be taken under consideration. Users will access these services obtainable on the cloud while not having any previous information on managing the resources concerned. Thus, users will concentrate a lot of on the core business processes instead of outlay time on gaining information on resources required to manage their business processes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

The main concern is the way to share the information firmly the solution is cryptography. The question is however will the encrypted information is to be shared. The user should offer the access rights to the opposite user because the information is encrypted and therefore the decipherment key ought to be send firmly. For example use keeps her non-public information i.e. photos on dropbox and she or he doesn't need to share it with everybody because the offender might access the information therefore it's unattainable to have faith in predefine privacy protective mechanism therefore all the photos were encrypted by her on encoding key whereas uploading it.

II. RELATED WORK

A literature survey is a discussion of the literature in a given area of the study. It is concise overview of what has been studied, argued and established about a topic, and it is usually organized chronologically or thematically. Following is the listing of the things that were required to be studied for project.

Cloud computing is visualised as design for succeeding generation. It has many facilities though have a risk of attacker who can access the data or leak the users identity. While setting a cloud users and service providers authentication is necessary. The issue arises whether cloud service provider or user is not compromised. The data will leak if any one of them in compromised. The cloud should be simple, preserving the privacy and also maintaining users identity.

In Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing the versatile use of cloud storage for user could be a would like because it is seams accessing information domestically although that's gift at remote facet. it's necessary to examine the info assail the cloud. Therefore it's necessary to permit a public audit for integrity of outsourced information through third party auditor (TPA). TPA is additionally helpful for cloud service supplier. It checks the correctness of the outsourced information. TPA ought to be ready to do public auditability, storage correctness, privacy conserving, Batch auditing with minimum communication and computation overhead . Batch auditing: There are K users having K files on the same cloud They have the same TPA. Then, the TPA can combine their queries and save in computation time. Data dynamics, the data on the cloud may change according to applications. We utilize the homomorphic authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage[2].

There are several cloud users who needs to transfer there information while not providing a lot of personal details to different users. The namelessness of the user is to be preserved in order that to not reveal the identity of information owner. Provable Data possession (PDP) uses similar demonstrating marks to scale back computation on server, and network traffic. PDA ensures the info gift on cloud that is un-trusted is original while not accessing it. Security mediator (SEM) is approach permits the user to preserve the namelessness. Users are meant to transfer all their information to SEM in order that the SEM isn't able to perceive the information though it's reaching to generate the verification on data because the users ar signed at SEM it mustn't recognize the identity of uploader [3].

Dynamic and Efficient Key Management for Access Hierarchies in this proposed solution has the following properties: (i) only hash functions are used for a node to derive a descendant's key from its own key; (ii) the space complexity of the public information is the same as that of storing the hierarchy; (iii) the private information at a class consists of a single key associated with that class; (iv) updates (revocations, additions, etc.) are handled locally in the hierarchy; (v) the scheme is provably secure against collusion; and (vi) key derivation by a node of its descendant's key is bounded by the number of bit operations linear in the length of the path between the node. The advantage is the dynamic scheme achieve a worst- and average-case number of bit operations for key derivation that exponentially better than the depth of a balanced hierarchy[4].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Cryptographic key task plans intend to minimize the cost in putting away and overseeing master keys for general cryptologic utilization. Using a tree structure, a key for a given extension are frequently usual infer the keys of its relative hubs yet not the inverse means round essentially conceding the guardian key verifiably allows all the keys of its relative nodes.The greater part of those plans turn out keys for symmetric-key s [1].

Identity-based encryption (IBE) may be a public-key encryption during which the public-key of a user are often set as an identity-string of the user. There's a trusty party known as personal key generator in IBE that holds a master-secret key and problems a secret key to every user with reference to the user identity.It will take the general public parameter and a user identity to encrypt a message. The receiver will decode this ciphertext by secret key[6]. Multi-Identity Single-Key Decryption without Random Oracles, This Paper produce Multi-Identity Single-Key Decryption (MISKD).It is an Identity-Based Encryption (IBE) system where a private decryption key can map multiple public keys identities. More exactly, in MISKD, a single private key can be used to decrypt multiple cipher texts encrypted with different public keys associated to the private key[7]. In fuzzy IBE, one single compact secret key will decode ciphertexts encrypted below several identities, however not for discretional set of identities and so it doesn't match with the concept of key aggregation[8].

Attribute-based encryption (ABE) is powerful cryptographic primitive which provide encryption mechanism with fine grained access control. There are two kinds of ABE in the literarures, key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, sender ascribes attributes to the ciphertext which come from pre-defined universal attribute set ABE scheme with constant-size cipher texts allowing for as expressive policies as possible maintains each ciphertext to be associated with an attribute and the master-secret key holder can extract a secret key for a policy of these attributes so that a ciphertext can be decrypted by this key if its associated attribute conforms to the policy [9],[10].

Public-key cryptography , also known as asymmetric cryptography. It requires two distinct keys one of which is private and other one is public. Two parts of this key pair mathematically linked with each other. The public key is used for encryption and private key is used for decryption. Public Key encrypts the plain text to generate an encrypted data, while the private key is used to decrypt cipher text or to create original data. The term "asymmetric" arises from the use of different keys, each key is the inverse of the other.Public-key algorithms are primary security methods in cryptographic applications and protocols. They support various networking standards, such as (TLS) Transport layer Security. Some public key algorithms provide key distribution and secrecy (e.g., Diffie-Hellman key exchange), some provide digital signature (e.g., Digital signature), and some provide both (e.g., RSA)[11].

III. PROBLEM DEFINATION

In cloud computing the main concern is to provide the security to end user to protect files or data from un authorized user. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. The local user scan store their data in there motecloud storage servers, from that the users can access the data from any where in the world. But storing data in a third party cloud system may affect the data confidentiality. For avoid this issue the data's are encrypted before storing into storage server.In the general encryption system the data owner encrypts the data by using cryptographic methodology and stores the encrypted data at the cloud storage server. It provides data confidentiality but it does not provide high security and dynamic data modification. The unauthorized user may get the data while transfer from the data owner to the cloud server,or he can decrypt the data directly from the cloud server by getting cryptographic keys. Then the hacker may perform some modifications at the hacked data and again stored into the storage server like a data owner. The cloud users and data owner can't identify the data hacking. The data displays like original data. The receiver thing like the data came from the data owner, it affects the data originality, data origin authentication, security and data integrity.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Constant-size decryption key require pre-defined hierarchical relationship. The fixed hierarchy is used. In that there is only one way in which we can partition the record. If we want to give out access rights based on something else e.g. based on document type or sensitivity of data we will have to look at all the low-level categories involved, and give a separate decryption key for each. More number of decryption key was used.

IV. PROPOSED WORK

A key-aggregate cryptographic scheme comprises of five polynomial-time algorithms as follows.
The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen. Messages can be encoded by means of Encrypt by any individual who likewise chooses what ciphertext class is connected with the plaintext message to be encrypted. The data owner can utilize use the master-secret to generate an aggregate decryption key for a set of ciphertext classes via Extract. The generated keys can be passed to delegatees securely by means of secure e-mails or secure devices. Finally, any user with an aggregate key can decrypt any ciphertext provided that the ciphertext's class is contained in the aggregate key by means of Decrypt.

1.Data-owner repository
Data owners is user who wants to keep their data for sharing. Dataowner first register their credentials in the cloud server. Data owners get their access by authoring their credential information from cloud server. Data owner can able to process or create any kind of data file and forms the data repository which is further used for the processing of derivating the access policy or data owner attributes.

2. Cipher-class key generation
Cipher class consisting of Dataowner's id and message and the master/public key of the data owner attributes. Using the reverse encryption algorithm, public key and secret key is generated. Ciphering algorithms are applied using the secret key, thus secured secret key is generated by Key aggregate policie.

3. Aggregate key aggregation
It is the process of pairing up the attribute information and using master-key and the data-owner attributes. Aggregate key is considered as secret key for data security for the data being outsourced in the cloud. Key aggregate policie is unique key generation scheme for secure and robust cloud data security mechanism. It differs from the normal and cryptography techniques by generating the keys from the various attributes of dataowner. Thus proved the effective key generation process.

4. Secure Cloud Storage The Data owner's file have been applied security. These files are stored in the cloud servers. In order to do that the cloud server have to configure.In cloud servers client files are stored as secured files so the crypto process have applied.For crypto process we use RSA for the encryption and decryption process.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

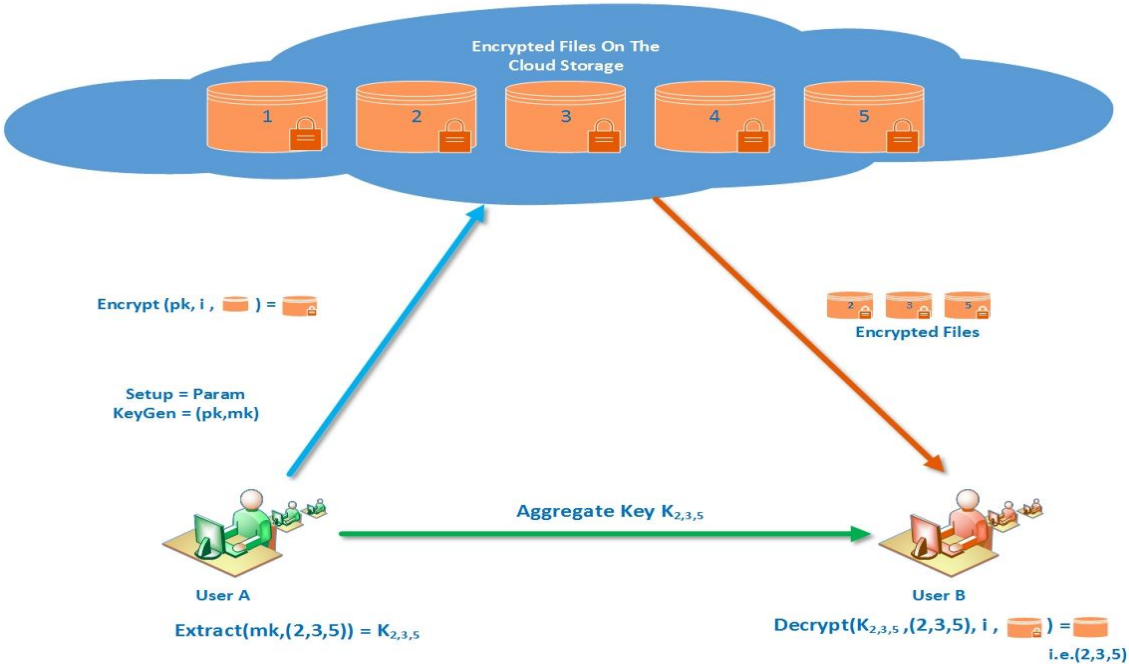

Figure 4.1: Proposed KAP Framework for data sharing.

5. Secure Retrieval

Data retrieval process not only consist of retrieval of encrypted files from the cloud server and decrypted using respected private keys. But the data are provided to the users upon the authentication of the hierarchical access control of Cloud system architecture. Data or keys are revocated in the cloud frequently depending upon the kind of data owner's identity and the data to be stored on the cloud.

In KAC scheme data owner use RSA algorithm to encrypt files. Files are encrypted under different ciphertext classes on data owner's choice. The data owner produces public/master-secret key pair using REA algorithm in this phase. Aggregate key generation phase is divided in three steps. Messages can be encrypted using Encrypt( ) function by anyone who also decides which ciphertext class is associated with the plain text message. The data owner can use master-secret to generate an aggregate decryption key for ciphertext classes using function Extract( ).

V. EXPERIMENTAL RESULT AND ANALYSIS

This section show the performance analysis of the system and the result gatherd from the various framework that how this scheme is better than other schemes. The framework is mainly desgin for the secured transfer user information.The experiments are made using the prototype application that has built to test efficiency of the protocol. The performance analysis of the system and the result gatherd from the various framework shows how this scheme is better than other schemes. The framework is mainly design for the secured transfer of user information over the network. The proposed system is more efficient than the curent system. This section illustrative graphs and tables with the statistical data of the system working constraints such as key generation, extraction and decryption time.The system transfers the data over the secure transport layer of the network architecture. Mainly the system is made efficient by deducting the unnecessary system contraints.The following table illustrates the performance analysis of proposed system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Table 5.1: User side uploading response time.

File Size	Total No. of Files Uploaded	Public and Master Key Generation (ms)	Encryption Time(ms)
10 kb	1	1.4	2.1
20 kb	2	1.4	2.4
30 kb	3	1.4	2.8
40 kb	4	1.4	3.3
50 kb	5	1.4	3.8

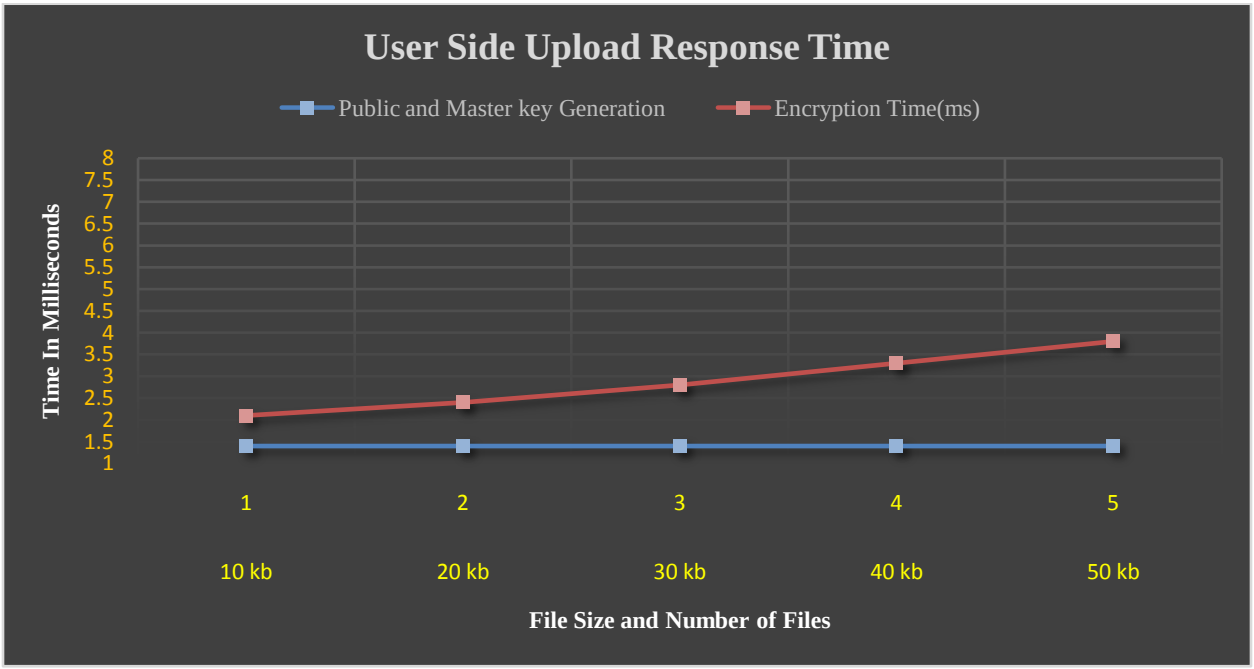

Figure 5.1: User Side Upload Response Time

In the above table 5.1 illustrates the public and master key generation and extraction time for the multiple files and file sizes of 10KB to 50KB. Both of the values are represented in the millisecond unit. The below Chart represents that the time for the encryption increases as the number of file as well as when the file size increases.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Table 5.2: Aggregate key generation response time.

No of File	File size	File Extract Time (ms)	Aggregate key Generation (ms)
1	10 kb	0.11	1.6
2	20 kb	0.12	1.6
3	30 kb	0.13	1.6
4	40 kb	0.14	1.6
5	50 kb	0.16	1.6

The above table 5.2 represents the aggregate key generation time for the system as well as the file extraction time for the same multiple files and file sizes of 10KB to 50KB. Both of the values are represented in the millisecond unit same as represented above for the unit of time. From the above graph in the closure it determined that file extraction time is increasing as the file sizes as well as number of the files are increasing.

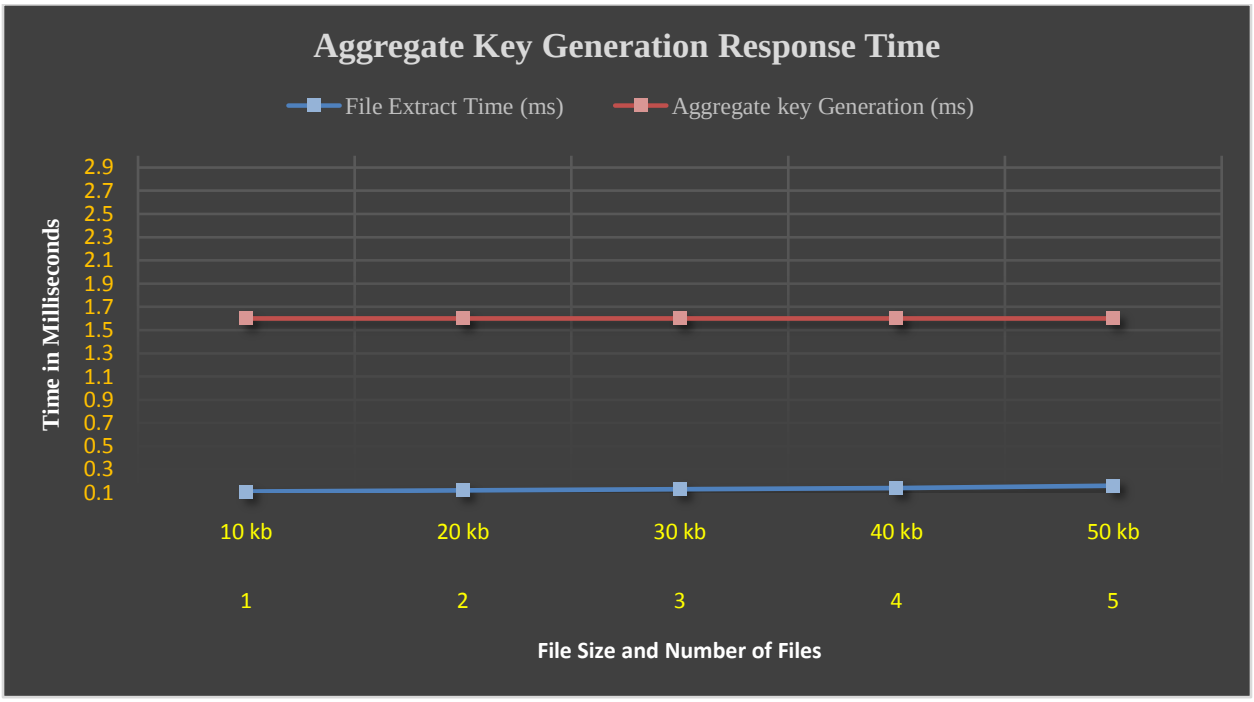

Figure 5.2: Aggregate key Generation Time.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Table 5.3: Existing System and Proposed System Comparison.

Delegation Ratio (r) in Millisecond	Existing System		Proposed System	
	Extraction	Decryption	Extraction	Decryption
0.1	2	4	1	2.6
0.2	4	6	1.6	4.2
0.3	5	9	2.2	7.1
0.4	7	12	3.9	10.4
0.5	8	14	5.2	12

The table 5.3 shows the comparison between the existing system and the proposed system. The examination is done on the premise of the extraction and the decryption time of the framework is in the millisecond unit where the designation proportion is expanding by 0.1millisecond for every different document in the framework. The execution times of Setup of a record, KeyGen for documents, Encrypt time are autonomous of the appointment proportion r. In existing framework the execution times of Setup, KeyGen, Encrypt are autonomous of the assignment proportion r. KeyGen takes 3:3 milliseconds and Encrypt takes 6:8 milliseconds. Obviously, the running time complexities of Extract and Decrypt increment directly with the appointment proportion r which decides the span of the assigned set S.

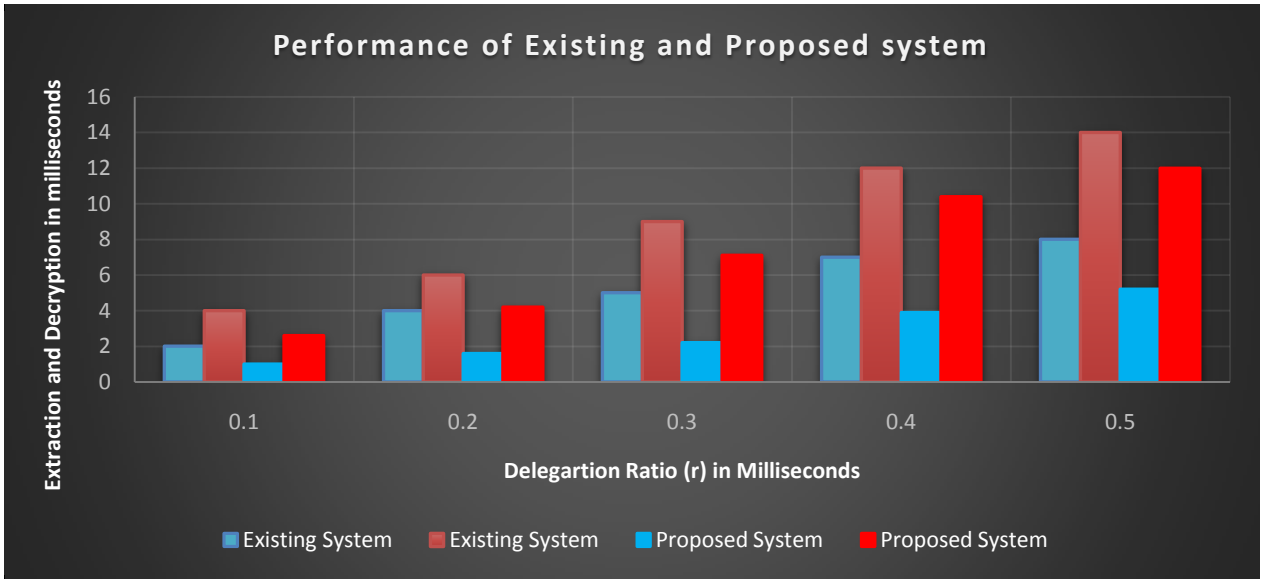

Figure5.3: Existing and Proposed System comprasion

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

In new KAP plan the setup of a record on untrusted server take 5.2 millisecond. When record is made a client can transfer and impart their information to approved client. At the time of uploading public and master key is arbitrarily created for each record. It utilizes symmetric key era which offers the most noteworthy productivity than different sorts. Encryption and decryption key size is consistent. Encryption of information should be possible in steady time, while decoding should be possible with single accumulated key, where S is the situated of ciphertext classes decryptable by the conceded total key. The KeyGen and Encrypt takes negligible time. Key extraction obliges less time. The exploratory results demonstrates that this plan have preferable pressure over the tree-based methodology. KAP conceded small key for each ciphertext classes, the setup of number of ciphertext classes can be made productively which takes less time. Of course, the running time complexities of Extract and Decrypt increment directly with the appointment proportion r which decides the measure of the assigned set S. The Extract and Decrypt two matching operations take insignificant time, the running time of Decrypt is around a twofold of Extract. At long last, it comment that for applications where the quantity of ciphertext classes is huge however the nonconfidential storage is constrained, one ought to send this plans which spared costly secure storage without discovering troubles of dealing with a progression of designation classes. From the below graph and the above table it is conclude that the proposed system is more efficient than the current system.

VI. CONCLUSIONS AND FUTURE SCOPE

The key aggregate policies enable a content provider to share her data in a confidential and selective way, with a fixed and small cipher text expansion, by distributing to each authorized user.However, it is apparent to see that the aggregate key encryption combined with ciphertext, is more efficient due to the shorter parameters and lower ciphertext overhead which provides user revocation and prevents replay attacks with high security. Meanwhile, KAC scheme does not require fixed and bounded number of users, thereby acquires more flexibility. The proposed system is more secure as the cloud admin verify data for security purpose. Key aggregate policies provides delegation of secret keys for various ciphertext categories in cloud storage. The delegation of decryption can be efficiently implemented with the aggregate key with high security. This approach is more flexible than hierarchical key assignment as it provide rigorous security analysis, and extensive performance.

For future extension it's necessary to order enough cipher texts categories as a result of in cloud cipher texts grows rapidly and therefore the limitation is that predefined sure of the quantity of most cipher text categories.Distributed hash table architecture for collaborative intrusion detection overcomes the challenges of the collaboration, such as data routing, load balancing, scalability and central points of failure.

REFERENCES

[1]Cheng-KangChu,ShermanS.M.Chow,Wen-GueyTzeng,JianyingZhou,andRobertH. Deng,SeniorMember, "Key-Aggregatefor ScalableDataSharing inCloud Storage",IEEETransaction on Parallel and Distributed System, Feb 2014,Vol. 25,NO. 2.

[2]C.Wang,S.S.M.Chow,Q.Wang,K.Ren,andW.Lou, "Privacy-PreservingPublicAuditing forSecureCloud Storage",IEEETrans. Computers,2013, vol. 62, no. 2, pp. 362-375.

[3] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[4] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies", ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

[5] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing", Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001,pp. 213–229.

[6] A. Sahai and B. Waters (2005), "Fuzzy Identity-Based Encryption", Advances in Cryptology EUROCRYPT, ser. LNCS, vol. 3494. Springer, 2005,pp. 457–473.

[7] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key", Pairing-Based Cryptography (Pairing '07), ser. LNCS, vol. 4575. Springer,2007, pp. 392–406.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

[8] F. Guo, Y. Mu, Z. Chen, and L. Xu , "Multi-Identity Single-Key Decryption without Random Oracles", Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer,2007, pp. 384–398.

[9] V. Goyal, O. Pandeey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data", The 13th ACM Conference on Computer and Communications Security (CCS '06). ACM,2006, pp. 89–98.

[10] Yong Cheng,JiangchunRen,ZhiyingWang,"AttributesUnioninCP-ABEAlgorithmfor Large Universe CryptographicAccessControl",SecondInternationalConference onCloudand Green Computing,2012, pp.180-186.

[11]ChristofPaar, Jan Pelzl, "Introduction to Public-key Cryptography", Understanding Cryptography, Springer, 2009.