Research Paper Engineering

Secure Scalable Data Sharing in Cloud Storage using Randomized Key Aggregate Crypto System

Vaddi Nagamani — V Nagamani, M.Tech Student, SriVasavi Engineering College, Tadepalligudem, AndhraPradesh, India.

Vedula Venkateswara Rao — VedulaVenkateswara Rao, Associate Professor, Dept of Computer Science Engineering,Sri Vasavi Engineering College, Tadepalligudem, AndhraPradesh, India.

Dr Mandapati Venkateswara Rao — Departement of Information Technology, Gitam Institute of Technology, Gitam University, Visakhapatnam, India

ABSTRACT

Now a days cloud computing is emerging computing technology in computing world. Cloud computing provides integration of several servers, storage space as a single entity. The cloud computing provides interconnection of several physical computing resources as a single entity so that the customers can use them on pay per use method. The cloud computing also uses virtualization technology to increase the computing resources so that with minimum resources we can implement work efficiently. Cloud provides different layers in its architecture so that the users can use all the resources in cloud as service model. In this cloud computing environment cloud storage is one of the services that are most popular in present world. Data sharing is an important functionality in cloud storage in this case the data placed by user may shared and accessed by many users in such a case the data sharing must be secure, flexible and efficient with others. Clod computing had overlaps many existing concepts such as distributed system. Data security is the challenging issue in cloud computing paradigm where the user store sensitive information on cloud servers. Also, data confidentiality against cloud server is required, when users outsource data for storage in the cloud. Existing solutions generally use cryptographic methods like encryption and decryption. The biggest concerns with cloud data storage is that of data integrity verification at untrusted server. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. For this it is proposed to have a public key cryptosystem for storing and accessing for data in cloud. In existing system this cryptosystem produces constant size cipher text. Now this system proposes to introduce variable size cryptosystem that is supported with a set of secret keys as a single keys and the process uses the power of the all the keys by using these compact aggregate key we encrypt files and storing cloud. This key is positive others who shares the data. By using this key others can share data in secured way.

KEYWORDS : Cloud computing, virtualization, cloud storage, cryptosystem, encryption, decryption, aggregate key

1 Introduction

Effective and secure information sharing, especially across multiple cooperating yet mutually suspicious organizations, is a fundamental challenge in today's information-rich and information-dependent society. The necessity to share but protect is among the oldest challenges for trustworthy computing. There has been a growing trend in the recent times to store data in the cloud with the dramatic increase in the amount of digital information such as consumers' personal data to larger enterprises wanting to back up databases or store archival data. Cloud data storage can be attractive for users with uncertain storage demands, requiring a cheap storage tier or a low cost, long-term archive. By outsourcing users' data to the cloud, service providers can focus more on the design of functions to improve user experience of their services without worrying about resources to store the growing amount of data. However, several recent surveys [2], [3] show that 88% potential cloud consumers are worried about the privacy of their data, and security is often cited as the top obstacle for cloud adoption. There are different types of infrastructures associated with a cloud [4]. A recent survey [5] shows that nearly half, 43% of all companies report utilisingprivate clouds and 34% of companies say they will begin to use some form of private cloud in the next six to twelve months. a secure RBAC based cloud storage system where the access control policies are enforced by a new role-based encryption (RBE). This RBE scheme enforces RBAC policies on encrypted data stored in the cloud with an efficient user revocation using a broadcast encryption mechanism described in [5]. RBE scheme is able to deal with role hierarchies, whereby roles inherit permissions form other roles. A user is able to join a role after the owner has encrypted the data for that role. The user will be able to access that data from then on, and the owner does not need to re-encrypt the data. A user can be revoked at any time in which case, the revoked user will not have access to any future encrypted data for this role. With new RBE scheme, revocation of a user from a role does not affect other users and roles in the system. In addition, we outsource part of the decryption computation in the scheme to the cloud, in which only public parameters are involved. By using approach [1], RBE scheme achieves an efficient decryption on the client side. This also uses the same strategy of outsourcing to improve the efficiency of the management of user to role memberships, involving only public parameters. Based on the proposed RBE scheme, develop a secure cloud data storage architecture using a hybrid cloud infrastructure. In RBAC, a user will have access to any object according to his/her assigned role in the system. The roles are assigned according to the job functions. Permissions are assigned on job authority and responsibilities according to the job. Operations on the given object will be invoked based on the permissions assigned to the job authority. RBAC models are more flexible than the other access control models such as discretionary and mandatory models, and this model suits for use in cloud environments, especially for the services for the users cannot be tracked with a fix identity. The paper mainly focuses on the following three categories of control models for cloud computing these are: 1] Role-based 2] Attribute-based encryption and 3] Multi-tenancy models. The paper provides review of this existing literature on each of the above access control models and their variants (with technical access, aspect and relevancy). Due to which we can identify future research directions for creating access control models for cloud computing environments which will be more effective.

1.1 Our Contributions

In modern cryptography, a fundamental problem weoften study is about leveraging the secrecy of a smallpiece of knowledge into the ability to perform cryptographicfunctions (e.g. encryption, authentication) multipletimes. In this paper, we study how to make adecryption key more powerful in the sense that it allowsdecryption of multiple ciphertexts, without increasing itssize. Specifically, our problem statement is –

Given service users need to regain control over their data together with PBE's ability to offer selective fine grained access control over encrypted data .our work to investigate how predicate based encryption schemes can be leveraged within the cloud to protect data.

The investigation was divided broadly into 3 stages.

Data security and the cloud: The initial stage sought to provide a clear definition for cloud computing and the security issues there in, looking to identify precisely where and when threats can occur to data how these threats ought to be mitigated.

Predicated based encryption: The next stage focused slowly upon PBE schemes discussing how they work and what they allow for. This provide a foundation upon which their deployment as part of a cryptosystem could b explored to define the types of problem that PBE schemes can be used to solve.

Leveraging PBE: The final stage of investigation built upon, and combined the results,of the previous stages .here the investigation looked to determine the problem that PBE schemes can be used to solve with in the colud,and the quality of solution provided.

1.2 Outcomes:

From the work ,it was determined that PBE(predicate based encryption) which is key aggregate cryptosystem can be used to protect the data with in the cloud the main results for each stage of the investigation (work)are described below.

1. Data security and cloud: Here two threat models are produced.
2. Predicate based encryption: Here we design a PBE scheme based on Characterstics.
3. Liverging predicate based encryption: Here 3 schnarieous are described to explain the process of encryption

2 Related Work

Cloud computing is visualized as architecture 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 loud 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 [1]

The flexible use of cloud storage for user is a need as it is seams accessing data locally though that is present at remote side. It is important to inspect the data set on the cloud. So it is necessary to allow a public audit for integrity of outsourced data through third party auditor (TPA). TPA is also beneficial for cloud service provider. It checks the correctness of the outsourced data. TPA should be able to do public auditability, storage correctness, privacy preserving, Batch auditing with minimum communication and computation overhead [2].

There are many cloud users who wants to upload there data without providing much personal details to other users. The anonymity of the user is to be preserved so that not to reveal the identity of data owner. Provable data possession (PDP) uses similar demonstrating marks to reduce computation on server, and network traffic. PDA ensures the data present on cloud which is un-trusted is original without accessing it. Security mediator (SEM) is approach allows the user to preserve the anonymity. Users are meant to upload all their data to SEM so that the SEM is not able to understand the data although it's going to generate the verification on data. As the users are signed at SEM it should not know the identity of uploader [3].

Another way for sharing encrypted data is Attribute-Based Encryption (ABE). It is likely to encrypt the data with attributes which are equivalent to users attribute rather than only encrypting each part of data. In ABE attributes description is considered as set so that only a particular key which is matched with attribute can decrypt the ciphertext. The user key and the attribute are matched if it matches it can decrypt a particular ciphertext. When there are k attributes are overlay among the ciphertext and a private key the decryption is granted [5].

A multi group key management accomplishes a hierarchical access control by applying an integrated key graph also handling the group keys for different users with multiple access authorities. Centralized key management plan uses tree structure to minimize the data processing, communication and storage overhead. It maintains things related to keying and also updates it. It accomplishes an integrated key graph for every user [6].

Identity-based encryption (IBE) is a vital primary thing of identity bases cryptography. The public key of user contains distinct information of user's identity. The key can be textual value or domain name, etc. IDE is used to deploy the public key infrastructure. The identity of the user is used as identity string for public key encryption. A trusted party called private key generator (PKG) in IBE which has the master secret key and gives secret key to users according to the user identity. The data owner collaborate the public value and the identity of user to encrypt the data. The ciphertext is decrypted using secret key [7].

In a multi attribute-authorities numbers of attributes are analyzed regarding the decryption key and the user must get a particular key related to the attribute while decrypting a message. The decryption keys are allocated independently to users those who have attribute identity without interaction between each other. Multi-authority attribute-based encryption allows real time deployment of attribute based privileges as different attributes are issued by different authorities. The attribute authorities ensure the honesty of the user privilege so the confidentiality is maintained by central authority [8].

2.1 View of Cloud Computing : M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia are a term of persons presented data security is one of the most important objections in the cloud computing. There is also analysis about storage area as hard disk, virtual machine memory contents and its requirements for audit-ability. Namely user-level encryption of storage is common for high-value data outside the cloud architecture, its tools and existing user information are available. This cloud approach was successfully used by TC3, in the area of healthcare company. This is used for access of data about patient records and claims, when moving their compliant application to AWS. Audit-ability could be added as an additional layer within the virtualized guest OS, and its audit-ability and confidence providing facilities to improve more security into the applications development and centralizing. Theses software responsibilities related into a single logical layer to focusing the applications and services.

2.2**. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing :** C.Wang, Q. Wang, K. Ren, and W. Lou are presented a cloud based storage system containing storage server's collections. TPA is a separate system which contains serious eight causes concerns over data confidentiality in data. Generally encryption method is used for data protection but also limit the functionality of the storage system because a few operations are supported over encrypted data storing. The challenges of secure storage system is support multiple functions with no central authority and distributed type. They propose a secure storage distributed system which propose a threshold proxy re-encryption scheme to integrate decentralized code. The distributed storage supports secure, retrieval and robust type of data storage. In the retrieval supporting secure storage distributed system a user can forward any type of data into storage servers and other user cannot able to retrieving the data recovery. The main technical contribution is proxy re-encryption scheme, which supports encrypted type messages to perform encoding. They suggest suitable parameters for the number of dispatched message copies to storage servers and the storage servers are queried by using a key server.

2.3. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing : S. Yu, C. Wang, K. Ren and W. Lou are presented new challenges for data security and access control, when confidential user data sharing on un-trusted cloud server. The cryptographic methods are using for existing solutions in the disclosing data decryption keys. The problem are depends upon some of its properties fine-graininess, scalability, and confidentiality and access control are remain unresolved. In this paper mention this open challenging issue by hand, define and enforcing access policies based on data attributes, The elevate data owner to commutated this tasks ,which involved in fine-grained data access control in to un-trusted cloud servers .The main goal by exploiting and unique wise combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. They proposed scheme has salient user access properties of confidentiality and accountability.

2.4. Scalable and Efficient Provable Data Possession : G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik are developed a design a scalable and effective cloud based distributed storage. The design based on step by step cooperative PDP scheme, which contain lightweight and secure provably property. Using in architecture to develop a hierarchy structure which supports file storage representation. The hierarchical structure represents relationships among all blocks in the stored resources. Homomorphic verifiable is the CPDP key technique which reduces the communication bandwidth and support dynamic type operations.. The PDP or PoR is a probabilistic proof technique, which focus in the single data storage un-trusted cloud servers but not suitable for a multi cloud environment. The data possession without downloading data at un-trusted stores, not suitable for distributed cloud storage since they were not originally constructed on interactive proof system. The homomorphic doesn't responses from multiple clouds, when using a scalable and unsuitable third party auditor for verification.

2.5 Ensuring Data Storage Security in Cloud Computing : C. Wang, Q. Wang, K. Ren, and W. Lou are proposed distributed architecture to ensure the data correctness of IT Enterprise and users. The distributed storage system provides guarantee in redundancy and dependability. In the centralized large data centers which act as a application software as well as databases to management and services provider in the data storage server. In this work studies about ensuring the integrity of data storage containing the problem in cloud Computing. In particular, a third party auditor (TPA), to verify dynamic data and its integrity in the cloud. The dynamics data support in the forms of data operation such modification, insertion, and deletion. So the cloud data services are not limited to archive or data backup

2.6 Role Based Encryption (RBE) Scheme

In RBE scheme, the owner of the data encrypts the data in such a way that only the users with appropriate roles as specified by a RBAC policy can decrypt and view the data. The role grants permissions to users who qualify the role and can also revoke the permissions from existing users of the role. The cloud provider (who stores the data) will not be able to see the content of the data if the provider is not given the appropriate role. The RBE scheme is able to deal with role hierarchies, whereby roles inherit permissions form other roles. A user is able to join a role after the owner has encrypted the data for that role. The user will be able to access that data from then on, and the owner does not need to re-encrypt the data. A user can be revoked at any time in which case, the revoked user will not have access to any future encrypted data for this role. With RBE scheme, revocation of a user from a role does not affect other users and roles in the system. In addition, RBE outsources part of the decryption computation in the scheme to the cloud, in which only public parameters are involved. By using this approach, RBE scheme achieves an efficient decryption on the client side. The same strategy of outsourcing to improve the efficiency of the management of user to role memberships, involving only public parameters.

2.7 Attribute Based Encryption Model (ABE)

Attribute-based encryption is more suitable to protect the confidentiality and secrecy of data in a cloud. It is useful for the source of the data that unknown of the personality of the receiver and their public key; it only knows certain attributes of the receiver. ABE identifies a user with a set of attributes. Two variants are proposed in the literature as an extension of ASE: Key Policy based ABE (KP ABE) scheme and the Cipher Text Policy based ABE (CP ABE) scheme. In KP ABE [18], the key is related with the access tree and the cipher text is related with an attribute set. The encrypting party will not have control for users who are going to access the data and it can define the set of attributes necessary for decrypting the cipher text. In CP-ABE [19], the cipher text is related to the access tree and the owner will determine the policy for decrypting the data, the key is related with a attribute set.

3 Proposed Method

In proposed system, instead of showing complete data, fetching of required data is carried out thus achieving fine-grained access control. This resulted in an efficient system response time as well as increased performance of the system. For security purpose, the proposed scheme consists of 3 keys: Private, Public and Master key. Public key is used in encryption of data, Private and public key is used to decrypt the data and Master key is used for accessing the allowable data. We are also achieving scalability which manages the workload within company by assigning lower level authority task to higher level authority in case of lower level authority absence or leave. It also involves flexible access of data in which when an employee is transferred to another location/branch, the main database is updated. It reduces the work of manual data transfer. Another feature provided is User Revocation [5] that allows expiration of user's key to be updated after the duration of key is near to expiration. This system also maintains a single cloud with a main database for multiple branches as a virtual partition viewing as every branch has its own cloud.

In order to achieve secure,scalable and fine grained data sharing on out sourced data in the cloud we are using the cryptography technique called KP-ABE with private aggregate key from a key hierarchy in this proposed scheme we have following steps.

1.Identify the attribute of files to be stored in cloud.
2.Constructing a key hierarchy structure with attributes of files.
3.Key generation.
4.Encryption.
5.Decryption.

Our proposed scheme explained with following case study with health care data.

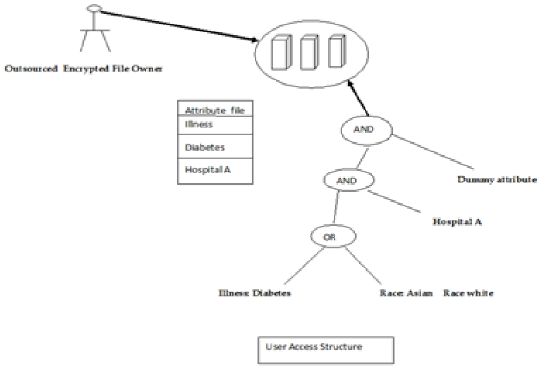


Fig1 Heirarchical Key Structure

The steps or in phases in our proposed system can be explained in detail as follows.

1.Identify the attribute of files to be stored in cloud: Thisis the liminary step which is required for generating a key this is performed by data owner.In this case based on the content stored in the file the data owner identifies the attributes here attributes nothing but some important key words in the content for example in previous case study when the hospital information is stored in the cloud as file the attributes can be various key words related to hospital disease,doctors,diagonosis,medicines.

2.Constructing a key hierarchy structure with attributes of files(key generation): Actually thesteps 1 and 2 called as key generation phase in this phase once attributes are identified then using those attributes we construct a key hierarchy structure.Here key hierarchy structure means a tree of various keys based on parent child relationship between attribute is found.

Example: When we consider previous case study is the hierarchical key structure is asa follows.

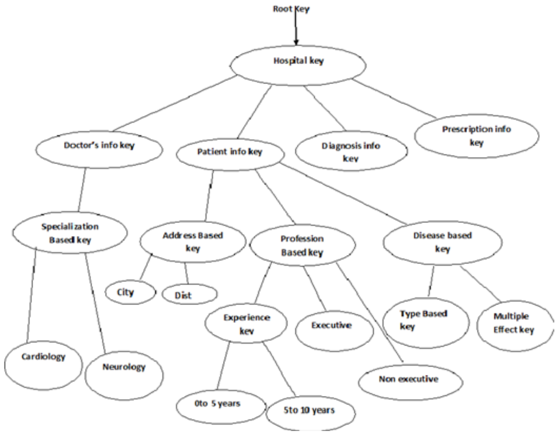


Fig2 Heirarchical Key Structure Example1

Example2: The following the hierarchical key structure based on patient health record information.

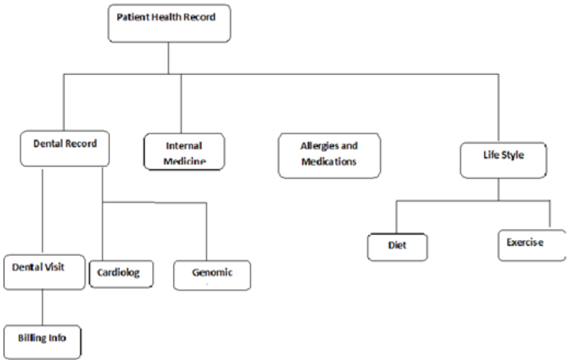


Fig 3 Heirarchical Key Structure Example2

In order to construct this heirachy key structure we use set theory in mathamatics the following are detail steps for heirachicalstructre using set theory.

1.From the given attribute list a master key is identified which is called universe set this is called root key structure.
2.Now from the attribute we form different sets of information based on attribute now each set becomes one key.
3.Now we apply set union and intercept operations to know the common between different sets based on these operation we form hierarchy of parent child relationship.
4. Here every key in key heirachiacl aggregation of several keys.

3. Key generation

Here whenever we encrypt/decrypt files a aggragate key is generated.

4.Encryption: This is the phase where file is encrypted into secret form .
1.Data owner extracts required key from key heirachy and applies encryption of file now it generates a cipher text file.
2.This file is stored in cloud which is unreadable for others.
3.Sharing of encrypted data once file is encrypted in stored in cloud then the data owner the file shred in to any other user.Then the data owner transmits the key to the user now user can read and sometimes modify the data based on priviliges.

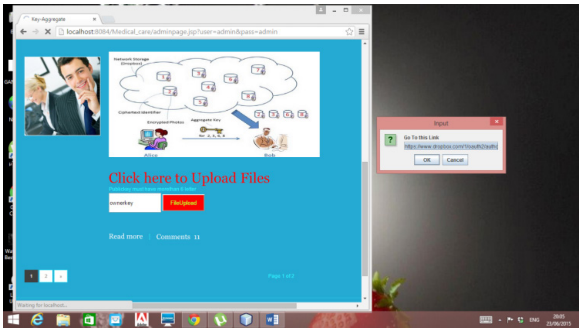
5.Decryption: Any user who access the encrypted file from cloud is first applied with decryption when decryption is compared with extracted key from heirachiacl structure then decryption is performed .

The both encryption and decryption are based DES alogorithms.

4 Experimental Setup and Results Analysis

This section describes the experimental setup for carrying out the experiments we designed and deployed the application in the testbed (sample cloud) to reseamble the real world scenario.

We designed the testbed using a server with intelxenon during core processor,2GB memory in this server we created a host meachine and several virtual meachine in the host meachine we deployed web server and web application, in one virtual meachine we deployed my SQL data base and in other virtual mecahines we created aglobal disk space for storing file.The host meachine and virtual meachine collectively acts as cloud the web application provides interface for end users to upload and download files.The following Figures represents the execution process of the sysyem. These Figures represents storing data in cloud by uploading files, encryption during upload process, share the files, downloading the files and decrypting the files during downloading process.



localhost:8084/Medical_care/adminpage.jsp?user=admin&pass=admin

Click here to Upload Files

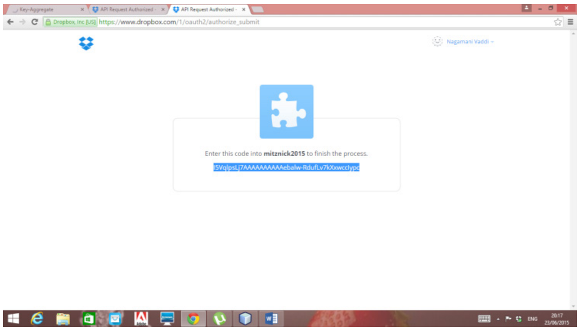
Publickey must have morethan 6 letter

ownerkey

Go To this Link

https://www.dropbox.com/1/oauth2/authc

Figure 4 Uploading Files and Key Generation

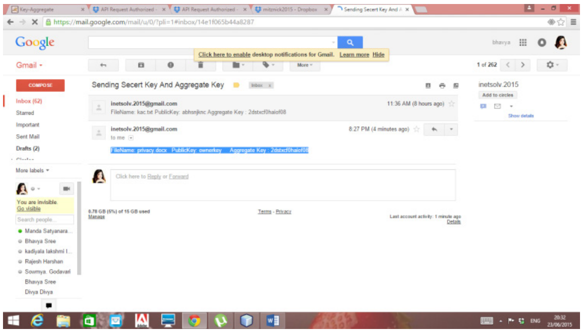


https://www.dropbox.com/1/oauth2/authorize_submit

Enter this code into **mitznick2015** to finish the process.

I5VqlpsLj7AAAAAAAAAAebalw-RdufLv7kXxwcclypc

Figure 5 Key Generation



https://mail.google.com/mail/u/0/?pli=1#inbox/14e1f065b44a8287

Click here to enable desktop notifications for Gmail. Learn more Hide

Sending Secert Key And Aggregate Key

inetsolv.2015@gmail.com 11:36 AM (8 hours ago)
FileName: kac.txt PublicKey: abhsnjknc Aggregate Key : 2dstxcf0haiof08

inetsolv.2015@gmail.com 8:27 PM (4 minutes ago)
to me

FileName: privacy.docx PublicKey: ownerkey Aggregate Key : 2dstxcf0haiof08

Click here to Reply or Forward

0.78 GB (5%) of 15 GB used
Manage

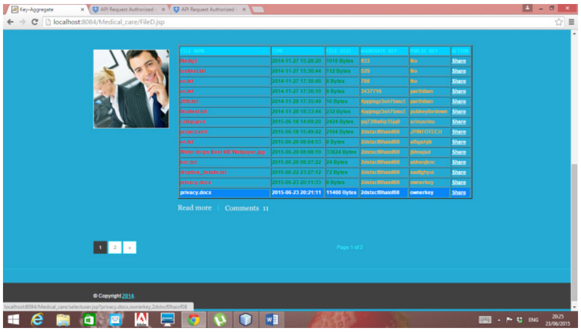
Terms - Privacy

Last account activity: 1 minute ago
Details

inetsolv.2015

You are invisible.
Go visible

Figure 6 Uploading Files into drop Box (Cloud)



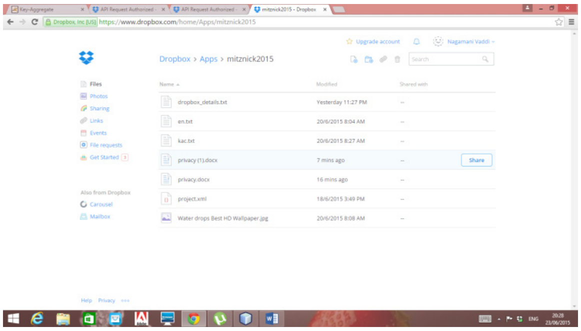
localhost:8084/Medical_care/FileD.jsp

FILE NAME	TIME	FILE SIZE	AGGREGATE KEY	PUBLIC KEY	ACTION
filedig3	2014-11-27 15:28:20	1016 Bytes	933	No	Share
lasttest.txt	2014-11-27 15:30:44	112 Bytes	529	No	Share
en.txt	2014-11-27 17:30:40	8 Bytes	708	No	Share
en.txt	2014-11-27 17:36:10	8 Bytes	3437716	parthiban	Share
28th.txt	2014-11-28 17:35:49	16 Bytes	4ppjmgz3sh7bmct	parthiban	Share
finaltest.txt	2014-11-28 18:33:44	232 Bytes	4ppjmgz3sh7bmct	pubkeyfordown	Share
callup.java	2015-06-18 14:09:20	2424 Bytes	pq73f8a6iy35jq0	srinusrinu	Share
project.xml	2015-06-18 15:49:42	2104 Bytes	2dstxcf0haiof08	JPINFOTECH	Share
en.txt	2015-06-20 08:04:53	8 Bytes	2dstxcf0haiof08	afbgshjk	Share
Water drops Best HD Wallpaper.jpg	2015-06-20 08:08:19	33824 Bytes	2dstxcf0haiof08	jbhnajsd	Share
kac.txt	2015-06-20 08:27:22	24 Bytes	2dstxcf0haiof08	abhsnjknc	Share
dropbox_details.txt	2015-06-22 23:27:12	72 Bytes	2dstxcf0haiof08	sadfghyui	Share
privacy.docx	2015-06-23 20:11:33	8 Bytes	2dstxcf0haiof08	ownerkey	Share
privacy.docx	2015-06-23 20:21:11	11400 Bytes	2dstxcf0haiof08	ownerkey	Share

© Copyright 2014.

localhost:8084/Medical_care/selectuser.jsp?privacy.docx,ownerkey,2dstxcf0haiof08

Figure 7 Viewing Files in drop Box (Cloud)



Key-Aggregate | API Request Authorized - | API Request Authorized - | mitznick2015 - Dropbox

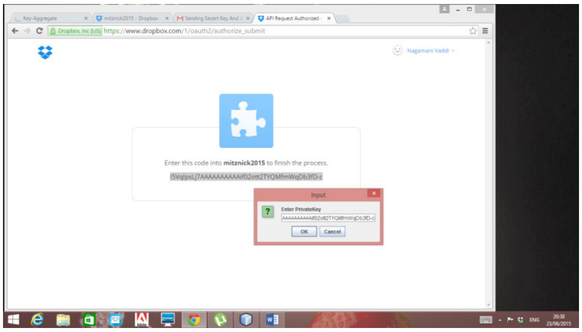
Dropbox, Inc [US] https://www.dropbox.com/home/Apps/mitznick2015

Upgrade account | Nagamani Vaddi

Dropbox > Apps > mitznick2015

Name	Modified	Shared with
dropbox_details.txt	Yesterday 11:27 PM	--
en.txt	20/6/2015 8:04 AM	--
kac.txt	20/6/2015 8:27 AM	--
privacy (1).docx	7 mins ago	--
privacy.docx	16 mins ago	--
project.xml	18/6/2015 3:49 PM	--
Water drops Best HD Wallpaper.jpg	20/6/2015 8:08 AM	--

Figure 8 Secure data in drop Box (Cloud)



Key-Aggregate | mitznick2015 - Dropbox | Sending Secert Key And A | API Request Authorized -

Dropbox, Inc [US] https://www.dropbox.com/1/oauth2/authorize_submit

Nagamani Vaddi

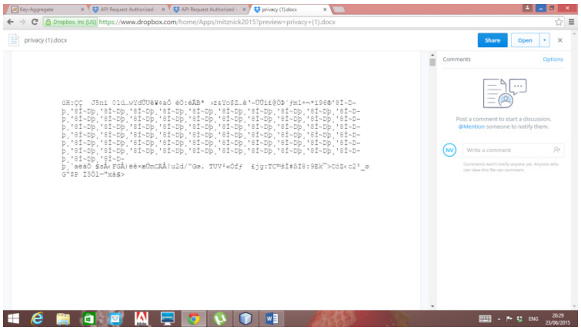
Enter this code into **mitznick2015** to finish the process.

I5VqlpsLj7AAAAAAAAAAif02ott2TYQMfmWqDb3fD-c

Input

Enter PrivateKey: AAAAAAAAAAif02ott2TYQMfmWqDb3fD-c

Figure 9 Downloading Files from Cloud (Drop Box).



Key-Aggregate | API Request Authorized - | API Request Authorized - | privacy (1).docx

Dropbox, Inc [US] https://www.dropbox.com/home/Apps/mitznick2015?preview=privacy+(1).docx

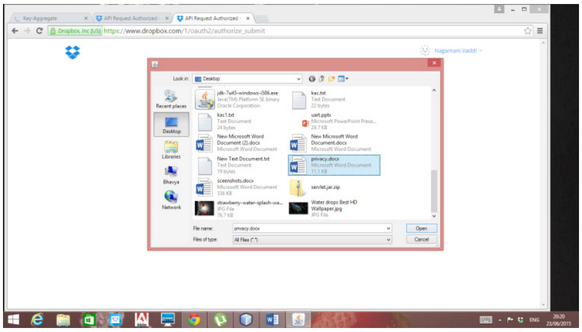
privacy (1).docx

```
úH:ÇÇ  J5nı 01ù…wYdÛÜè¥¢aÔ èÖ:èÄB* >z&Yo$Z…ê'-ÛÜi£@ÓÞ´ƒm1÷¬*196®'8Î~D-
þ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~D-
þ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~D-
þ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~D-
þ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~D-
þ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~D-
þ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~Dþ,'8Î~D-
þ,'8Î~Dþ,'8Î~D-
þ,¨aeàÔ $sÅ‹FGÅ)ëë×æÛmCÅÅ!u2d/"Gœ. TUV¹«Ôfƒ  £jg:TC™šÎ#ßÏ8:9Ek¯>CòZ‹c2³_ø
G"$P I5Ö1—"xà$>
```

Comments | Options

Post a comment to start a discussion. @Mention someone to notify them.

Figure 10 Sharing Secret key and Aggregate Key



Key-Aggregate | API Request Authorized - | API Request Authorized -

Dropbox, Inc [US] https://www.dropbox.com/1/oauth2/authorize_submit

Nagamani Vaddi

Look in: Desktop

jdk-7u45-windows-i586.exe Java(TM) Platform SE binary Oracle Corporation	kac.txt Text Document 22 bytes
kac1.txt Text Document 24 bytes	uart.pptx Microsoft PowerPoint Prese... 29.7 KB
New Microsoft Word Document (2).docx Microsoft Word Document	New Microsoft Word Document.docx Microsoft Word Document
New Text Document.txt Text Document 19 bytes	privacy.docx Microsoft Word Document 11.1 KB
sceenshots.docx Microsoft Word Document 336 KB	servlet.jar.zip
strawberry-water-splash-wa... JPG File 76.7 KB	Water drops Best HD Wallpaper.jpg JPG File

File name: privacy.docx

Files of type: All Files (*.*)

4.1 Factors In Analyzing The Cryptosystem

We consider some factors such as key tree of height h, ciphet texdt classes 2^h,n_a number oof symmetric keys to be assigned, r delegation ratio the ratio of the delegated ciphertext classes to the total classes. for different h values we tabulate the results as follows.

h	r	0.1	0.2	0.3	0.4	0.5
16	n_a	6024.8	10072.5	10579.3	20045.8	20520.7
	na N	4.65%	8..5%	12.2%	14.8%	16.9%
18	n_a	24024.8	40072.5	40579.3	80045.8	80520.7
	na N	4.65%	8..5%	12.2%	14.8%	16.9%
20	n_a	97024.8	160072.5	164579.3	320045.8	330520.7
	na N	4.65%	8..5%	12.2%	14.8%	16.9%

Table 1 Comression rattio's of different tree heights

The following Diagram explains the Comression factor and Delegation ratio.

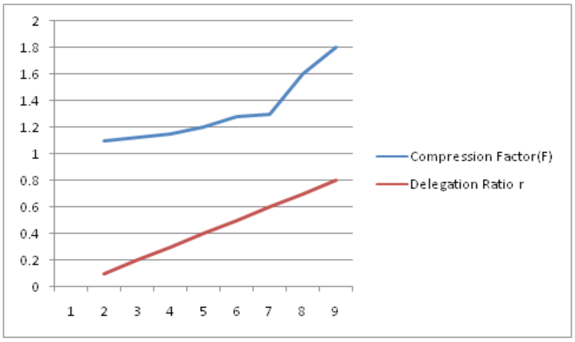


Figure 11 Comression Factor for Different Keys

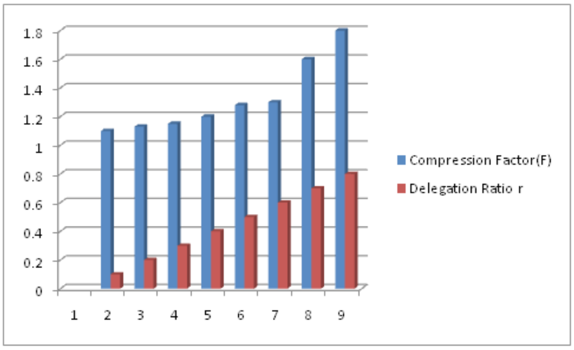


Figure 12 Comression Factor for Different Keys

5 Conclusion

To share data flexibly is vital thing in cloud computing. Users prefer to upload there data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Public-key cryptosystems provides delegation of secret keys for different ciphertext classes in cloud storage. The delegatee gets securely an aggregate key of constant size.

Thus, we efficiently provide a fine grained access control with flexibility and scalability with a hierarchical structure in our system. Our contribution to this paper will be providing security to the users from outsiders or intruders by implementing session hijacking and session fixation security in our system. Also, a performance analysis will be done by the employee's updating monthly record performance.

REFERENCES

[1].Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, andRobert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage". | [2].S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICESimple Privacy-Preserving Identity Management for Cloud Environment"in Applied Cryptography and Network Security – ACNS2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543. | [3]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Stor-age," IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013. | [4]. B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Dataon the Cloud via Security-Mediator," in Interna-tional Conferon Distributed Computing Systems - ICDCS 2013. IEEE, 2013. | [5]. S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng,"Dynamic Secure Cloud Storage with Provenance," in Cryptographyand Security: From Theory to Applications - Essays Dedicatedto Jean-Jacques Quisquater on the Occasion of His 65th Birthday, serLNCS, vol. 6805. Springer, 2012, pp. 442–464. | [6]. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggre-gateand Verifiably Encrypted Signatures from Bilinear Maps," inProceedings of Advances in Cryptology - EU-ROCRYPT '03, ser. LNCS,vol. 2656. Springer, 2003, pp. 416–432. | [7]. M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamicand Efficient Key Management for Access Hierar-chies," ACMTransactions on Information and System Security (TISSEC), vol. 12,no. 3, 2009. | [8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Pa-tientControlled Encryption: Ensuring Privacy of Electronic MedicalRecords," in Proceedings of ACM Workshop on Cloud ComputingSecurity (CCSW '09). ACM, 2009, pp. 103–114. | [9]. F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Sin-gle-KeyDecryption without Random Oracles," in Proceed-ings of InformationSecurity and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990.Springer, 2007, pp. 384–398. | [10]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attrib-ute-Based Encryption for Fine-Grained Access Control of Encrypted data,"in Proceedings of the 13th ACM Conference on Computer and CommunicationsSecurity (CCS '06). ACM, 2006, pp. 89–98. | [11]. S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problemof Access Control in a Hierarchy," ACM Transac-tions on ComputerSystems (TOCS), vol. 1, no. 3, pp. 239–248, 1983. | [12]. G. C. Chick and S. E. Tavares, "Flexible Access Control withMaster Keys," in Proceedings of Advances in Cryptolo-gy - CRYPTO'89, ser. LNCS, vol. 435. Springer, 1989, pp. 316–322. | [13]. W.-G. Tzeng, "A Time-Bound Cryptographic Key As-signmentScheme for Access Control in a Hierarchy," IEEE Transactions onKnowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188,2002. | [14]. G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masuc-ci,"Provably-Secure Time-Bound Hierarchical Key Assign-mentSchemes," J. Cryptology, vol. 25, no. 2, pp. 243–270, 2012. | [15]. R. S. Sandhu, "Cryptographic Implementation of a Tree Hierarchyfor Access Control," Information Processing Let-ters, vol. 27, no. 2,pp. 95–98, 1988. | [16]. Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control inSecure Group Communications," in Proceedings of the 23th IEEEInternational Conference on Computer Communications (INFOCOM'04). IEEE, 2004. | [17] Q. Zhang and Y. Wang, "A Centralized Key Manage-mentSchemefor Hierarchical Access Control," in Proceedings of IEEE GlobalTelecommunications Conference (GLOBECOM '04). IEEE, 2004, pp.2067–2071. | [18] J. Benaloh, "Key Compression and Its Application to DigitalFingerprinting," Microsoft Research, Tech. Rep., 2009. | [19] B. Alomair and R. Poovendran, "Information Theoreti-cally SecureEncryption with Almost Free Authentication," J. UCS, vol. 15,no. 15, pp. 2937–2956, 2009. | [20] D. Boneh and M. K. Franklin, "Identity-Based Encryp-tion from theWeil Pairing," in Proceedings of Advances in Cryptology - CRYPTO'01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229. | [21] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryp-tion," inProceedings of Advances in Cryptology - EU-ROCRYPT '05, ser. LNCS,vol. 3494. Springer, 2005, pp. 457–473. | [22] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "PracticalLeakage-Resilient Identity-Based Encryption from Simple Assumptions,"in ACM Conference on Computer and CommunicationsSecurity, 2010, pp. 152–161. | [23] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How toDecrypt Multiple Ciphertexts Using a Single Decryption Key," inProceedings of Pairing-Based Cryptography (Pairing '07), ser. LNCS,vol. 4575. Springer, 2007, pp. 392–406. | [24] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conferenceon Computer and Communications Security, 2009, pp. 121–130. | [25] T. Okamoto and K. Takashima, "Achieving Short Ci-phertexts orShort Secret-Keys for Adaptively Secure General Inner-ProductEncryption," in Cryptology and Network Security (CANS '11), 2011,pp. 138–159. | [26] R. Canetti and S. Hohenberger, "Chosen Ciphertext Secure Proxy Re-Encryption," in Proceedings of the 14th ACM Conference onComputer and Communications Security (CCS '07). ACM, 2007,pp. 185–194. | [27] C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Reencryptionwithout Random Oracles," in Information Security Conference (ISC'07), ser. LNCS, vol. 4779. Springer, 2007, pp. 189–202. | [28] C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng,"Conditional Proxy Broadcast Re Encryption," in Aus-tralasianConference on Information Security and Privacy (ACISP '09), ser.LNCS, vol. 5594. Springer, 2009, pp. 327–342. | [29] S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "EfficientUnidirectional Proxy Re-Encryption," in Progress in Cryptology AFRICACRYPT 2010, ser. LNCS, vol. 6055. Springer, 2010, pp.316–332. | [30] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Im-provedProxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Transactions on Infor-mation and SystemSecurity (TISSEC), vol. 9, no. 1, pp. 1–30, 2006. | [31] D. Boneh, C. Gentry, and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," inProceedings of Advances in Cryptology - CRYPTO '05, ser. LNCS,vol. 3621. Springer, 2005, pp. 258–275. | [32].L. B. Oliveira, D. Aranha, E. Morais, F. Daguano, J. Lopez, andR. Dahab, "TinyTate: Computing the Tate Pairing in ResourceConstrainedSensor Nodes," in Proceedings of 6th IEEE InternationalSymposium on Network Computing and Applications (NCA '07).IEEE, 2007, pp. 318–323. | [33]. D. Naor, M. Naor, and J. Lotspiech, "Revocation and TracingSchemes for Stateless Receivers," in Proceedings of Advances inCryptology - CRYPTO '01, ser. LNCS. Springer, 2001, pp. 41–62. | [34]. T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu, "IdentityBasedEncryption Resilient to Continual Auxiliary Leakage," inProceedings of Advances in Cryptology - EU-ROCRYPT '12, ser. LNCS,vol. 7237, 2012, pp. 117–134. | [35]. D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical Identi-ty BasedEncryption with Constant Size Ciphertext," in Pro-ceedings of Advancesin Cryptology- EUROCRYPT '05, ser. LNCS, vol. 3494.Springer, 2005, pp. 440–456. | [36]. D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen CiphertextSecurity from Identity-Based Encryption," SIAM Journal on Computing(SIAM-COMP), vol. 36, no. 5, pp. 1301–1328, 2007. | |