An Implementation of data sharing in Public Cloud using revocable-storage identity-based encryption and KUNode Algorithm

M.Saraswathi[1],V.Balu[2]

Assistant Professor ,Department of CSESCSVMV University,

Enathur, Kanchipuram, Tamilnadu

saraswathi.kumar@gmail.com[1]balukanchi@gmail.com[2]

Abstract

Data sharing is an important concept in cloud computingfor sharing data to public users.Cloud provides different servicesto the users for accessing data from cloud.Storage as aservice, it allows the data owners to store and share their data to usersthrough cloudserver. In this type of service it is necessary to place cryptographically enhanced access control on the shared data, named Identity-based encryption. Whenaccessing data some user's authorization is expired, there should be a mechanism that can remove him/her from the system. As a result, the revoked user unable to access both the previously stored data. Thus, propose a notion called revocable-storage identity-based encryption (RS-IBE) .In this paper, we implemented and proved that a revoked user can able to access the previous data using secret key in Just cloud environment and same data to be shared to public users.

Index Terms—Cloud computing, data sharing, Cloudstorage, Access control, Identity-based encryption, Just cloud

1. Introduction

The Cloud Computing refers to "Computing over the Internet". It provides huge computation capacity and vast memory space at a low cost [4].The network, servers, and storage and virtualization technologies to form a shared infrastructure that enables web-based value added services. End users access cloud-based applications through a web browser or a light-weightdesktop or mobile application. Thecloud model comprises five vital characteristics are on-demand self-service, broad network access, resourcepooling, rapid elasticity, and measured services. It alsooffers main three service models such as software as aservice (SaaS),Platform as a service (PaaS), andinfrastructure as a service (IaaS)and four deploymentmodels are public, private, community, or hybrid Cloud. Cloud services should be scalable, service orientedand shared, metered by use, customer focused, use internettechnologies in cloud system.

Cloud storage as a service is an important service of cloud computing which allows data owners tomove data from their local computing systems to the cloud system.Cloud systems can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user.Cloud storage has several advantages over traditional data storage relief from the burden for storage management, universal data access with location independence and avoidance of capital expenditure on hardware, software and personnel maintenances [3].Example :Google Docs provides data sharing capabilities as groups of students or teams working on a project can share documents and can collaborate with each other effectively. The architecture of Data sharing is represented in below fig 1.1

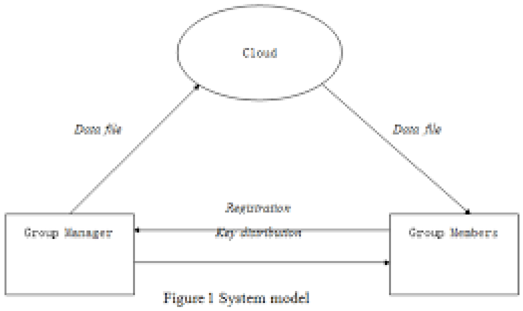


Fig 1.1 Data sharing Architecture

1.1 OBJECTIVE:

Main objective of this paper is achieving secure data sharing in public cloud environment. Data owner can upload the shared data to the cloud server in Just Cloud Storage .Cloud service provider giving provisions to download or sharing a files to the authenticate users from the cloud server.The plaintext of the shared data is not available for an unauthorized user and even the cloud service provider also. If, authorization gets expired, the user can download the cipher text of the shared data, and then decrypt-then-re-encrypt the shared data and then upload the re-encrypted data to the cloud server again.

2. EXISTING SYSTEM

In this Existing System, Outsourcing data to the cloud server denote that data is control out of users and cloud service provider also. The data usually consists of valuable and sensitive information. Thisoutsourced data can be shared in an open in the cloud environment and the cloud server would become a target of attacks. It's concept of the key management system and then uses the algorithm of revocable-storage identity-based encryption (RIBE).

RIBE Based data sharing procedure:

1. The data owner encrypts the data and uploads the ciphertext to the cloud server then decides the authenticate users to share the data
2. If the user is authenticated,he/she download and decrypt the ciphertext.
3. If any user authentication gets expired ,he/she is prevented to access the plaintext of the data.In this case,the data owner download the ciphertext of the shared data and then decrypt then re encrypt it.

Such a data sharing system fulfils the three security goals. The security goals are data confidentiality, Forward secrecy, and backward secrecy

Data confidentiality: Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server.

Forward secrecy: Forward secrecy means that, when a user’s authority is expired, or a user’s secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her

Backward secrecy: Backward secrecy says that, when a user’s authorization is expired, or a user’s secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

Limitation in existing system is the process of decrypt then reencrypt ,it is inadvisable to update the ciphertext periodically by using secret key. Overall Efficiency will be decreased and computation cost also increased

3. Proposed system

In the proposed system, used a mechanism revocable-storage identity-based encryption (RSIBE) and KUNode algorithm for building a cost-effective data sharing system .It enables a data owner to add the current time period to the ciphertext such that the receiver can decrypt the ciphertext within that time period.

The proposed system attains the following characteristics: We can provide formal definitions for RS-IBE• and its corresponding security model; and backward/forward secrecy simultaneously.

KUNODES ALGORITHM: By using this algorithm onlynon-revoked user at a time period are able to decrypt the cipher text.

INPUT: Binary tree revocation list,Time period

OUTPUT: outputs the smallest subset Y of nodes of BT such that Y contains an ancestor for each node that is not revoked before the time period t.

STEP 1: Data owner upload the file in cloud with validity time

2. Data user access the data.

 2.1. if the user tries to access the data within a specified time only he/she is able to access the data

 2.2. Otherwise data owner need to update the key.

3. Data owner update the key used by the user.

4. Then he will update the cipher text. This will provide both forward and backward security to the data stored in a cloud.

By this algorithm ,when we revoke the leaf node(id3) their ancestors also get updated(nodes in green color) and the node which shares the same key of revoked nod(nodes in orange color)e also get updated.

Algorithm 1 KUNodes(BT, RL, t)

```
:$X,Y\leftarrow-\emptyset$
:for all $(\eta i ,ti)\in RL$ do
    : if $ti\leq t$ then
        : Add Path($\eta i$) to X
    : end if
:end for
:for all $\theta\in X$ do
    : if $\theta l\in/X$ then
        : Add $\theta l$ to Y
    : end if
    : if $\theta r\in/X$ then
        : Add $\theta r$ to Y
    : end if
: end for
: if $Y=\emptyset$ then
    : Add the root node $\varepsilon$ to Y
: end if
: returnY
```

DEFINITION IN RS-IBE:

A revocable-storage identity-based encryption scheme with message space M, identity space I and total number of time periods T is comprised of the following seven polynomial time algorithms

[1]. Setup(1λ , T, N): the setup algorithm takes as input the security parameter λ ,the time bound T and the maximum number of system users N , and it outputs the public parameter P P and the master secret key M SK, associated with the initial revocation list RL=∅ and state st.

[2]. PKGen(P P, M SK, ID): The private key generationalgorithm takes as input P P , M SK and an identity ID ∈I, and it generates a private key SKIDfor ID and an updated state st.

[3]. KeyUpdate(P P, M SK, RL, t, st): The key update algorithm takes as input P P , M SK, the current revocationlist RL, the key update time t≤T and the state st, it outputs the key update KUt

[4]. DKGen(P P, SKID, KUt): The decryption key generation algorithm takes as input P P , SKID and KUt , and it generates a decryption key DKID,t for ID with time period t or a symbol ⊥ to illustrate that ID has been previously revoked.

[5]. Encrypt(P P, ID, t, M): The encryption algorithm takesas input P P , an identity ID, a time period t≤T , and a message M∈M to be encrypted, and outputs a cipher text CTID,t.

[6]. CTUpdate(P P, CTID,t, t′): The ciphertext update algorithm takes as input P P , CTID,t and a new time period t ′ ≥ t, and it outputs an updated ciphertextCTID,t′ .

[7]. Decrypt(P P, CTID,t, DKID,t′): The decryption algorithm takes as input P P , CTID,t, DKID,t′ , and it recovers the encrypted message M or a distinguished symbol ⊥ indicating that CTID,t is an invalid ciphertext.

[8]. Revoke(P P, ID, RL, t, st): The revocation algorithmtakes as input P P , an identity ID∈I to be revoked, the current revocation list RL, a state st and revocation time period t≤T , and it updates RL to a new one

4. Implementation

In this paper hasdeveloped five modules such as user Registration page, keyaccess, fileupload, RSIBE and Data sharing

4.1User Registration Page:

To connect with Cloud server user must login with their username and password then only they can able to connect with the server. Server will create the account for the user to maintain upload file and download/sharing file to other user. If the user is new user, user must record their details such as username, password, reenter password,gender and Email idetc or already existing user directly can login into the server.

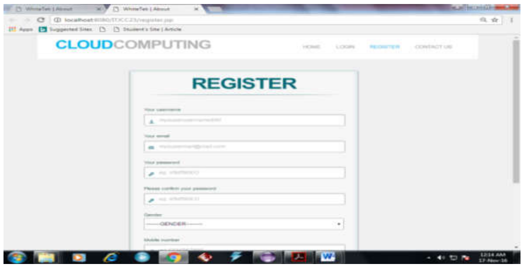
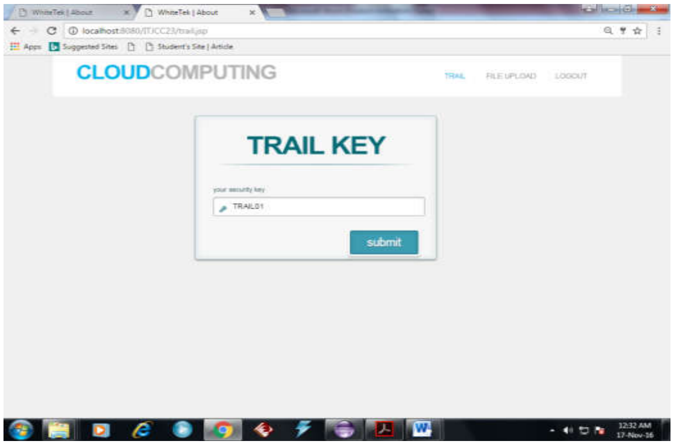


Fig 4.1 New User Registration Page

4.2 KEY ACCESS:

In this module, once registration process completed the user can login to the server, the server sent the dynamic Trial/secret key for uploading the file. Using that key user can upload many files at a time.



your security key: TRAIL01

Fig 4.2 Key Generation

4.3 File Upload

After receiving key from Data owner he/she upload a many documents with using same key.

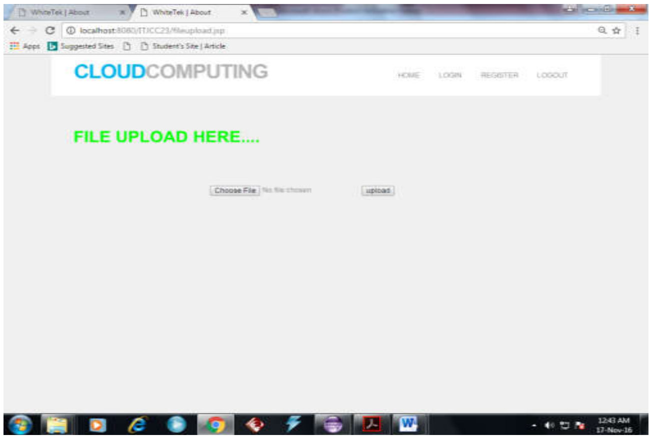
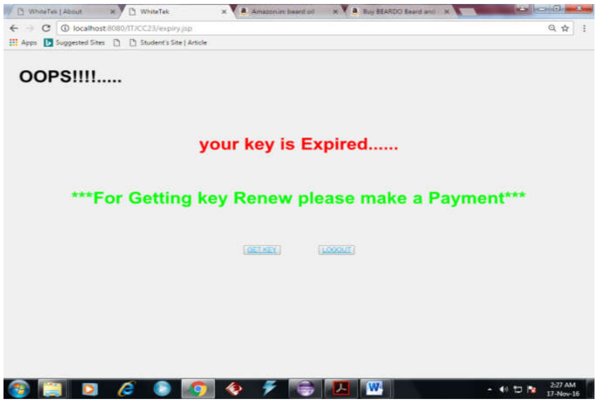


Fig 4.3 File Upload

4.4 Revocable storage Identity Based Encryption

In this module, implemented Forward secrecy. i.e if the user's authority is expired or secret key is compromised should be prevented to accessing the plaintext of the shared data that can be previously accessed from the server. Itis shown in below figure 4.4. New key will be generated as per existing user request.



OOPS!!!!.....

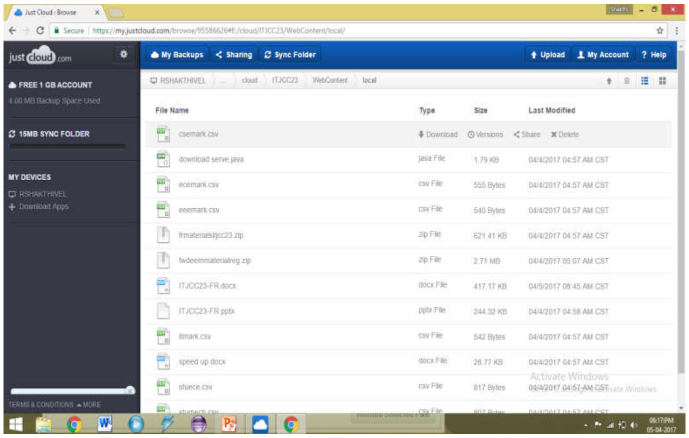
your key is Expired......

For Getting key Renew please make a Payment

4.4 New Key generation

4.5 File store to cloud server

Cloud file sharing, also called cloud-based file sharing or online file sharing, is a system in which a user is allotted storage space on a server and reads and writes are carried out over the Internet. Here we are used Just Cloud with Free Trial Version for file storage with 1 GB space. In the below fig representsthe authorized user uploaded documents with the details such as file name, FileType, size and modified date and Time.


https://my.justcloud.com/browse/95586626#E:/cloud/ITJCC23/WebContent/local/
justcloud.com
My Backups
Sharing
Sync Folder
Upload
My Account
Help
FREE 1 GB ACCOUNT
4.00 MB Backup Space Used
15MB SYNC FOLDER
MY DEVICES
RSHAKTHIVEL
Download Apps
RSHAKTHIVEL … cloud ITJCC23 WebContent local

File Name	Type	Size	Last Modified
csemark.csv	Download	Versions Share	Delete
download serve.java	java File	1.79 KB	04/4/2017 04:57 AM CST
ecemark.csv	csv File	555 Bytes	04/4/2017 04:57 AM CST
eeemark.csv	csv File	540 Bytes	04/4/2017 04:57 AM CST
frmaterialsitjcc23.zip	zip File	621.41 KB	04/4/2017 04:57 AM CST
fwdeemmaterialreg.zip	zip File	2.71 MB	04/4/2017 05:07 AM CST
ITJCC23-FR.docx	docx File	417.17 KB	04/5/2017 08:45 AM CST
ITJCC23-FR.pptx	pptx File	244.32 KB	04/4/2017 04:58 AM CST
itmark.csv	csv File	542 Bytes	04/4/2017 04:57 AM CST
speed up.docx	docx File	28.77 KB	04/4/2017 04:57 AM CST
stuece.csv	csv File	817 Bytes	04/4/2017 04:57 AM CST
stumech.csv	csv File	[illegible]	[illegible]

4.5 File store to cloud server

5. Conclusion

In this paper, implemented secure data sharing in public cloud using Revocable storage Identity based encryption RS-IBE and KUNODE Algorithm, which supports identity revocation and cipher text update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data.

6. References

[1]. Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo “Secure Data Sharing in the Cloud “DOI: 10.1007/978-3-642-38586-5_2, © Springer-Verlag Berlin Heidelberg 2014

[2]. Jianghong Wei, Wenfen Liu, Xuexian Hu”Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption” IEEE Transactions on Cloud Computing (Volume: PP, Issue: 99) March 2016

[3]. B.V.Varshini#1, M.Vigilson Prem#2, J.Geethapriya# A Review on Secure Data Sharing in Cloud Computing International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 3, March 2017 Environment.

[4]. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.