International Journal of Computer science engineering Techniques-– Volume 8 Issue 2, 2024

RESEARCH ARTICLE OPEN ACCESS

An Encryption-Based Revocable Storage Identity and Lucas Kanade Algorithm-Based Public Azure Cloud Data Sharing System

S Sundeep kumar [1],
[1](Asst. prof,,Dept of CSE Sree Dattha Institute of Engineering and Science)
Sridhar Reddy Surukanti[2]
[2](Assistant Professor, Dept of CSE, Sreyas Institute Of Engineering And Technology,T.S ,India)
E.RAJENDRA[3] ,
[3](Assistant professor, Dept of CSE, Sri Indu College Of Engineering And Technology, ,T.S ,India)

Abstract

In cloud computing, data sharing is a key idea for disseminating data to general users.Users can access data from the cloud via a variety of services offered by the cloud. Data owners can store and share their data with customers via cloud servers thanks to storage as a service. Identity-based encryption, a cryptographically strengthened access control method, is required for this kind of service. There should be a way to delete a user from the system when their authorization to access data expires. The revoked user is consequently unable to access any of the previously saved data. In light of this, introduce the idea of revocable-storage identity-based encryption (RS-IBE).Using a secret key, we implemented and demonstrated in this work that a revoked user can still access earlier data.

Index Terms— Access control, identity-based encryption, cloud computing, data sharing, cloud storage, and just cloud

I. INTRODUCTION

The term "Computing over the Internet" relates to cloud computing. It offers enormous memory capacity and processing power at a cheap price [1].A shared infrastructure made up of the network, servers, storage, and virtualization technologies allows for web-based value-added services. End users can utilize a mobile or lightweight desktop application, or a web browser, to access cloud-based apps. Five essential features of the cloud model are resource pooling, quick flexibility, wide network access, on-demand self-service, and measured services. Additionally, it provides four deployment modes: public, private, community, or hybrid cloud. The core three service models [2] are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Cloud services should leverage internet technology [3] in a cloud system and be scalable, service-oriented, shared, metered by use, and customer-focused.

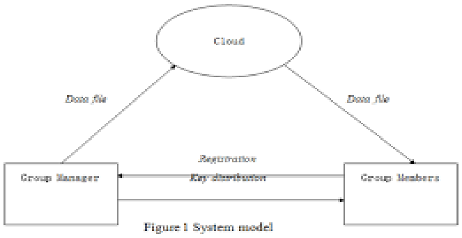


Fig 1.1 Data sharing Architecture

1.1 OBJECTIVE:

This paper's primary goal is to enable safe data sharing in public cloud environments. The shared data can be uploaded by the data owner to the Just Cloud Storage cloud server. The cloud service provider allows users who have verified their identity to download or share files from the cloud server. Both the cloud service provider and an unauthorized user cannot access the shared data's plaintext.

II. EXISTING SYSTEM

Outsourcing data to the cloud server [4] under this current system indicates that users and the cloud service provider both have control over the data. Usually, the data includes sensitive and important information. The cloud server may become the target of assaults if this outsourced data was shared in an open environment. It employs the revocable-storage identity-based encryption algorithm (RIBE) [5] after introducing the notion of the key management system. Procedure for sharing data based on RIBE:

1. After encrypting the information and uploading the cipher text to the cloud server, the data owner selects which authenticated users can access the data.

2. The user downloads and decrypts the cipher text if they are authenticated.

3. A user's ability to access the data's plaintext is blocked if their authentication [6] expires. In this instance, the data owner downloads the shared data's cipher text, decrypts it, and then re-encrypts it. Objectives. Data confidentiality accessible to unauthorized users. Transparent secrecy: In order to

maintain forward secrecy, a user's Backward secrecy: Backward secrecy says that, when a user's 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.

III PROPOSED SYSTEM

Following qualities: At the same time, we are able to offer formal definitions for backward/forward secrecy [8], RS-IBE, and the related security model.

KUNODES ALGORITHM: This algorithm allows the encrypted text to be decrypted by a single non-revoked user at a time.
INPUT: Revocation list of binary trees, time period
The result, Y, is the smallest subset of BT nodes, containing an ancestor for every node that hasn't been revoked before time period t.
Data owner uploads file to cloud with validity period in step one.
2. A data user retrieves data.
2.1. The user is the only one who can access the data if they attempt to do so within the allotted period.
2.2. The data owner must update the key in any other case.
3. The data owner updates the user's key.
4. He will then make updates to the cipher text. This will offer both forward and 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 node(nodes in orange color) [10] also get updated. Algorithm 1
KUNodes(BT, RL, t)

```
:$X,Y \leftarrow - \emptyset$
:for all $(\eta_i, t_i) \in RL$ do
    : if $t_i \leq t$ then
        : Add Path($\eta_i$) to X
    : end if
:end for
:for all $\theta \in X$ do
    : if $\theta_l \notin X$ then
        : Add $\theta_l$ to Y
    : end if
    : if $\theta_r \notin X$ then
        : Add $\theta_r$ to Y
    : end if
```

[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]. CT Update(P P, CTID,t, t′): The authorization is expired, or a user's secret computation cost also increase

The suggested method builds a cost-effective data sharing system using the KUNode algorithm [7] and the revocable-storage identity-based encryption (RSIBE) mechanism. It allows the owner of the data to include the current time in the ciphertext so that the recipient can decrypt it within that time frame.The system that is being suggested achieves the

```
: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 [9] 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 [11] 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 generation algorithm[12]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 revocation list 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 [13] 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 decryption algorithm takes as input P P , CTID, t, DKID,t′ ,

[7]. Decrypt (P P, CTID,t, DKID,t′): The

[8]. Revoke(P P, ID, RL, t, st): The revocation algorithm takes as input P P , an identity ID∈I to be revoked,

VI. IMPLEMENTATION

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

1.1 User Registration Page:

Users are only able to connect to the Cloud server after successfully logging in with their username and password. The user will be able to upload, download, and share files with other users after the server creates their account. If the user is a new one, they must input their login information (password, username, gender, email address, etc.) or they can log in to the server directly if they already have an account.

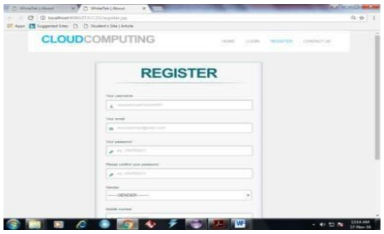
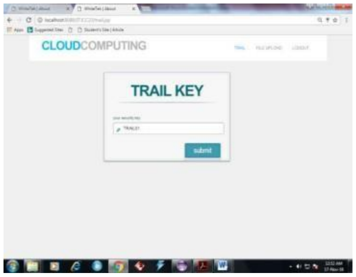


Fig 4.1 New User Registration Page

KEY ACCESS:

In this module, once registration process completed the user can login to the server, the server sent the dynamic Trial/secret key [14] for uploading the file. Using that key user can upload many files at a time.

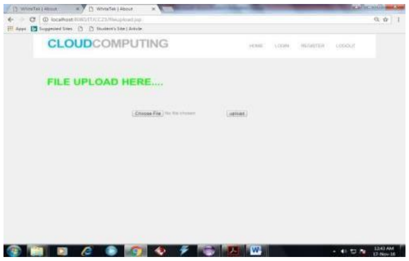
Fig 4.2 Key Generation



1.1 File Upload

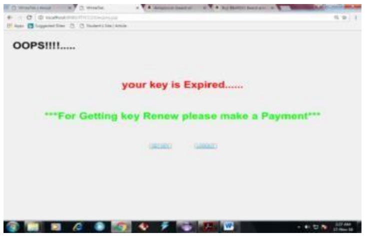
After receiving key from Data owner he/she upload a many documents with using same key.

Fig 4.3 File Upload



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

1.1 File store to cloud server

New Key generation

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 represents the authorized user uploaded documents with the details such as file name, File Type, size and modified date and Time.

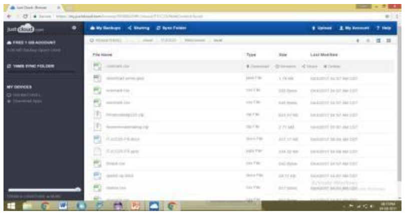


Fig 4.4 File store to cloud server

V. CONCLUSION

Revocable storage identity-based encryption (RS-IBE) and the KUNODE algorithm, which supports identity revocation and cipher text update simultaneously and prevents a revoked user from accessing previously shared data as well as later shared data, are used in this paper to implement secure data sharing in public clouds.

VI. 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]. Ravi, Chinapaga, et al. "Analysis of Concept Drift Detection–A Framework for Categorical Time Evolving Data."

[3]. Bhushan, P. Vinay, et al. "An Efficient System for Heart Risk Detection using Associative Classification and Genetic Algorithms."

[4]. Chnarsimha Chary, International Journal Of Scientific research In Computer Science, Engineering And Information Technology, "Duo Mining Techniques In Knowledge Discovery Process In Data Base", 2018/06, Volume 3, Issue 1.

[5].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

[6]. BHUSHAN, P. V., NITESH, V., CHARY, C. N., & GUPTA, K. G. Novel Approach for Multi Cancers Prediction system using Various Data Mining Techniques.

[7]. GUPTA, K. GURNADHA, CH NARASIMHA CHARY, and A. KRISHNA. "STUDY ON HEALTH CARE LIFE LOG BY THE LEVEL OF CARE REQUIRED USING KEYGRAPH TECHNOLOGY IN TEXT DATA MINING."

[8].chnarasimha chary, INTERNATIONAL JOURNAL OF RESEARCH,, "CLASSIFICATION OF MACHINE LEARNING TECHNIQUES AND APPLICATIONS IN ARTIFICIAL INTELLIGENCE", 2019/02,Volume 1, Issue 1.

[9].NarasimhacharyCholleti, "ANALYZING SECURITY OF BIOMEDICAL DATA IN CANCER DISEASE", Journal of Critical Reviews,2020/5, Volume 7, Issue 7, Pages 150-156

[10].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.

[11].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.

[12]. CHOLLETI, NARASIMHACHARY, and TRYAMBAK HIRWARKAR."BIOMEDICAL DATA ANALYSIS IN PREDICTING AND IDENTIFICATION CANCER DISEASE USING DUO-MINING." Advances in Mathematics: Scientific Journal 9 (2020): 3487-3495

[13].chnarasimha chary,JOURNAL OF CRITICAL REVIEW,"ANALYZING SECURITY OF BIOMEDICAL DATA IN CANCER DISEASE",Volume 9, Issue 1

[14]. CHOLLETI, NARASIMHACHARY, And TRYAMBAK HIRWARKAR. "BIOMEDICAL DATA ANALYSIS IN PREDICTING AND IDENTIFICATION CANCER DISEASE USING DUO-MINING." Advances in Mathematics: Scientific Journal 9 (2020): 3487-3495

4.4