International Journal of Current Engineering and Technology
©2021 **INPRESSCO**®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Detectable group sharing with fine grained access control in cloud computing

Miss.Rupali Yadav and Prof.H.A.Hingoliwala

Department of Computer Engineering JSPM's Jayawantrao Sawant College of Engineering,Pune Savitribai Phule Pune University Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

In Cloud Computing Data Sharing empowers various members to uninhibitedly share the distinctive gathering information, which generally enhance the proficient of work. The most effective method to guarantee the security of information sharing inside gathering and redistributed information in gathering way are formable difficulties. The Key conventions have assumed a critical job in secure and productive gathering in distributed computing. To take care of this issue, we propose Symmetric adjusted fragmented square structure (SBIBD) are utilized for key Security. SBIBD is utilized the general recipe for creating the basic meetings key K for numerous Participants. General equation (v, k+1, 1) square plan is utilized to information are put away. As Result of putting away information from dynamic gathering and Data are separated Blocks and System Performances are a superior when contrasted with Exiting Scheme with help of best calculations is Blows fish and DES.

Keywords: *Cloud storage, outsourcing computing, cloud storage auditing, key update, verifiability.*

Introduction

In Cloud Computing Data Sharing empowers various members to unreservedly share the diverse gathering information, which broadly enhance the proficient of work in helpful. Instructions to guarantee the security of information sharing inside gathering and redistributed information in gathering way are formable difficulties. The Key conventions have assumed an essential job in secure and effective gathering in distributed computing.

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interest of most researchers because a lot services are provided by the cloud service providers which helps to reduce costs needed for various resources[3][1]. Cloud storage is one of the most vital service in cloud computing. Scalability is another attracting factor which allows user to scale up and scale down the resources as required. Cloud computing also provides convenient and flexible ways for data sharing. There are two ways to share data in cloud storage. The first case refers to the scenario where one client authorizes access to his/her data for many clients known as one-to-many pattern and the second case refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time known as many-to-many pattern[1]. As the data shared on the cloud is valuable, various security methods are provided by cloud. In current cloud applications various algorithms are used for data encryption and decryption. In encryption is based on ABE [Attribute Based Encryption [1]. Symmetric-key cryptography is used in to enable efficient encryption. Practical group key management algorithm based on a proxy re-encryption technology [7].

A. Motivation

1) Health Play very important role in every persons life and there is need of Security of heath records so here proposed System used the Methods of privacy and Access Control.
2) Our System Used specific and sensitive attributes value in access policies.
3) The sensitive information can be protected other information can be shared.
4) Easy to used and Easily get Report from Application.

Review of literature

1) Smart Health: A Context-Aware Health Paradigm within Smart Cities "The new period of versatile wellbeing introduced by the wide selection of pervasive processing and portable interchanges has conveyed open doors for governments and organizations to reexamine their idea of human services. All the while, the overall urbanization process

speaks to a considerable test and draws in consideration toward urban areas that are required to assemble higher populaces and furnish subjects with administrations in a productive and human way. These two patterns have prompted the presence of portable wellbeing and brilliant urban areas. In this article we present the new idea of shrewd wellbeing, which is the setting mindful supplement of versatile wellbeing inside brilliant urban communities. We give a diagram of the fundamental fields of learning that are engaged with the way toward building this new idea. Furthermore, we examine the fundamental difficulties and openings that s-Health would suggest and give a shared view to additionally look into.

- Advantage: - Improving Policy Decisions and Cost Saving.
- Disadvantage: - Online Predication sometime failure.

2) "Cloud Quall: A Quality Model for Cloud Services":Distributed computing is a critical part of the foundation of the Internet of Things (IoT). Mists will be required to help extensive quantities of cooperations with shifting quality necessities. Administration quality will consequently be a critical differentiator among cloud suppliers. So as to separate themselves from their rivals, cloud suppliers should offer unrivaled administrations that live up to clients' desires. A quality model can be utilized to speak to, measure, and look at the nature of the suppliers, with the end goal that a shared comprehension can be built up among cloud partners. In this paper, we take an administration point of view and start a quality model named CLOUDQUAL for cloud administrations. It is a model with quality measurements and measurements that objectives general cloud administrations. CLOUDQUAL contains six quality measurements, i.e., ease of use, accessibility, unwavering quality, responsiveness, security, and flexibility, of which ease of use is emotional, while the others are objective. To exhibit the viability of CLOUDQUAL, we lead exact contextual analyses on three stockpiling mists. Results demonstrate that CLOUDQUAL can assess their quality. To exhibit its soundness, we approve CLOUDQUAL with standard criteria and demonstrate that it can separate administration quality.

3)

- Advantage: - A quality model for cloud services, called CLOUDQUAL, which specifies six quality dimensions and five qualities metric and Security..
- Disadvantage: - offer an infinite amount of storage space.

4) Attribute-based encryption for fine-grained access control of encrypted data" As progressively delicate information is shared and put away by outsider destinations on the Internet, there will be a need to scramble information put away at these locales. One disadvantage of scrambling information is that it very well may be specifically shared just at a coarse-grained level (i.e., giving another gathering your private key). We build up another cryptosystem for fine-grained sharing of scrambled information that we call Key-Policy AttributeBased Encryption (KP-ABE). In our cryptosystem, figure writings are marked with sets of traits and private keys are related with access structures that control which figure messages a client can unscramble. We show the materialness of our development to sharing of review log data and communicate encryption. Our development bolsters assignment of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

- Advantage: -Key-Policy Attribute-Based Encryption (KP-ABE) and Hierarchical Identity-Based Encryption (HIBE).
- Disadvantage: - coarse-grained level encryption and generated the private key but private key is not secure

5) Fuzzy Identity-Based Encryption: - We present another kind of Identity-Based Encryption (IBE) plot that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we see a way of life as set of illustrative traits. A Fuzzy IBE plot takes into consideration a private key for a character, , to unscramble a figure content scrambled with a personality, 0, if and just if the characters and 0 are near one another as estimated by the "set cover" remove metric. A Fuzzy IBE plan can be connected to empower encryption utilizing biometric contributions as characters; the mistake resistance property of a Fuzzy IBE plot is correctly what takes into consideration the utilization of biometric personalities, which innately will have some clamor each time they are tested. Furthermore, we demonstrate that Fuzzy-IBE can be utilized for a kind of utilization that we term "property based encryption".

- Advantage: -Attributed – based encryption (ABE) and Fuzzy Identity-Based Encryption
- Disadvantage: - error tolerance property is used for fault tolerance Scheme

6) "Security challenges for the public cloud"Distributed computing is the most up to date term for the since quite a while ago envisioned vision of registering as an utility. The cloud gives advantageous, on-request organize access to a brought together pool of configurable registering assets that can be quickly conveyed with extraordinary proficiency.

- Advantage: -Public Cloud is used when the data are stored in greater efficiency. Fully Holomorphic encryption(FHE
- Disadvantage: - No trustworthy public cloud environment to become a reality

7) "Provable Data Possession at Untrusted Store"We present a model for provable information ownership (PDP) that permits a customer that has put away information at an untrusted server to confirm that the server has the first information without recovering it. The model produces probabilistic evidences of ownership by testing arbitrary arrangements of squares from the server, which definitely decreases I/O costs. The customer keeps up a steady measure of metadata to confirm the evidence

- Advantage: -Provable data possession (PDP) is used scheme
- Disadvantage: - Original data are retrieving with access control

8) "POR S: Proofs of Irretrievability for Large files"In this paper, we characterize and investigate evidences of retrievability (PORs). A POR plot empowers a file or back-up administration (prover) to deliver a compact confirmation that a client (verifier) can recover an objective document F, that will be, that the file holds and dependably transmits record information adequate for the client to recuperate F completely.

- Advantage: -Existing cryptographic techniques help users ensure the privacy and integrity of files they retrieve. users to want to verify that archives do not delete or modify files prior to retrieval
- Disadvantage: - POR can also provide quality-ofservice guarantees, i.e., show that a file is retrievable within a certain time bound

9) "Privacy Preserving Public Auditing for Secure Cloud Storage"Utilizing Cloud Storage, clients can remotely store their information and appreciate the on-request top notch applications and administrations from a mutual pool of configurable processing assets, without the weight of nearby information stockpiling and upkeep.

- Advantage: - Integrity checking is used • Disadvantage: - Only Own file access control.

10) "Compact Proofs of retrievability"In a proof-of-retrievability system, a data storage center must prove to a verifier that he is actually storing all of a client's data. The central challenge is to build systems that are both efficient and provably secure — that is, it should be possible to extract the client's data from any prover that passes a verification check. In this paper, we give the first proof-of-retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski.

- Advantage: - Proof of owner ship is used in application. Proof-of-irretrievability protocol in which the client's query and server's response are both extremely short. pseudorandom functions (PRFs)
- Disadvantage: - No Security for public verification. Efficient Holomorphic authentication is used but only one way

System Architecture/ System Overview

In Our System proposed an identity-based data integrity auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding. In our Application doctor upload the data into cloud with user and researcher when Doctor Share the data with User that file go to Admin and admin convert into Binary format and after that binary format file again convert into Homomorphic encryption and Stored into Block Level.

In System there are four roles such as the Doctor and Admin and Patient (User) and Researcher and First in System Doctor upload the Report According to their choice of User and Researcher if Doctor Select the Patient Upload the Report with patient ID after uploading Admin Convert the Data into Binary format using Specialized Algorithms. After converting into Binary part Cloud Server provider is stored the Data into Second level Encryption such as called as the content Level Encryption and Copy into Block Level. At that Cloud Server provider admin generated Private Key of File and stored . User Search the Report then Search By patient ID then admin First auditing that and given permission of Report and again admin Given Private key the user Download the Report.

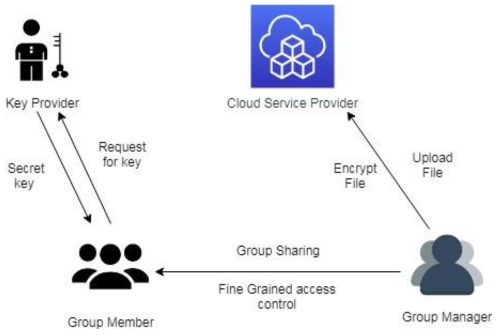


Fig. 1. Proposed System Architecture Explanation

1) User Search by two ways one by Own id and Doctor Name after user get All file which Upload by Doctor then User Select file and Request Send to Admin , the admin Accepted the request and provide the private key and User Download the Report.
2) Doctor Select two option for Uploading such as the share with User and researcher when doctor select user then doctor

A. Algorithms

1. Generation of Block B

```
1) for i=0;i¡=k;i++ do
2) for j=0;j¡=k;j++ do
3) if j==0 then
4) Bi,j=0; else
5) bi,j=ik+j;
6) end if
7) end for
8) end for
9) for i=k+1 ;i¡=k +k ;i++ do
10)     for j=0;j¡k ;j++
11)     j==0 then
12)     Bi,j=[(i-1)/k +1]
13)     Else
14)     Bi.k=jk+1 +Mod k+1(i-j+(j-1)[i-1]/k+1)
15)     End if
16)     End for
17)     End for
```

2. Re-construction of B 1) E0=B0; Steps 1

```
2) For t=1;t¡=k+1;t++ do
3) Et=Btk+1 Steps 2
4) Btk=[Flag]=1;
5) Eet,1=B[Et,t/ K] steps 2
```

```
6) Btk+1[flag]=1
7) End for
8) For i=k+1 ;i¡k+1; i++ do
9) If Bi[Flag]!=1 then
10)    Ebi[i+1/K]=Bi steps 3
11)    End if
12)    End For
```

3. AES Algorithms 1) Input:
2)128 bit /192 bit/256 bit input(0,1) 3)secret key(128 bit)+plain text(128 bit).
4) Process:
5)10/12/14-rounds for-128 bit /192 bit/256 bit input
6)Xor state block (i/p)
7)Final round:10,12,14
8)Each round consists:sub byte, shift byte, mix columns, add round key.
9)Output:
10)cipher text(128 bit)

B. Mathematical Model

X=(x1,x2,x3,x4......................xB) Here B block of data
H(x)=B log2 q bits. Let N be the number of available CSPs for the user to store data. Before storing the file, the user encodes the B blocks of data into n blocks. We use f:FB =Fn
which maps x into y, to denote the encoding function y=(y1,y2,y3,............................yn) for i=1,2,3..............................N here N is sub-vectors
let yi=(yi,1,yi,2,...........yi,ni) Fni
Be the data stored on CSP(Cloud Services provider) n= (i=1) N nI
(1) n= total number of encoded block (i=1) N nI =sum of Number of Encoded block stored in each CSp.
Let,
Vi for i N be the amount of blocks which can be downloaded from CSP i within a predefined time delay, it is required that niVi (2)
H: $\{0,1\}^* \rightarrow G_1$ ....(3) here H is A Cryptography Hash Function x is An Element in Z_i^p ....(4) u,u1,u2,u3....u_n the Element in G_1 ....(5) n is number of data block of Files F
F= $\{m,m_1,m_2.....m_n\}$
The Original File F ....(6)
$F^* =\{m_1^*,m_2^*,m_3^*.....m_n^*\}$ ....(7)
The Blinder file send to Admin
ID the user's Identity
K_1 The Set of index of Data Block corresponding to personal Admin information
K_2 The Set of index of Data Block corresponding to System Admin information psk The master Private Key
$\Phi =\{\sigma_i\}_1 \leq i \leq n$ ....(8)
Here The Signature Set of blinded file
$\Phi' =\{\sigma_i'\}_1 \leq i \leq n$ ....(9)
Here The Signature Set of Admin File

Hardware and Software Requirements

Hardware Requirements

1) Processor - Intel i5 core
2) Speed - 1.1 GHz
3) RAM - 2GB
4) Hard Disk - 40 GB
5) Key Board - Standard Windows Keyboard
6) Mouse - Two or Three Button Mouse
7) Monitor - SVGA
8) Floppy Drive - 44 Mb

Software Requirements

1) Operating System - XP, Windows7/8/10
2) Coding language - Java, MVC, JSP, HTML, CSS etc
3) Software - JDK1.7
4) Tool - Eclipse Luna
5) Server - Apache Tomcat 8.0
6) Database - MySQL 5.0

System Analysis and Result

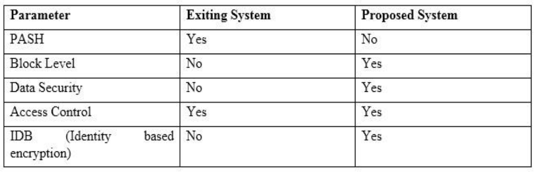
In this subsection, our System evaluate the performance of the proposed scheme by several experiments. system run these experiments on a window machine with an Intel Pentium 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the many type of encryption algorithms such as AES and RAS Algorithms and Also using Block Level Concepts . In our experiments, System first Install required Software. The Data are stored in the Block Level.In Block Level concepts the Data are stored into random block which generated by (SBIBD) Approach.

The Commutation Overhead of Proposed Schema

Entity	Role	Commutation Overhead
Admin	Auditing Challenge	$c \cdot \|n\| + \|p\|)$
Cloud	Auditing Prof and Stored Data	$\|p\| + \|q\|$

The Commutation Complexity of Different Entities in Different Phases

Entity	User	Admin	Cloud
Data Blinding	O(d_1)	—	—
Signatur generation	e O(n)	—	—
Binary Con- vector	—	O(d_1+d_2)	—
Block generation	—	—	(v,k+1, 1)
Prof generation	—	O(c)	—-



Parameter	Exiting System	Proposed System
PASH	Yes	No
Block Level	No	Yes
Data Security	No	Yes
Access Control	Yes	Yes
IDB (Identity based encryption)	No	Yes

Fig. 2. Compassion of Exiting System and Proposed System

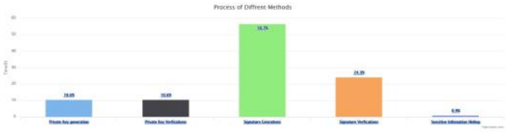


Fig. 3. Process of Different Methods

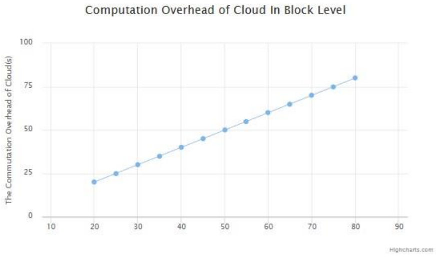


Fig. 4. Computation Overhead of Cloud Storage

Conclusion

In this paper, we proposed group sharing for secure distributed storage, which bolsters information imparting to touchy data stowing away. In our plan, the document put away in the cloud can be shared and utilized by others depending on the prerequisite that the delicate data of the record is secured. Plus, the remote information respectability examining is as yet ready to be proficiently executed. The security confirmation and the exploratory investigation exhibit that the proposed plan accomplishes attractive security and privacy.

References

[1] Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Perez-Mart´ ´ınez, R. Di Pietro, D. N. Perrea et al., “Smart health: a context-aware health paradigm within smart cities,” IEEE Communications Magazine, vol. 52, no. 8, pp. 74-81, 2014.

[2] Y. Yuehong, Y. Zeng, X. Chen, and Y. Fan, “The internet of things in healthcare: An overview,” Journal of Industrial Information Integration, vol. 1, pp. 3-13, 2016.

[3] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 22332243, 2014

[4] X. Zheng, P. Martin, K. Brohman, and L. Da Xu, “Cloudqual: a quality model for cloud services,” IEEE transactions on industrial informatics, vol. 10, no. 2, pp. 1527-1536, 2014.

[5] J. Katz, A. Sahai, and B. Waters, “Predicate encryption supporting disjunctions, polynomial equations, and inner products,” in Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT’08), 2008, pp. 146-162.

[6] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan. 2012.

[7] G. Ateniese et al., “Provable data possession at untrusted stores,” in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[8] A. Juels and B. S. Kaliski, Jr., “Pors: Proofs of retrievability for large files,” in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[9] H. Shacham and B. Waters, “Compact proofs of retrievability,” J. Cryptol., vol. 26, no. 3, pp. 442–483, Jul. 2013.v

[10] K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, “Privacy-preserving attribute- based access control model for XML-based electronic health record system,” IEEE Access, vol. 6, pp. 9114-9128, 2018.

[11] H. Hu, G. Ahn, and J. Jorgensen, “Multiparty access control for online social networks: Model and mechanisms,” IEEE Trans. on Knowledge and Data Engine, vol. 25, no. 7, pp. 1614-1627, 2013.

[12] Q. Huang, Y. Yang, and M. Shen, “Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing,” Future Generation Computer Systems, vol. 72, pp. 239-249, 2017.

[13] J. Hur, “Improving security and efficiency in attribute-based data sharing,” IEEE Trans. on Knowledge and Data Eng., vol. 25, no. 10, pp. 2271-2282, 2013.

[14] K. Yang and X. Jia, “Expressive, efficient, and revocable data access control for multi-authority cloud storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1735-1744, 2014.

[15] S. Jiang, T. Jiang, and L. Wang, “Secure and efficient cloud data deduplication with ownership management,”, IEEE Transactions on Services Computing, https://ieeexplore.ieee.org/document/8100969

[16] B. Lynn. The pairing-based cryptography library. [Online]. Available:

[17] http://crypto.stanford.edu/pbc/, accessed March 1, 2018.