IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

Survey on Data Security Mechanism by Distributed Data over Cloud Using Client-Server Architecture

Prof.Kanchan Sonawane[1], MOHD Shahid Saifi[2] ,Vipul Gautame[3], Guruprasad Dastane[4]

Professor, Computer Dept., RMD, Pune, India [1]
Student, Computer Dept., RMD, Pune, India [2, 3, 4]

Abstract: Data sharing is an critical functionality in cloud storage. In this article, we display a way to securely, efficiently, and flexibly share information with others in cloud storage. Deduplication may be a storage saving technique that has been adopted by several cloud storage suppliers likeDropbox. In cloud storage services, deduplication technology is commonly accustomed cut back the world and data live necessities of services by eliminating redundant knowledge and storing entirely one copy of them. Deduplication is best once multiple users supply an identical data to the cloud storage, but it raises issuesconcerning security and possession. Issues over information security still forestall several users from migratinginformation to remote storage. The standard resolution is to write in code the info before it leaves the owner's premises.Client-side information deduplication specifically ensures that multiple transfers of constant content solely consume network information measure and space for storing of one upload. We'll use server facetinformation deduplicationWe additionally describe other utility of our schemes. In precise, our schemes provide the first public-key encryptionhierarchy, which turned into but to be acknowledged.

Keywords: Searchable encryption, data sharing, cloud storage, data privacy.

I. INTRODUCTION

Cloud storage has emerged as a promising solutionfor imparting ubiquitous, handy, and on-call for accesses to massive amounts of facts shared over theInternet. Today, hundreds of customers are sharing personalinformation, along with pix and films, with their buddiesthrough social community packages based totally on cloud storage on a every day foundation. We exhibit the execution of encryption and decryption algorithms about data privacy, computational efficiency and effectiveness of the cloud storage system. We demonstrate novel approach of three level encryption on huge data stored on cloud. Business users are being attracted by way of cloud storage due to its numerous benefits,including decrease price, more agility, and higherresource utilization. Although combining a searchable encryption scheme with cryptographic cloud storage can achieve the fundamental security requirements of a cloud storage, imposing the sort of device for massive scale applications involving thousands of customers and billions of files may also nevertheless be hindered by means of practical problems involving the efficient management of encryption keys, which, to the great of our know-how, are in large part omitted inside the literature. First of all, the need for selectively sharing encrypted facts with one-of-a-kind customers (e.g., sharing a photo with sure pals in a social community utility, or sharing enterprisereport with sure colleagues on a cloud power) generally demands exclusive encryption keys to be used for distinctive files. However, this means the range of keys that need to be dispensed to users, both for them to go looking over the encrypted documents and to decrypt the documents, could be proportional to the quantity of such documents. Such a big number of keys.

Motivation of project

Large amount of data is stored on the cloud. To secure this information, efficient cryptographic technique is required. Our aim is to provide more advanced cryptographic technique for secure data transmission.

II. LITERATURE SURVEY

- Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing.

Cloud computing is develop computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As to assure as it is, this paradigm also brings forth many new challenges for data security

DOI 10.17148/IJARCCE.2018.7537

and access control when users outsource annoyed data for sharing on cloud servers, which are not within the same trusted influence, as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by to cause to appear data decryption keys only to authorized users. The problem of simultaneously accomplish fine grained access, scalability, and data confidentiality of access control actually still remains not resolved.

- Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing.

Success of data forensics in cloud computing is based on secure place that records ownership and process history of data objects. But it is the still challenging issue in this paper. In this paper, they proposed a new secure provenance scheme based on the bilinear pairing techniques .As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud. Secure authentication on user access, and place tracking on disputed documents is provided in this paper. With the provable security techniques, this paper formally demonstrates the proposed scheme is secure in the standard model.

- Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud.

In this paper character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Due to the frequent change of membership sharing data in multi-owner manner while preserving data and identify privacy from untrusted cloud is still a challenging issue.

III. EXPERIMENTAL SETUP

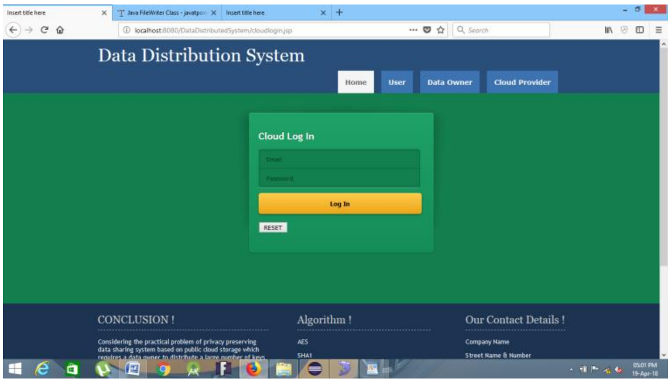
We have design three modules

1. User
2. Data owner
3. Cloud

User will fill all details in registration section. After registration, user will get login credentials. User will enter email-id and password for login to application. Similarly, data owner will fill all details in registration section. After registration, data owner will get login credentials. Data owner will enter email-id and password for login to application. User can request for file to data owner. Data owner can view request of users for various file. File will stored in encrypted format on cloud. User will get key to decrypt file on his/her email account. Data owner will verify user and send key and file to user. Redundancy is avoided in application. If data is repeated , it is eliminated.

IV. RESULT AND DISCUSSION

Login of user , data owner and cloud is provided. Email-id and password is provided to login to application as shown in figure.



localhost:8080/DataDistributedSystem/cloudlogin.jsp

Data Distribution System

Cloud Log In

CONCLUSION !

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys

Algorithm !

AES

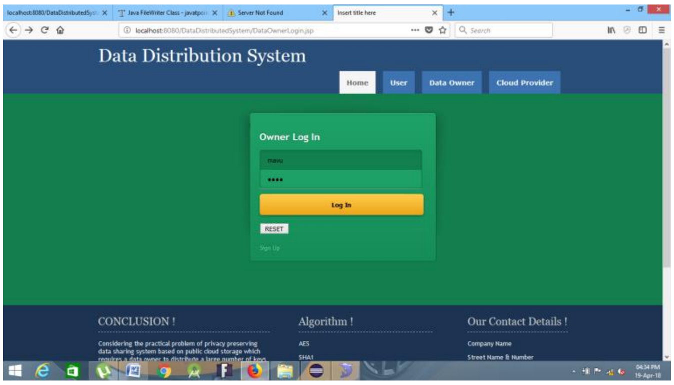
SHA1

Our Contact Details !

Company Name

Street Name & Number

Fig 1(a)


localhost:8080/DataDistributedSys
Java FileWriter Class - javatpoi
Server Not Found
Insert title here
localhost:8080/DataDistributedSystem/DataOwnerLogin.jsp
Search
Home
User
Data Owner
Cloud Provider
Log In
RESET
Sign Up
04:34 PM
19-Apr-18

Data Distribution System

Owner Log In

mavu

••••

CONCLUSION !

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys

Algorithm !

AES

SHA1

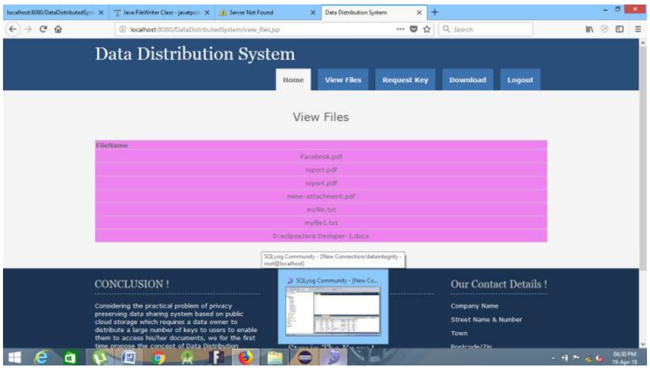
Our Contact Details !

Company Name

Street Name & Number

Fig 1(b)

User will request for required file to data owner. User can request for key of file which is in encrypted form. User will get key on his/her email account. User can download key and using key user is able to decrypt file as shown in fig 2(a) and (b).


localhost:8080/DataDistributedSys
Java FileWriter Class - javatpoi
Server Not Found
Data Distribution System
localhost:8080/DataDistributedSystem/view_files.jsp
Search
Home
View Files
Request Key
Download
Logout
SQLyog Community - [New Connection/dataintegrity - root@localhost]
SQLyog Community - [New Co...
04:30 PM
19-Apr-18

Data Distribution System

View Files

FileName
Facebook.pdf
report.pdf
report.pdf
mime-attachment.pdf
myfile.txt
myfile1.txt
D:eclipseJava Devloper-1.docx

CONCLUSION !

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of Data Distribution

Our Contact Details !

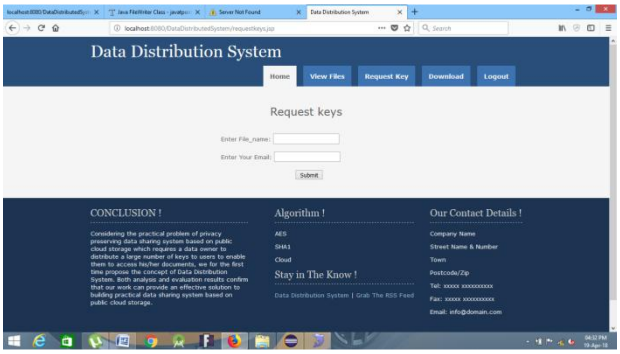
Company Name

Street Name & Number

Town

Postcode/Zip

Fig 2(a)


localhost:8080/DataDistributedSys
Java FileWriter Class - javatpoi
Server Not Found
Data Distribution System
localhost:8080/DataDistributedSystem/requestkeys.jsp
Search
Home
View Files
Request Key
Download
Logout
Submit
04:32 PM
19-Apr-18

Data Distribution System

Request keys

Enter File_name:

Enter Your Email:

CONCLUSION !

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of Data Distribution System. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage.

Algorithm !

AES

SHA1

Cloud

Stay in The Know !

Data Distribution System | Grab The RSS Feed

Our Contact Details !

Company Name

Street Name & Number

Town

Postcode/Zip

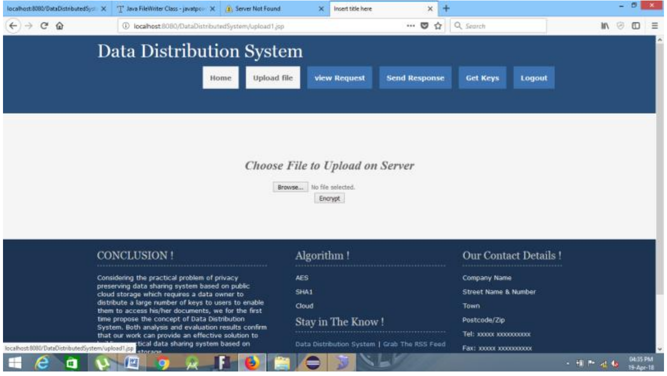
Tel: xxxxx xxxxxxxxxx

Fax: xxxxx xxxxxxxxxx

Email: info@domain.com

Fig 2(b)

File will uploaded by data owner and key with file is sent to user. It is shown in fig 3


localhost:8080/DataDistributedSys
Java FileWriter Class - javatpoi
Server Not Found
Insert title here
localhost:8080/DataDistributedSystem/upload1.jsp
Search
Home
Upload file
view Request
Send Response
Get Keys
Logout
Browse...
Encrypt
localhost:8080/DataDistributedSystem/upload1.jsp
04:35 PM
19-Apr-18

Data Distribution System

Choose File to Upload on Server

No file selected.

CONCLUSION !

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of Data Distribution System. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage.

Algorithm !

AES

SHA1

Cloud

Stay in The Know !

Data Distribution System | Grab The RSS Feed

Our Contact Details !

Company Name

Street Name & Number

Town

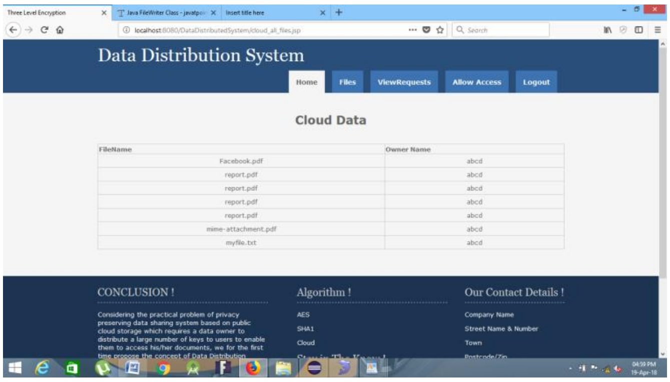
Postcode/Zip

Tel: xxxxx xxxxxxxxxx

Fax: xxxxx xxxxxxxxxx

Fig. 3

Cloud can view request and send data to data owner as shown in fig. 4(a) and (b).



Data Distribution System

Cloud Data

FileName	Owner Name
Facebook.pdf	abcd
report.pdf	abcd
report.pdf	abcd
report.pdf	abcd
report.pdf	abcd
mime-attachment.pdf	abcd
myfile.txt	abcd

CONCLUSION !

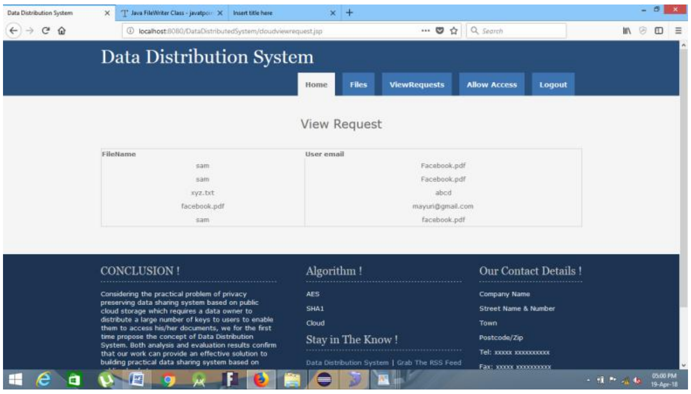
Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of Data Distribution

Algorithm !

AES
SHA1
Cloud

Our Contact Details !

Company Name
Street Name & Number
Town
Postcode/Zip



Data Distribution System

View Request

FileName	User email
sam	Facebook.pdf
sam	Facebook.pdf
xyz.txt	abcd
facebook.pdf	mayuri@gmail.com
sam	facebook.pdf

CONCLUSION !

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of Data Distribution System. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on

Algorithm !

AES
SHA1
Cloud

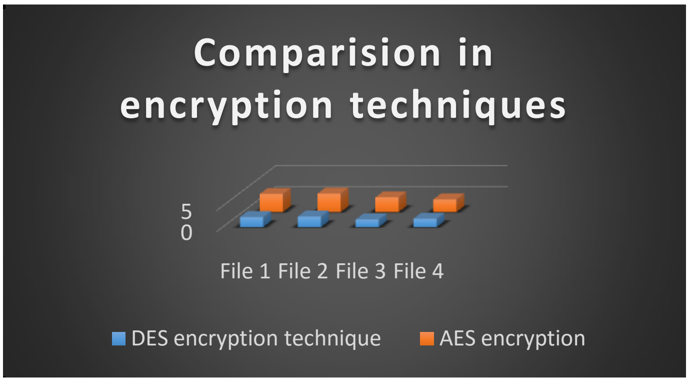
Stay in The Know !

Data Distribution System | Grab The RSS Feed

Our Contact Details !

Company Name
Street Name & Number
Town
Postcode/Zip
Tel: xxxxx xxxxxxxxxx
Fax: xxxxx xxxxxxxxxx

Comparison is given between AES and DES algorithm. It is found that AES is more secure than DES algorithm.



V. CONCLUSION

Overseeing encrypted information with deduplication is essential and noteworthy practically speaking for accomplishing an effective distributed storage benefit, particularly for huge information stockpiling. In this paper, One of the component is, information is in encrypted shape so protection of client is kept up. we proposed a reasonable plan to deal with the encrypted huge information in cloud with deduplication in view of possession test and PRE. Our plan can adaptably bolster information refresh and offering to deduplication notwithstanding when the information holders are disconnected. Encrypted information can be safely gotten to on the grounds that lone approved information holders can get the symmetric keys utilized for information unscrambling. Broad execution investigation and test demonstrated that our plan is secure and proficient under the portrayed security show and extremely reasonable for enormous information deduplication

REFERENCES

[1] [1] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing”, Proc. IEEE INFOCOM, pp. 534-542, 2010.

[2] [2] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing”, Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

DOI 10.17148/IJARCCE.2018.7537

[3] [3] X. Liu, Y. Zhang, B. Wang, and J. Yan. “Mona: secure multiowner data sharing for dynamic groups in the cloud”, IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.

[4] [4] C. Chu, S. Chow,W. Tzeng, et al. “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[5] [5] X. Song, D.Wagner, A. Perrig. “Practical techniques for searches on encrypted data”, IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[6] [6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. “Searchable symmetric encryption: improved definitions and efficient constructions”, In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[7] [7] P. Van,S. Sedghi, JM. Doumen. “Computationally efficient searchable symmetric encryption”, Secure Data Management, pp. 87-100, 2010.