ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 4, April 2016

CRYPTOGRAPHY USING R.S.A. ALGORITHM AND DATA ACCOUNTABLITY FOR DATA SHRING ON CLOUD

Authores: Deepika Patil, Arshi Akab, Swagnik Das, Ashish Modak

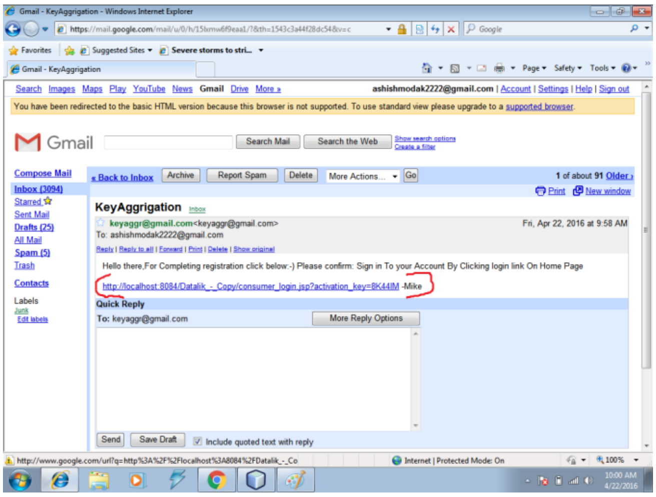
Abstract— Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and softwaremanagement. Though the benefits are clear, such a service is also relinquishing users physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also that can cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure,malicious data modification attack, and evenserver colluding attacks

***Index Terms*— key aggregate cryptography,encryption,decryption,cloud**

INTRODUCTION

Cloud network is a space where data is stored on remote location rather than local storage. Cloud owner allows to data owner to store data on his cloud..then user can access and share the data from any corner of world. To provide security and authentication while sharing data on cloud is very essential. Existing system was unable to provide multiple security and authentication level while sharing data on cloud.The process of encryption of data on cloud was entrusted because data and encryption key was held by the cloud server. Previous systems was so costly because encryption was done at server side. That drawbacks are overcome in proposed system.

A proposed system is provide multilevel authentication And security to data on cloud. It can happen in such way that data owner and cloud owner first register to cloud. Then system sends login link to owner or user in his email.data owner or user follows that link to log in to cloud. After login to cloud they can access the cloud services.



You have been redirected to the basic HTML version because this browser is not supported. To use standard view please upgrade to a supported browser.

KeyAggrigation

keyaggr@gmail.com<keyaggr@gmail.com> Fri, Apr 22, 2016 at 9:58 AM
To: ashishmodak2222@gmail.com

Hello there,For Completing registration click below:-) Please confirm: Sign in To your Account By Clicking login link On Home Page

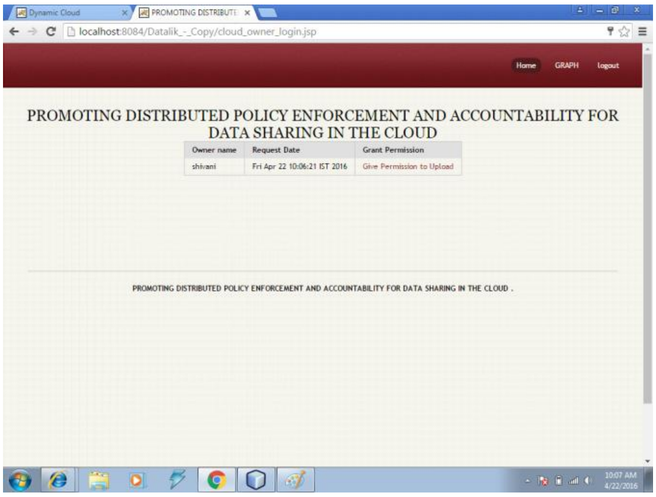
http://localhost:8084/Datalik_-_Copy/consumer_login.jsp?activation_key=8K44IM -Mike

To: keyaggr@gmail.com

http://www.google.com/url?q=http%3A%2F%2Flocalhost%3A8084%2FDatalik_-_Co

From data owner side when he log in to cloud first side then he send request to cloud owner get upload file. Cloud owner gives a rights to data owner to upload file. Every time file encryption is necessary before upload to cloud. This operation is done at client side. So this operation is trusted and has low cost.

In existing system encryption was done at server side so that cloud subscriber needed to pay more charges. Data and encryption keys was held by server so that system was entrusted.



Dynamic Cloud | PROMOTING DISTRIBUTE

localhost:8084/Datalik_-_Copy/cloud_owner_login.jsp

Home GRAPH logout

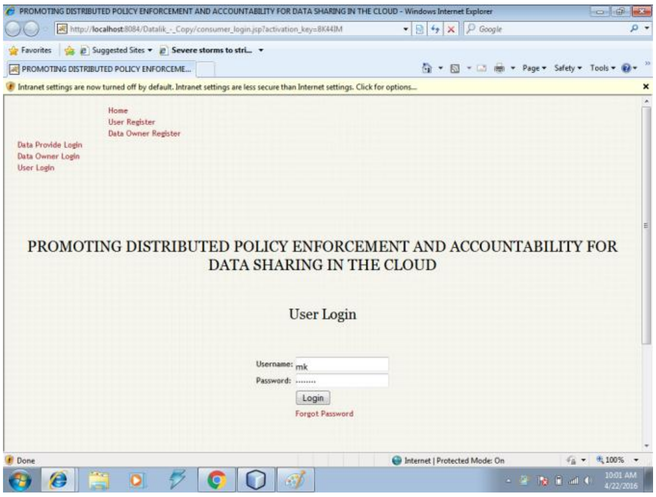
PROMOTING DISTRIBUTED POLICY ENFORCEMENT AND ACCOUNTABILITY FOR DATA SHARING IN THE CLOUD

Owner name	Request Date	Grant Permission
shivani	Fri Apr 22 10:06:21 IST 2016	Give Permission to Upload

PROMOTING DISTRIBUTED POLICY ENFORCEMENT AND ACCOUNTABILITY FOR DATA SHARING IN THE CLOUD .

10:07 AM 4/22/2016

Now proposed system at user side cloud user login to cloud by following the link which is on his email. So user needs to login to email and then login to cloud. After two way login user can access cloud.



PROMOTING DISTRIBUTED POLICY ENFORCEMENT AND ACCOUNTABILITY FOR DATA SHARING IN THE CLOUD - Windows Internet Explorer

http://localhost:8084/Datalik_-_Copy/consumer_login.jsp?activation_key=8K44IM

Intranet settings are now turned off by default. Intranet settings are less secure than Internet settings. Click for options...

Home
User Register
Data Owner Register

Data Provide Login
Data Owner Login
User Login

PROMOTING DISTRIBUTED POLICY ENFORCEMENT AND ACCOUNTABILITY FOR DATA SHARING IN THE CLOUD

User Login

Username: mk
Password: ....
Login
Forgot Password

Done
Internet | Protected Mode: On
100%
10:01 AM 4/22/2016

MATH

Now see how to generate aggregate key for file encryption,by taking a example.

Suppose we have multiple files then select file which we want to upload .suppose files are f1,f2,f3,generate random key of respective file. suppose that are k1,k2,k3 Let,k1=123,k2=456,k3=789 .combine the keys and add separator(ie.0)between them .Take one Quadratic equation,

$F(x)=n1x+n2x^2 +s$

Let,n1=19,n2=6,x=3(as sending files are 3)

$.F(x)=(19*3)+6*(3^2)+s$

$F(x)=57+54+s$

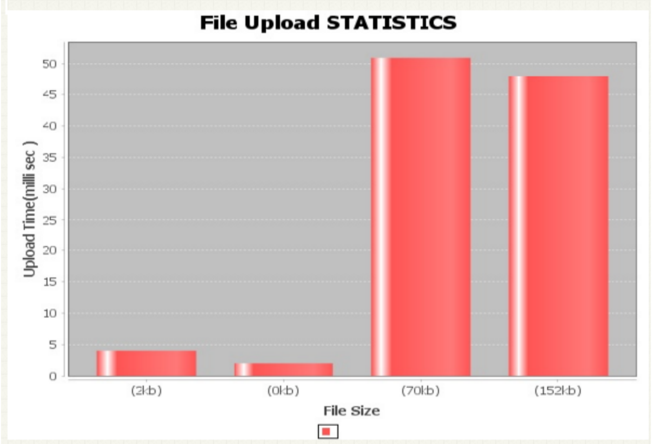
$F(x)=111+s$

$.f(x)=111+12304560789$

$=1.230456e^{10}$

$.1.230456e^{10}$ this is aggregate key used to encrypt file before upload to cloud.

The process of encryption of file and upload file to cloud is depends upon file size. Following graph shows scenario.



A. *References*

1. An Efficient Remote Data Possession Checking in Cloud Storage

Advantages:

An efficient remote data possession checking (RDPC) scheme is proposed.It almost satisfies all the requirements for cloud storage. First, it is efficient interms of computation and communication. Second, it allows verification without the need for the challenger to compare against the original data, and it can be verified by comparing only the responds returned by the storage server. Users need to store only two secret keys and several random numbers. Finally, based on Eulers theorem, a challenge updating method is proposed. The efficiency of the scheme makes it ideally suited for use in cloud storage.

Disadvantages:

The paper doesnt consider data updating which will be the future works. In addition, we will apply the scheme to a practical system.

2. Private Editing Using Untrusted Cloud Services

Advantages:

The contents of the file are protected (both confidentiality and optionally integrity) even against attacks from a possibly malicious cloud service provider. The extension has minimal impact on the existing functionality of the cloud application and requires no cooperation from the application provider. The incurred runtime and bandwidth costs are acceptable for typical uses. We achieve this by using a new data structure that supports variable-length blocks in an incremental encryption scheme.

Disadvantages:

It is a light-weight component.The techniques cannot provide the highest level of privacy,especially against a malicious adversary with control over the client application.

3. Privacy-Preserving PublicAuditing for Data Storage Security in Cloud
Advantages:
We utilize the homomorphic authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient
auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users fear of their outsourced data leakage.

Disadvantages:
Batch auditing: There are K users having K files on the same cloud They have the same TPA. Then, the TPA can combine their queries and save in computation time. Data dynamics: The data on the cloud may change according to applications.

B. Abbreviations and Acronyms

List of Abbreviations:
KAC-Key Aggregate Cryptosystem
IBE-Identity based Encryption
ABE-Attribute Based Encryption
CS-Cloud Server CSP-Cloud Service Provider

[1] MySQL – My Structured Query Language:
A database management system (DBMS) that runs as a server providing multi-user access to number of databases. It is consider the world's most popular open sources database.
[2] Database platform – DB2:
DB2 Database is the database management system that delivers a flexible and cost effective database platform to build robust on demand business applications and supports the J2EE and web services standards.
[3] Java:
Java is a computer programming language that is concurrent, class-based, object- oriented, and specifically designed to have as few implementation dependencies as possible. Using JDBC-ODBC connection we can connect database with the java program and can manipulate database through it.

Document Conventions:
The proposed approach uses the public key cryptosystems where M is the message or the plain text which is to be encrypted. The system can be divided into 3 parts (K,E,D):
A pair of public and private key (lk,pk) is generated.
A ciphertext or encrypted message c=Elk(m,r) is obtained where m € M and r is a randomvalue.
Decryption Dpk(c)=m is used to obtain plain text again.

C.Equations

RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman who first publicly described the algorithm in 1977, based on the difficulty of factoring large integers. This public-key cryptography algorithm defines $n = pq$, where p and q are primes, a private key d, and a public key e such that

$$de \equiv 1(mod\ \phi(n))$$

$$(e, \phi(n)) = 1$$

Where , $\phi(n) = (p-1)(q-1)$ represents a secret that is not disclosed to the public. Similarly, the private key is not publicized but rather must be calculated using the
congruence relation stated in (1). Only the public key is easily accessible by everyone. Suppose the message sent using the RSA algorithm is denoted *M*. To encode this message, *M*, the sender chooses a value *n* = pq and a public key *e* and sends message *E*:

$$E \equiv M^e(mod\ n)$$

Then to decode, the receiver (who is the only one to know *d*)
computes

$$E^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{N\phi(n)+1} \equiv M(mod\ n)$$

Using the RSA algorithm, the identity of the sender can be determined as legitimate without revealing his or her private code.

Example using RSA

Suppose Bob would like to send Alice a message, M = 65 using the RSA algorithm.
As a result, Bob provides Alice with *n* = pq = 61 * 53 = 3233.

Therefore:

$$\Phi(n) = (p-1)(q-1)$$

$$\varphi(3233) = (61-1)(53-1) = 3120.$$

Suppose Bob provides the public key of e = 17 since it can be any number 1 < e <3120 that is coprime to 3120. So, Bob must first encode his message M = 61 by using equation (2).

$$E \equiv 65^{17}(mod\ 3233) \equiv 2790$$

Then, after calculating d, the modular multiplicative inverse of e (mod (p-1)(q-1)), it is found that d = 2753. Finally, to decrypt the message, we calculate:

$$E^d \equiv 2790^{2753}(mod3233) \equiv 65$$

II. CONCLUSION

This application is useful in cloud computing to scalable system using different cryptographic algorithm. How to defend users‟ data privacy is a central problem of cloud storage. With more mathematical concept, cryptographic schemes are getting more multipurpose and often involve multiple keys for a single system. In this System we consider how to "compact" secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. Our approach is more flexible than hierarchical key assignment which can only save storage spaces if all key-holders share a similar set of privileges. A limitation in our work is the predefined bound of the number of maximum cipher text classes. In cloud storage, the number of cipher texts usually grows rapidly. So we have to reserve enough cipher text classes for the future extension..

ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on ‘’.CRYPTOGRAPHY AND DATA ACCOUNTABLITY FOR SECURE DATA SHARING ON CLOUD". I would like to take this opportunity to thank my internal guide **Prof.U.A.Bodke** for giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful.I am also grateful to **Prof. D.C.Mehtre** Head of Computer Engineering Department, In K.J.College of engineering for his indispensable support, suggestions.In the end our special thanks to **Prof.Parth Sagar** for providing various resources such as laboratory with all needed software platforms, continuous Internet connection,for Our Project.

REFERENCES

1.S. S. M. CHOW, Y. J. HE, L. C. K. HUI, AND S.-M. YIU, ―SPICE - SIMPLE PRIVACY-PRESERVING IDENTITY-MANAGEMENT FOR CLOUD ENVIRONMENT,‖ IN APPLIED CRYPTOGRAPHY
2. . HARDESTY, ―SECURE COMPUTERS AREN'T SO SECURE,‖ MIT PRESS,2009,HTTP://WWW.PHYSORG.COM/NEWS176107396.HTML.3.C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ―Privacy- Preserving Public Auditing for Secure Cloud Storage,‖ 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 DATA ON THE CLOUD VIA SECURITY-MEDIATOR,‖ IN INTERNATIONAL CONFERENCEON DISTRIBUTED COMPUTING SYSTEMS - ICDCS 2013. IEEE, 2013.

Deepika Patil, *Computer Engineering, Savatribai Phule University, Pune / K.J.College of engineering/ Pune, India,, Mobile No:8482854995*
Arshi Akab *Computer Engineering, Savatribai Phule University, Pune / K.J.College of engineering/ Pune, India,, Mobile No:9764997867*
Swagnik Das, *Computer Engineering, Savatribai Phule University, Pune / K.J.College of engineering/ Pune, India,, Mobile No:8237523483*
Ashish Modak, *Computer Engineering, Savatribai Phule University, Pune / K.J.College of engineering/ Pune, India,, Mobile No:9763294780*