ISSN 2395-1621

Privacy-Preserving of Data and Public Auditing for Data Storage security in Cloud Computing

[#1]Shreya Thite, [#2]Monali Yenpure, [#3]Surabhi Mohite, [#4]Prof. Tejshree Borbande

[1]thiteshreya@gmail.com
[2]monali.yenpure@gmail.com
[3]surabhimohite20@gmail.com
[4]tejshreeborbande@gmail.com

[#123]Student, Computer Engineering,

NESGOI, Naigaon, Pune, India - 412213.

ABSTRACT

The cloud storage has lot of problems about security and data integrity. So we need to prevent the all problems. Cloud storage users can remotely store their data into the cloud, so as to enjoy the on-demand high quality application and services from shared pool of configurable computing resources without burden of local data storage and maintenance. Users are not able to check this data again and again from the cloud storage it is secure or not. In view of the large size of outsourced data makes integrity protection in cloud computing which is very challenging and potential formidable task. To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. thus by enabling public auditability user can resort to a third party auditor(TPA) to check the integrity of the outsourced data. In this paper, we propose a public auditing scheme for the regenerating-code-based-cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, we introduce a design a novel public verifiable authenticator, which is priviledged to regenerate the authenticators into the Traditional public auditing system mode.

Keyword: Data storage, Privacy-preserving, Public auditability, Cloud computing, authenticator regeneration, Proxy.

ARTICLE INFO

Article History

Received: 2nd November 2016

Received in revised form :

2nd November 2016

Accepted: 6th November 2016

Published online :

6th November 2016

I. INTRODUCTION

Cloud computing is an internet based computing which enables sharing of services. Cloud computing allows users to use applications without installation any application and access their personal files and application at any computer with internet or intranet access. Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted. Thus, how to efficiently verify the correctness of outsourced data without the local copy of the data files becomes a big challenge for data storage security in cloud computing. Note that simply downloading the data for its integrity verification is not a practical solution due to the expensiveness in I/O cost and transmitting the file across the network.

In this paper, we propose a public auditing scheme for the regenerating-code-based cloud storage. The public auditing system consists of two phases, Setup and Audit:

Setup:

The user initializes the public and secret parameters of the system by executing Key Generation and pre-processes the data file F by using SigGen to generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server, and delete its local copy. As part of pre-processing, the user may alter the data file F by expanding it or including additional meta data to be stored at
server.

Audit:

The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message from a function of the stored data file F and its verification metadata by executing Generation Proof. The TPA then verifies the response via Verify Proof.

To solve the regeneration problem of failed authenticators in the absence of data owners, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudo random function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code-based cloud storage.

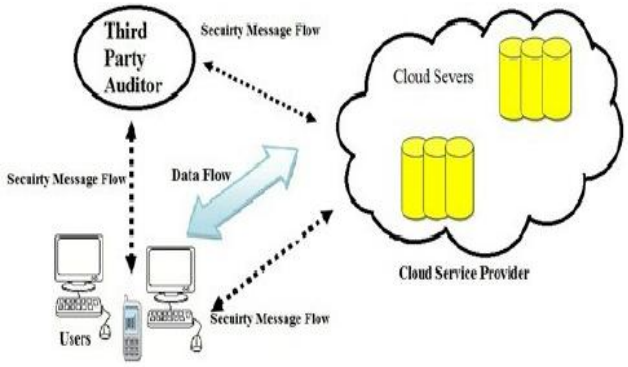

Fig.1: The Cloud Service Architecture

II. MATERIALS AND METHOD

1) Technologies Used:

During the solution development, following soft-wares were used:

- Visual Studio 2015
- .NET Framework 4.6

The system needs the following specifications:

- Hardware Requirement:
  - System : Compatible desktop
  - Hard Disk : 80GB or more
  - Dual core processor
  - RAM : At least 4 GB RAM
- Software Requirement:
  - Operating System : Windows 7 or higher versions
  - Coding language : ASP .NET
  - Database : MS-SQL

Stepwise flow of Methodology:

Step 1**:** Enter the confidential data during Registration of users. User enters the personal details for future generation of password which is used in login phase. When users create or register into the cloud, that time server generate random number for security purpose i.e. server apply the Random Number Generation Algorithm (RNG).

Step 2: Secret sharing technique:

Secret Sharing technique is mostly used in distributing sensitive information among specific people over the Internt. In this technique, data is divided into two shares.

Step 3: User try to login into his/her account.

User logins into his /her account and requests for generation of the password. Server use the Random Number Generation Algorithm for saring outsourced data and sends it to the user' s registered mail. This process repeats every time user tries to login into his account as it provides more security for the user .

Step 4: Data validation Phase.

During data validation, server extracts the data from Third party Auditor or another cloud user and validates it. If the validation is done successfully, user gets OTP (One Time Password).

Step 5: Login completion phase.

After proper data validation, user gets OTP (One Time Password) on his registered mobile number. User enters one time password, after its validation user logins successfully to his/her account.

- The communication of the user with the application can be shown with the help of following diagram :

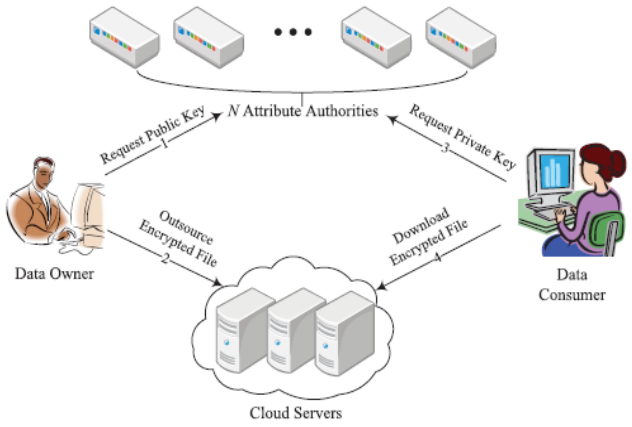

Fig.2: The Control Cloud Architecture

III. SYSTEM MODEL

In this paper, we consider data storage and sharing services in the cloud with three entities: the cloud, the third party auditor (TPA), and users who participate as a group (as shown in Fig. 3). Users in a group include one original user and a number of group users. The original user is the original
owner of data, and shares data in the cloud with other users.

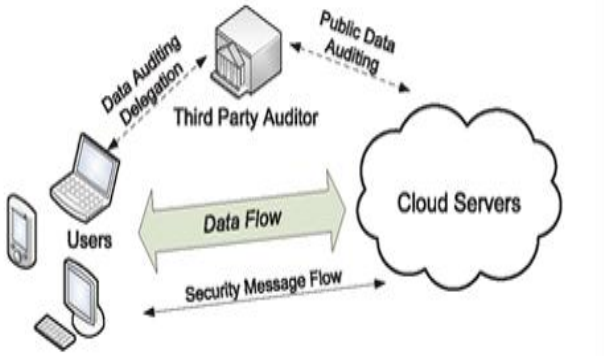

Fig.3: The Proposed System Architecture

Based on access control policies , other users in the group are able to access, download and modify shared data. The cloud provides data storage and sharing services for users, and has ample storage space. The third party auditor is able to verify the integrity of shared data based on requests from users, without downloading the entire data. When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing request, the TPA generates an auditing message to the cloud, and retrieves an auditing proof of shared data from the cloud. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.

Here, we use couple of keys for provide privacy to the data in cloud storage. Public key and private key is used for sharing the data over the cloud storage. The public key and private key are used by the authenticated person. The control architecture of cloud shows the uploading and downloading the data securely.

IV. ALGORITHM

Random Number Generation:

Random number generators are very useful in developing Privacy-Preserving Public-Auditing system, as debugging is facilitated by the ability to run the same sequence of random numbers again by starting from the same random seed. They are also used in cryptography, so long as the seed is secret. Sender and receiver can generate the same set of numbers automatically to use as keys. The generation of pseudo-random numbers is an important and common task in computer programming. While cryptography and certain
numerical algorithms require a very high degree of apparent randomness, many other operations only need a modest amount of unpredictability.

Mathematical Model :

Set Theory Analysis:

Let ‘ S’ be the System for regenerating code based
a. cloud storage using public auditing scheme,
S = {…….}

b. Identify the inputs as X .
S ={ f s, e, X, Y, Fme, DD, NDD, ϕ}

Where,
s = start of the web server.
1. Log in with server.
2. Deploy the web application on web server.

e = End of the web application.

To retrieve the useful transferring data form dataset and provide recommendation to the TPA.

X = Input of the program.
X = { F, m, ϕ, Ψ}
F be the file.
M be the Number of file block.
ϕ be the authenticators.
Ψ be the block of code.
Y = Output of the program.
Y = {⊥}
⊥ be the new coded block.

Responses and outputs a new coded block set by authenticator i.e. ⊥
X, Y ε U
Let , U be the set of system.
U = { F, ⊥ , A, R }
Where,
F, ⊥ , A, R are the element of the set.

F = File.
⊥ = new block of code.
A = Public auditing.
R = File replacement.
Above mathematical model is NP-Complete.

V. RESULTS / DISCUSSION

The Random Number Generation Algorithm has been applied in the system successfully. One of the experimental results of the Random Number Generation Algorithm is that it makes two shares of data after data uploading or downloading process. During login phase, after image validation, OTP (One Time Password) is generated and verified. Therefore system gives the some advantages .

Advantages:

1. Maintain Security
2. Cloud Integration with confidential data
3. Sharing cloud between multiple users

VI. CONCLUSION

The homomorphic linear authenticator and random masking utilize to guarantee that the TPA would not learn any knowledge about the data content store on the cloud server during efficient auditing process, which not only eliminates the burden of cloud user from the tedious and a possibly expensive auditing task, but also alleviates the users fear for their outsourced data leakage. considering TPA many concurrently handle multiple audit sessions from different users for their outsource data files, we further extend our privacy preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing task in batch manner for better efficiency Extensive analysis show that our scheme are provably secure and highly efficient.

VII. ACKNOWLEDGEMENT

We would like to thanks all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future. Also I would like to thank my guide Prof. Tejashree Gaikwad for her valuable guidance.

REFERENCES

[1] Jian Liu, Kun Haung, Hong Rong, Huimei Wang and Ming Xian, ” Privacy-Preserving Public Auditing for Regenerating Code-Based Cloud Storage, IEEE Transaction on Information and Security, vol 1 No 2015.

[2] Priyanka Deharya, Shweta Shrivastava, Vineet Richarya, ” Surveying Cloud Storage Correctness using TPA, with BLS” , International Journal of Engineering Research and General Science Volume 3,Issue 1 Jan,2015.

[3] Meera Randive,Bhavna Pansare, ” A survey on Privacy-Preserving Public Auditing For Regenerating-Code-Based Cloud Storage Using Attribute Based Approach ” , IJIICCE,vol 3, Issue 12,Dec 2015.

[4] Cong Wang, Student Member, Sherman S.-M. Chow, Qian Wang, Student Member, Kui Ren, Member and Wenjing Lou, Member, Privacy-Preserving Public Auditing for Secure Cloud Storage , Referenced on 2014.

[5] Miss. Nupoor M. Yawale , Prof. V. B. Gadichha,Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm ,International Journal of Advanced Research in Computer Science and Software Engineering 3(11), November - 2013, pp. 1032-1037.

[6] Abhinandan P Shirahatti, P S Khanagoudar , Preserving Integrity of Data and Public Auditing for Data Storage Security in Cloud Computing, sIMACST: VOLUME 3 NUMBER 3 JUNE 2012.

