TEST Engineering & Management

January - February 2020
ISSN: 0193-4120 Page No. 17012 - 17017

A Secure and Efficient Data Store and Remote Data Integrity Checking in Cloud Computing Using TPA

V.Santhoshamarnath[1],Ushadevi[2], B.Karissma[3],R.Nivashini[4]

[1,2,3,4]Department of Computer technology, Sri Krishna arts and science college,Coimbatore, India

Article Info
Volume 82
Page Number: 17012 - 17017
Publication Issue:
January - February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 29 February 2020*

Abstract

Cloud computing is emerging Technology which enables service to users store their significant data in the cloud. The Cloud data users need to encrypt the important and efficient data for cloud security. The point of data security which has always been a noteworthy aspect of quality, cloud computing cause a new security threat. Now a day's serious issues research going on regarding data security between user and service provider. Because Cloud Service Provider may be misuse the user data, maybe data modification, corruption can be perform by cloud service providers. So there is a threat to security and privacy of data. The Cloud Service Provider (CSP) can pass the user data without the user's knowledge. For doing auditing every time from user side it's a very difficult task to a user, it leads some problem to the user. To solve this kind of issues, proposed research system is effectively use the third party as an auditor. Third party auditor acts as an agent of data owners. Here the data will be encrypted at user side with the help of advanced NTRU Cryptosystem and will be in encrypted form over network. Multi Third Party Authentication (MTPA) will audit the data regular time interval with the help of Timer and scheduling process. After, it checks the data integrity of the client's data. No one else rather than the user is able to view data. But if someone tries to access the data or modify the data, then there will be a file alert generated to the user.Third Party Auditor provides regular auditing so that user no needs to worry about data privacy. Hence, finally, the user will have a more elaborated view over his data privacy.

Keywords – *Cloud computing, data integrity, TPA, data privacy, cloud service providers.*

I. INTRODUCTION

With a large amount of data, it is burdened on users to store data locally. Cloud storage enables users to remotely store their data and enjoy the on-demand the high-quality cloud applications without the burden of local hardware and software management. Now a day's cloud storage is used for the storage of large data and it provides a storage platform for enterprise and individuals and also using cloud storage system user can store and access data remotely.

It is avoiding committee of a large number of users for the managing and purchasing software and hardware. In the new data storage paradigm in the cloud is including many challenging design issues which have a profound influence on the security and performance of the overall system. The largest concerns with cloud data storage is that of data integrity verification at untrusted servers. The Cloud has been envisioning as the next generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history such as (i) on-demand self-service, (ii) ubiquitous network access, (iii) the location independent resource pooling, (iv) rapid resource elasticity, (v) usage-based pricing and (vi) transference of risk. The Cloud Computing that makes different kinds of special advantage after that

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 17012 - 17017

it also brings new and challenging the security threats towards users' outsourced data.

II. PROBLEM DEFINITION

The author has presented the paper [1] Technique called Identity Based Distributed Provable Data Control. This Method used in Multi-Cloud Environment. The faster profit growth of CSP is providing the features for the client based data. General CSP meets two issues namely, privacy preservation and data integrity.

The author has presented the paper [2] concept is Identity-Based Integrity Verification using DPDP in Multi-Cloud Storage. The Cloud provides a service like faster profit growth by giving the features for client's data or information. The single cloud service provider meets this problem category privacy preserving and data integrity. The multi-cloud storage is used in a distributed cloud environment.

The author has presented the paper[3] concept namely, Identity-Based DPDP in multi-cloud storage. The paper concept formalizes the ID-DPDP system model and security model. At the same time, it proposed the first ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard.

The author has presented the paper [4] concept is Identity-based Multi-cloud DP. The multi-cloud provides multiple services for improving the performance. These performance metrics can be used to improve the performance of applications running in the cloud it can be run on large EC2 instances.

The author has presented the paper [5] Technique Called as SDIVIP2 shared data integrity verification with identity privacy preserving in mobile clouds. It proposed a shared data integrity verification with identity privacy-preserving protocol named SDIVIP2 for mobile cloud storage.

The author has presented the paper [6] Technique name is effectively presented Management of User Revocation with Public Auditing for Shared Data in the Cloud. The public auditing for shared data with efficient user revocation in the cloud gives a new public auditing mechanism for shared data with efficient user revocation in the cloud.

The author has presented the paper [7] Technique is robust and efficient privacy-preserving public auditing for regenerating-code-based cloud storage and it proposes a privacy-preserving public auditing system where the data owners can allow a TPA for validating and integrity checking their data.

The author has presented the paper [8] Technique is Data Integrity Checking and Access Confidentiality in Multi-cloud Storage and its overview of future work of Data integrity checking and access confidentiality in multi-cloud storage is presented.

The paper [9] author has presented the Identity Based Cloud Storage Security System. In this system, it investigated proofs of storage in the cloud in a multi-user setting. It introduced the notion of identity-based data outsourcing and proposed a secure IBDO scheme.

The paper [10] has presented the concept is Data Integrity Checking in Dynamic Cloud. It has analyzed data storage correctness issue in reference to cloud computing. In this system has provided the mechanism for trusted and secure data storage model with a new scheme with integrity verification.

III. PROPOSED SYSTEM

The chapter discusses the proposed methodology and the steps involved in this proposed system. The existing framework does not guarantee the data availability in case of server failures. Therefore, correct data verification of storage in the cloud must be conducted without explicit knowledge of the whole data. Less Efficiency and Security level is low. Proposed system addressed the construction of an efficient audit service for data security in clouds. Here the data will be encrypted at user side with the help of advanced NTRU Cryptosystem and will be

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 17012 - 17017

in encrypted form over network. The proposed system is an interactive audit protocol to implement the audit service based on a MTPA (Multi Third Party Auditor). In this process, the MTPA (Multi Third Party Auditor) acts as an agent of data owners.

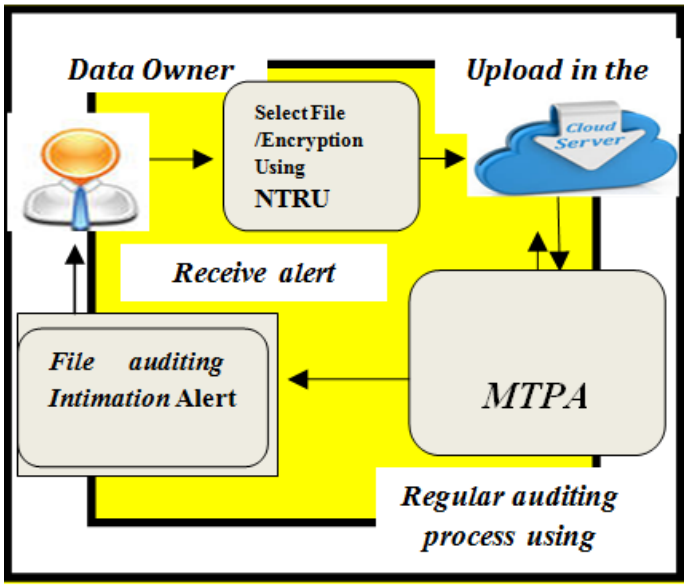

Figure 3.1 Proposed system architecture

Contributions of the proposed System

The followings are the contributions of the proposed system.

- The proposed system addressed the construction of an efficient audit service for data security in clouds.
- The main objective of the proposed system is to provide ensure secure data storage in the cloud. Provide the higher security to the user's data by using encryption technique and Multi Third-party auditor will audit the data and check the data integrity of the client's data.
- someone tries to change the data integrity, and then there will be a file alert generated to the user
- Proposed application providing solution for the user who needs security and privacy for their data.
- This application minimizes the workload of the cloud data owners.
- Third-party auditor performs regular verification to monitor the data. Auditor to ensure the privacy and security issues and successfully detect misbehavior of cloud service providers.
- Strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the Identification of misbehaving server.

IV. METHODOLOGIES

1. Cloud infrastructure and authentication

Network infrastructure creation with n number of servers and clients is the first step. The module creates the following interfaces.

- Storage server
- Client

The authentication phase defines the security and authority to access the above user types, for example, every client should be authenticated before accessing the resources in the storage cloud. An authorized person can upload and download the files. This user process should register with all basic information.

2. Data Selection and upload process

This module will be performed by the data owners after the successful authentication. The data owner can select text data. After the selection of data owner can upload the document in cloud servers.

3. Encryption process

NTRU stands for nth degree Truncated Ring polynomial Unit. NTRU is a relatively new Public Key Cryptosystem (PKCS).The algorithm is based on embedding messages in a Polynomial ring. The key generation and encryption/Decryption process in NTRU is much faster than other algorithm. Public Key Cryptography Encryption algorithm is proposed to maintain the data record along with its security and privacy in cloud outsources data. Once

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 17012 - 17017

document encrypted this document upload in the server.

NTRU Algorithm:

Encryption Process

// First, specify a number of parameters.

N -polynomials in the truncated polynomial ring

P, q- large and small modulus

F and G- Two polynomials

M – Message

H= public key

Step: 1 Initialize the parameters values;

N=11 q=32 p=3 df=4 dg=3

Q should be greater than p

//Secondly, key generation process. The process of key generation means randomly generates the //private or public keys follow the formula.

Step: 2 Key generation process

Needs to choose a polynomial f and polynomial g

h = pFq*g

Step: 3 multiply the integer

Result n=p. multiply (q); //this n used as modulus for public and private key

//Calculates random key values

Step 4: Calculate φ (n) = (p-1). (q - 1) Where φ is totient function

Big Integer phi = (p.subtract (one)).multiply (q.subtract (one));

//call Mod Inverse predefine library function to get private key

Private Key = publicKey.modInverse (phi);

Private Key is the pair of polynomials f and Fp.

Step 4: Encryption process

X1=assign file content info // The Variable X1 is assigns in to the file contents

X2=key info // The Variable X2 is assigns in to the key information

Encrypt (x1); //Using the Encrypt () function and encrypts the file

Big Integer encrypt (Big Integer message)

// In the encrypt () function is pass the 'message' value.

// The Variable of message is assign in to the above main function variable 'x1'.

{

Return message.modPow (public Key, modulus);

// Pass the modulo division value into main function with public key.

}

Decryption Process

// Use decrypt function and pass three parameter values such as private key// content values and modules.

Step 1: pass three input parameters to decrypt function

Private Key, Encryption content values // after call the decryption function and pass the variable 'encrypted'

Step 2: decryption function call

Big String decrypt (Big Integer encrypted) {

Return encrypted. ModPow (Private Key, Decrypt data);

}

Published by: The Mattingley Publishing Co., Inc.

TEST Engineering & Management

January - February 2020
ISSN: 0193-4120 Page No. 17012 - 17017

// the decrypted process is using the decrypted function value.

Step 3: Decrypt= (cModPow) Mod2.

4. Integrity Verification

Metrics	Dataset	Existing	Proposed System using MTPA
	DS1(50)	95	99
Misuse Detection Accuracy (%)	**DS2(100)**	93	98.8
	DS3(120)	93	98.5
	DS4(150)	90	98

This module helps to identify the cloud user data Integrity of Encrypted data. These modules calculate a hash value for each file stored in the cloud service. Trust Authority randomly request file blocks to a different server used to check file Integrity Verification. First, calculate a hash value for every block and compare hash values with the previous hash value. By verifying the values easily can verify the Integrity effectively.

5. Sms/mail Intimation

The mobile management is the process of enhancing the mobile service from the application. Including the relevant files and features in the application is more important to send automated SMS intimation to file owner whenever change the file integrity in cloud service.

V. RESULT AND ANALYSIS

Experimental Results

This section describes the execution progression. Execution is the recognition of a research application, or predefine plan of execution, scheme, replica, and design of proposed research. This section completely explains the software, hardware, system environment files and modules which are used to develop the research work. Then the experimental term is performed on an Intel core 2 duo 2.70 GHz processor with the maximum 3 GB RAM capacity. The proposed research algorithms are implemented in c# programming language and with dot net environment and are run under the Windows platform.

Data Set:

The data used in this study contains real-time cloud file data and the data store in a database. The dataset is generally composed of structured and unstructured text data. This data contains several attributes such as file name, date of upload, file format, etc contains much more categories there are a total of more than 500 file records in the database.

Table 5.1 Performance Evaluation

Results and Analysis

The experiments are designed so that the different parts of the work could be evaluated. These include the evaluation of the Encryption time above dataset. Finally, the performance of this proposed work Scheme was compared with the existing algorithms based on the following parameters.

- Accuracy – Determines the correctness
- Precision –Repeated process same result
- Time taken – Determines the processing time involved.

Encryption Time comparison

Metrics	File Size	CP-ABE	Hierarchical Attribute-Based Document Encryption	Proposed NTRU Encryption
	300Mb	1984	1500	1400
Time Comparison (ms)	**500Mb**	2300	2150	2000
	700 Mb	2500	2350	2200

Published by: The Mattingley Publishing Co., Inc.

TEST Engineering & Management

January - February 2020
ISSN: 0193-4120 Page No. 17012 - 17017

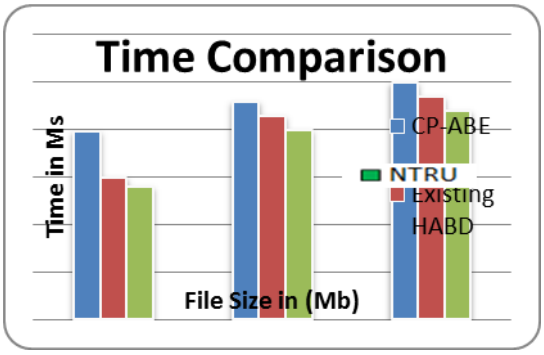

Figure 5.1 Times Taken Comparison

Performance comparison of the proposed system with existing approaches based on Encryption Time

From the results shown in the graphs, it can be observed that the proposed model-based approaches provide better accuracy and increased true positive rate when it is analyzed with the different number of datasets. The system finally performs the analysis to show the time accuracy of the proposed system in graph format.

VI. CONCLUSION

The study and research proposed a new scheme for cloud data auditing. Data integrity checking and access confidentiality in multi-cloud storage are presented. System design of remote data integrity checking is done by the verifier effectively for maintaining security and privacy in the multi-cloud is formalized. Survey of various techniques are used to secure the client's data in the cloud server is taken and their challenges are analyzed. The future direction is to implement the proposed work and analyze the performance of data integrity checking and access confidentiality in multi-cloud storage.

REFERENCES

[1] Manasa. P, VanishreeAbhay. Identity-Based Distributed Provable Data Possession A Method used in Multi-Cloud Environment. ISSN 2319-8885, Vol.04,Issue.04. International Journal of Scientific Engineering and Technology Research.February – 2015.

[2] NikhatMohammadi, ShaistaNousheen, KhadarbiShaik. Identity-Based Integrity Verification using DPDP in Multi-Cloud Storage. ISSN 2321-8665, Vol.03,Issue.04. International Journal of Innovative Technologies.July – 2015.

[3] S.M.Sisha, Sk. Karimulla, Dr. Praveen Sham. Identity-Based Distributed Provable Data Possession in Multi-Cloud Storage. ISSN 2348–2370
Vol.07, Issue.04.International Journal of Advanced Technology and Innovative Research.June – 2015.

[4] Y MeenaPriyadarshini, Dr. P S K Patra, S Prakash. Identity-based Multi-cloud Data Possession. ISSN: 2321-9939. International Journal of Engineering Development and Research. [2015].

[5] Yong Yu, Jianbing Ni, Qi Xia, Xiaofen Wang, Haomiao Yang, and Xiaosong Zhang. SDIVIP2: shared data integrity verification with identity privacy preserving in mobile clouds. DOI: 10.1002/cpe.3484. March 2015.

[6] Anju T G, Sivadasan E T, Management of User Revocation with Public Auditing for Shared Data in the Cloud. International Journal of Computer Science and Information Technology, Vol. 7 (2), 2016, 537-539.

[7] Tessy Vincent, Mrs. Krishnaveni. V.V. Robust and efficient privacy-preserving public auditing for regenerating-code-based cloud storage.International Journal of Engineering Sciences and Research Technology. ISSN: 2277-9655. June- 2017.

[8] B. Pavithra, C.S.Anitha. Data Integrity Checking and Access Confidentiality in Multi-cloud Storage. International Journal of Pure and Applied Mathematics. January 3, 2018.

[9] ShaikhNikkhatparvin, KarishmaManiyar, SnehalTawhare, Prof. Gholap P.S. Identity Based Cloud Storage Security System. International Journal of Innovative Research in Computer and Communication Engineering. Vol. 6, Issue 9, September 2018.

[10] R. Vinoth, R. Vimalraj, R. Sathishkumar, R. Sarathkumar. Data Integrity Checking in Dynamic Cloud.International Journal of Engineering Research in Computer Science and Engineering.Vol 5, Issue 3, March 2018.