Storage Security using an Efficient Protocol with Bi-directional Verification in Cloud Computing

Priyanka K. Deshmukh, Department of Computer Engineering, SNDCOE & RC, Yeola,

Imran R. Shaikh, Department of Computer Engineering, SNDCOE and RC, Yeola

Abstract*—In cloud computing, data owners upload data on cloud servers and users can access or download the data from the cloud servers. This technique of data hosting service creates new security problems which need to be checked for data integrity. Some of the existing solutions are inefficient to audit the integrity of the data. An efficient authentication protocol must have a desirable feature of denying the data access request which are not made by authenticated user and must collect the data required for analysis for validation results. In this paper, we propose an authentication and auditing protocol which provides an efficient way of mutual authentication data access and supports dynamic data operations. Better load management reduces the computational complexity of the user. In addition to this, we provide an error acknowledgement response scheme which handles the error efficiently along with reduction in computational overhead.

***Keywords* — Audit, Bi-directional Verification, Cloud computing, Integrity, Mutual authentication, Security,**

I. INTRODUCTION

Cloud computing is an effective technology, which is changing the path of designing and acquiring computer hardware and software for IT world. Standard model of cloud computing provides number of benefits including low cost, fast deployment, easy access, flexibility in resource management, best efficiency. But security is most important aspect which needs to be addressed in cloud computing.

In every organization security of stored data is a critical and essential aspect of cloud computing. Ensuring the safety of data is important for user as well as data owner. In this paper, we are proposing an efficient protocol for user authentication data access for cloud computing.

Data sharing improve connection and collaboration between researcher and data owner. Data sharing is most important and effective because it allows to share resources and ideas. In this system our purpose to provide access to data sharing in between authorized data owner and data user.

The techniques provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext given only the cipher text. The techniques provide controlling searching, so that the untrusted server cannot search for word without the user authentication.

In this system data owner can share their data in cloud server as well as also access the other data. When user wants to access the data to that particular data owner he/she sends request to that data owner, if data owner allows then and then only user can access their data.

II. REVIEW OF LITERATURE

Bin Feng et.al[1] proposed a new remote data-auditing system which support the bi-direction verification for data storage in cloud computing. A new entity to generate the authority credential was use in this paper.

Wei Zhang et.al[2] explored the problem of secure multi keyword search for multiple data owner in the cloud computing.To efficiently authenticate data user and detect attackers who steal the secret key and perform illegal searches ,they proposed a novel dynamic secret key generation protocol and new data user authentication protocol.

Dawn Xiaodong Song et.al.[4] In terms of security in this paper, the data stored data on a storage server such as file mail servers in encrypted form to reduce security privacy risks.

Qian Wang et.al [6] proposed public auditing system of data storage security in cloud computing, and provide a protocol supporting of totally dynamic data operation, especially to support block insertion, which is missing in most existing schemes.

A. Advantages

_ Enable a third party authentication to evaluate the service quality from an objective and independent perspective .

_ They explored the problem of providing simultaneous public audit ability and data dynamics for remote data integrity check in Cloud Computing.

B. Disadvantages

_ Less security in bi-direction verification.

_ Weak Filtration in multi-Keyword searching.

_ Security mechanisms is weak.

III. SYSTEM ARCHITECTURE

The following is our proposed system architecture

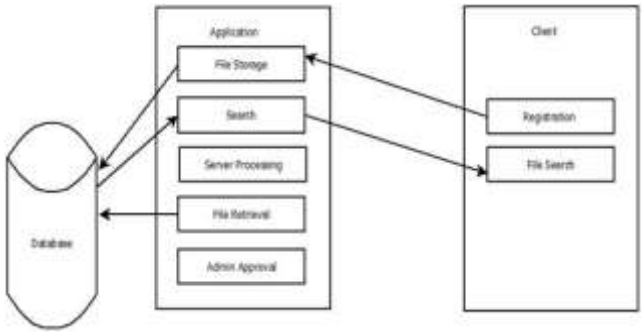

Fig. 1. Block Diagram of Proposed System (System Architecture)

A. System Architecture Module:

Users:

System should consists two different users:

1. Data Owner
2. Data User

Data Owner: Data Owner host there data on system and also search data from system. Data owner is having following module.

Data Owner's Modules

1) Login Module
2) Data Upload
3) View Files(Search)
4) File Share

1)Login Module:

When data owner want to upload data on the system, First he/she must be logged in into the system.

2) Data Upload:

The data uploading process on the cloud server will be done by using data upload module. Data owner can upload any type of data on cloud server.

3)Search Files:

If data owner need to search any specific file, Search File module will provide the facility to data owner to search any specific file

4) Share File:

File sharing to any data user who is authorized. Data owner share the file to data user by using file Share module. File sharing module is provided through this module it depends on data owner.

Data user is having following modules.

Data Users Modules:

1) Login/Registration:

In this module data user needs to register on to system.In registration process user need to produce some personal information which will be stored in system in back-end. After registration user-name password will be used to authenticate to that user.

2) View Files(Search):

In this module system will search any specific file as per the user requirement. User enters search domain on the searching bar, If the file exists for that particular domain,the file name will be shown on the dash board. If file doesn't exists for that particular domain, output will be NULL.

3) Download Files:

It depends on search file. In searching file process if user gets searched file in dashboard, download will be displayed for that file. User can select specific file download it by using the private key which is sent by data owner.

In this process when data user wants to access some particular file, he/she can send a request to data owner.Once the requested file is ready to send data owner will send a private key for authentication purpose.Then using that private key authentication of user will be done.once authentication is by data owner side then user can access or download that file.

IV. SYSTEM ANALYSIS

A. System Analysis

a) : These analysis are clearly stated by customer.

S1: System should be able to provide Secure Authenticate.
S2: System should securely Upload Data.
S3: System should provide quick results to the user.

B. Expected Results

b) : These results are implicitly type requirements. These are not stated by customer but are expected to be satisfied by the end system.

E1: System should be able to search files.
E2: System should be able to Bidirectional Authenticate.
E3: System should be able to store content in encrypted format.
E4: System should be able to Request for file access and response from owner of file.
E5: System should be able perform Capacity Determination.
E6: System should be able to perform Source Texture Recovery and Message Extraction.

C. Excited Results

c) : These results neither stated by customer nor expected. To achieve the total of satisfaction developer includes these requirements.

X1: Time complexity and space complexity should be less.
X2: System should be user friendly and platform independent.
X3: System should be consistent.
X4: System should be secure.

V. VALIDATION OF REQUIREMENT

A Validation of requirement is most important criteria, Requirement Validation of this system are given below.

A. Validation of Normal Requirements

VN1: System can provide secure Login .
VN2: System must use Encryption algorithm.
VN3: By avoiding time consumption system can provide quick result to the user.
VN4: System can provide authentication to the user by using secret key.

B. Validation of Expected Requirements

VE1: System can generate patch from source texture. Patch represents an image block of source texture where its size is user specified.
VE2: System can able to search files patch.
VE3: System can perform in any web browser.
VE4: System can perform to generate OTP and send on mail or mobile.
VE5: System can perform Capacity Determination by calculating total embedding capacity.

C. Validation of Excited Requirements

VX1: The Time and Space Complexity of the system will less, if system uses better performance algorithm.
VX2: System can be user friendly if better GUI is used.
VX3: System should be consistent.
VX4: System can be secure if secret key is provided.

VI. SYSTEM REQUIREMENT

The Software and Hardware requirement are as below,

A. Software Requirements

Software requirement for the this system are given below.

_ Operating System : Windows 7
_ Front End:Java ,Jsp, and Servlet
_ Back End: Mysql
_ UML Design :Rational Rose

B. Hardware Requirements

Hardware requirement for the this system are given below.

_ Hard Disk:120 GB
_ RAM:512 MB
_ Processor: Pentium 4
_ Input device: Keyword and Mouse
_ Output device: Monitor

VII. RESULT ANALYSIS

Here fig show the results in uploaded block size related to to data security provided by Cloud Service Provider. In this implemented system file is divided into blocks, and each block is having different key. It is difficult to hack whole file by hacker or cheating party, So the system provides high level security index.

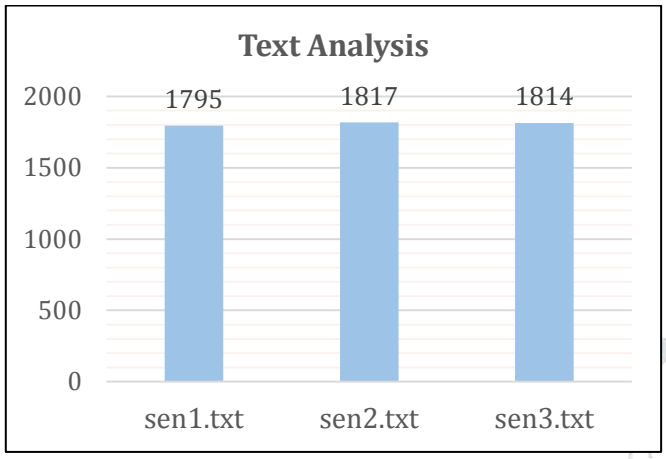

Fig. 2. Block name & Block Size Chart (System Architecture)

VIII. CONCLUSION

We define a system in which utilization of cloud data bydata user is made secure by doing authentication of user using a AES. For searching file we have used TFIDF (Term Frequency- Inverse Data frequency) algorithm.

ACKNOWLEDGMENT

I like to give my sincere thanks to PG Coordinator Prof. Dhakane V.N. and the departmental staff members for their support. I also express my special thanks to Department of Computer Engineering SNDCOE and RC Yeola for making all the possible help and guidance during my project implementation.

REFERENCES

[1] Bin Feng12, Xinzhu Ma12, Cheng Guo12, Hui Shi3, Zhangjie Fu4,(Member, IEEE), Tie Qiu12‘”An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing” ”,DOI 10.1109/ACCESS. 2016.2621005, IEEE Access 2169-3536 (c) 2016 IEEE

[2] Wei Zhang Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE,Jie Wu, Fellow, IEEE, and Siwang Zhou.‘”Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing” ”,DOI 10.1109/TC.2015.2448099, IEEE Transactions on Computers

[3] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou.“Aview of cloud computing,Communications of the ACM,.” vol.53, no.4, pp. 50-58,2010..

[4] Zhihua Xia,Xinhui Wang, Xingming Sun and Qian Wang.“”A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data””, IEEE Transactions on Parallel and Distributed Systems,vol. 27, no. 2, pp. 340-352, 2015

[5] Zhangjie Fu,Kui Ren, Jiangang Shu, Xingming Sun, and Fengxiao Huang, “Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement,”, IEEE Transactions on Parallel and Distributed Systems, DOI: 10.1109/TPDS.2015.2506573, 2015.

[6] Wang, Qian, et al. “Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing”, IEEE Transactions on Parallel Distributed Systems 22.5(2010): 847-859.

[7] Yang, Kan, and X. Jia.‘Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing ”,Parallel Distributed Systems IEEE Transactions on 24.9(2013):1717-1726.