isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

EFFICIENT APPROACH FOR DATA RETRIEVABILITY IN CLOUD STORAGE SYSYTEM

Priyanka T[1], Vishali C[2], Dr. R. K. Selvakumar[3]

Student, Department of Computer Science and Engineering, Agni College of Technology, India[1,2]

Head of Department, Department of Computer Science engineering and senior IEEE member Agni College of Technology, India[3]

ABSTRACT

Cloud computing is basically internet based computing where the virtual shared sources provide the users with software,infrastructure,platform,devices and other resources.It allows users to store their data in a remote server to get less expensive local storage and management costs so that they can access data of interest anytime anywhere.We propose an enhanced dynamic proof of retrievability scheme supporting public audit ability and communication-efficient recovery from data corruptions. We split up the data into small data blocks using network coding and encode that data block using Base64. To eliminate the communication overhead for small data corruptions within a server, each encoded data block is further encoded. Based on the encoded data blocks, we utilize tree structure to enforce the data sequence for dynamic operations, preventing the cloud service provider from manipulating data block to pass the integrity check in the dynamic scenario. We also analyze the effectiveness of the proposed construction in defending against pollution attacks during data retrievability.

***KEYWORDS*- Proof of retrievability, Cloud service provider, Communication overhead, Public audibility, Data Corruptions.**

1. INTRODUCTION

The scope of the project is the use of enhanced dynamic proof of retrievability scheme supporting public auditabilty and efficient recovery from data corruptions and make data availablity always to the users.The support of public auditability allow the data owner to delegate the checking tasks to a third party auditor, So as to save his own computational resourses .The original data file object can be reconstructed from the encoded blocks contained in the server. Thus , it tolerates the failure of any storage servers.The client can upload their files in cloud

environment where they access the files from anywhere and anytime by just login into cloud.If some information in the file are corrupted by byzantine failure or hacked by some external source, here we use auditor as a intermediate between client and admin so we can retrieve our details in the file by the use of auditor where we already registered our file using private key,hence it would be secure and safe.

2. EXISTING SYSTEM

- In existing system, while uploading, the entire data were uploaded as single block, so we couldn't find the particular data loss.
- No file auditor report and file audit delegation.
- Data corruption caused by server hacks or Byzantine failures. Get network overload on every servers.
- Do not support efficient data dynamics and/or suffer from security vulnerabilities when involving dynamic data operations. Here they haven't used any network codes or erasure codes hence they faced many difficulties while finding the redundancies.
- Security issues such as data integrity and availability are the main obstacles in this system.

3. PROPOSED SYSTEM

- We propose an enhanced dynamic proof of retrievability scheme supporting public audit ability and communication-efficient recovery from data corruptions.
- To this end, we split up the data into small data blocks and encode each data block individually using network coding.
- Network coding and erasure codes are adopted to encode data blocks to achieve within server and cross server data redundancy, tolerating data corruption.
- By combing range based 2-3 tree and improved version of aggregately signature based broadcast encryption, our construction can support efficient data dynamics while defending against data replay attack.

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

4.SYSTEM IMPLEMENTATION

4.1MODULE 1: USER

•User gives key request to auditor for upload file.

•After getting the key user can upload the file.

•User can view the uploaded file details.The files which user uploads are encrypted in this module.

•User can retrieve the file.

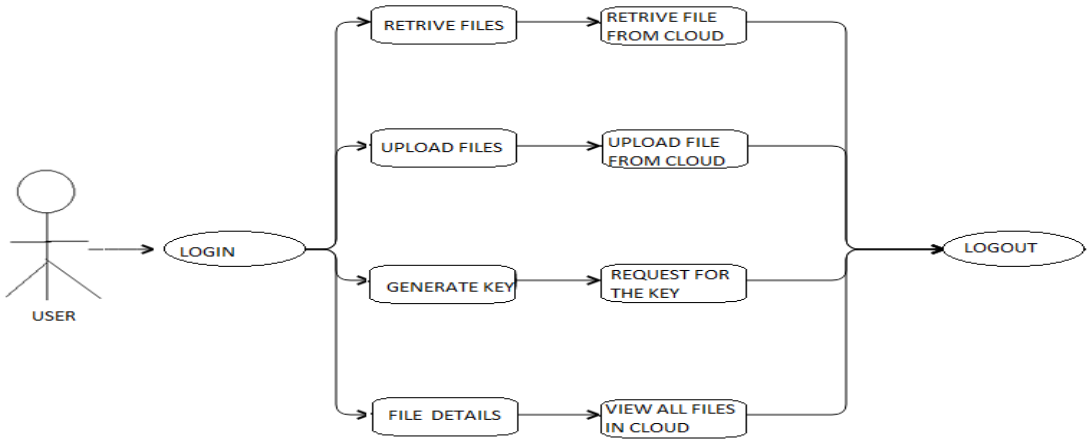

Figure 4.1:Represents the user process

•This module represents the login process of user

•User can retrieve,upload files by generating key.

•After getting the request from auditor the user can upload files and this has been described using module 2

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

4.2 MODULE 2: AUDITOR

- Auditor can provide the key to the user who gives the request.
- Auditor can view the all file details.
- Auditor can view the all key details.

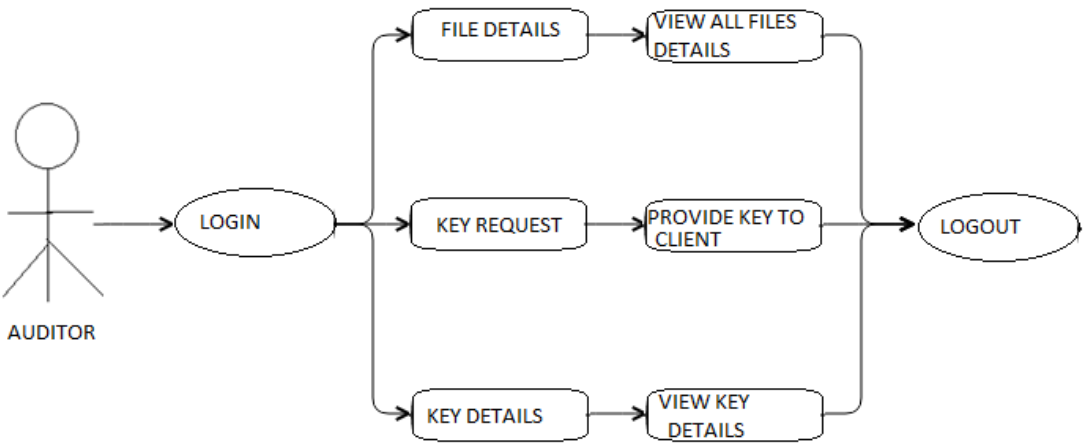

Figure 4.3: Representation of auditor process

- Public audibility is represented in this module
- Only the auditor can give the key to the user
- The key which is provided by the auditor is a unique key.

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

4.3 MODULE 3: ADMIN

- Admin can view the all client details.
- Admin can view the all file details with limited access.

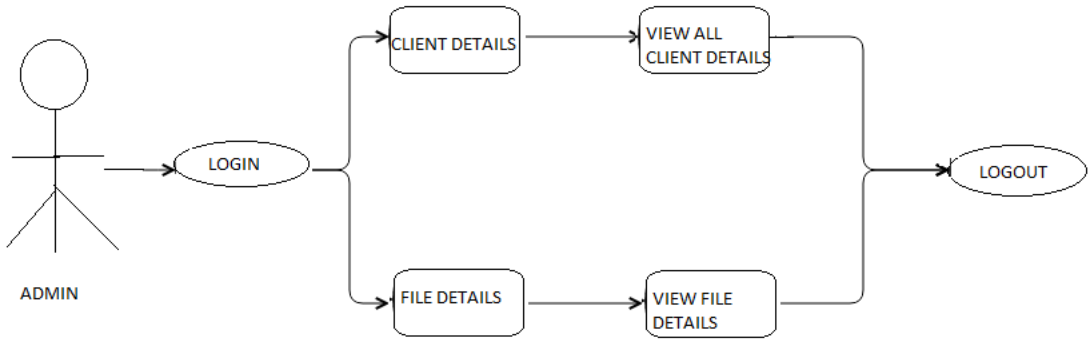

Figure 4.3:Represents admin process

5.ARCHITECTURE DIAGRAM

5.1 System architecture

The purpose of the architecture diagram is to represent the type of software architecture (Figure 5.1)that is used by the system, to describe the various hardware and software components that are used for the system implementation.

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

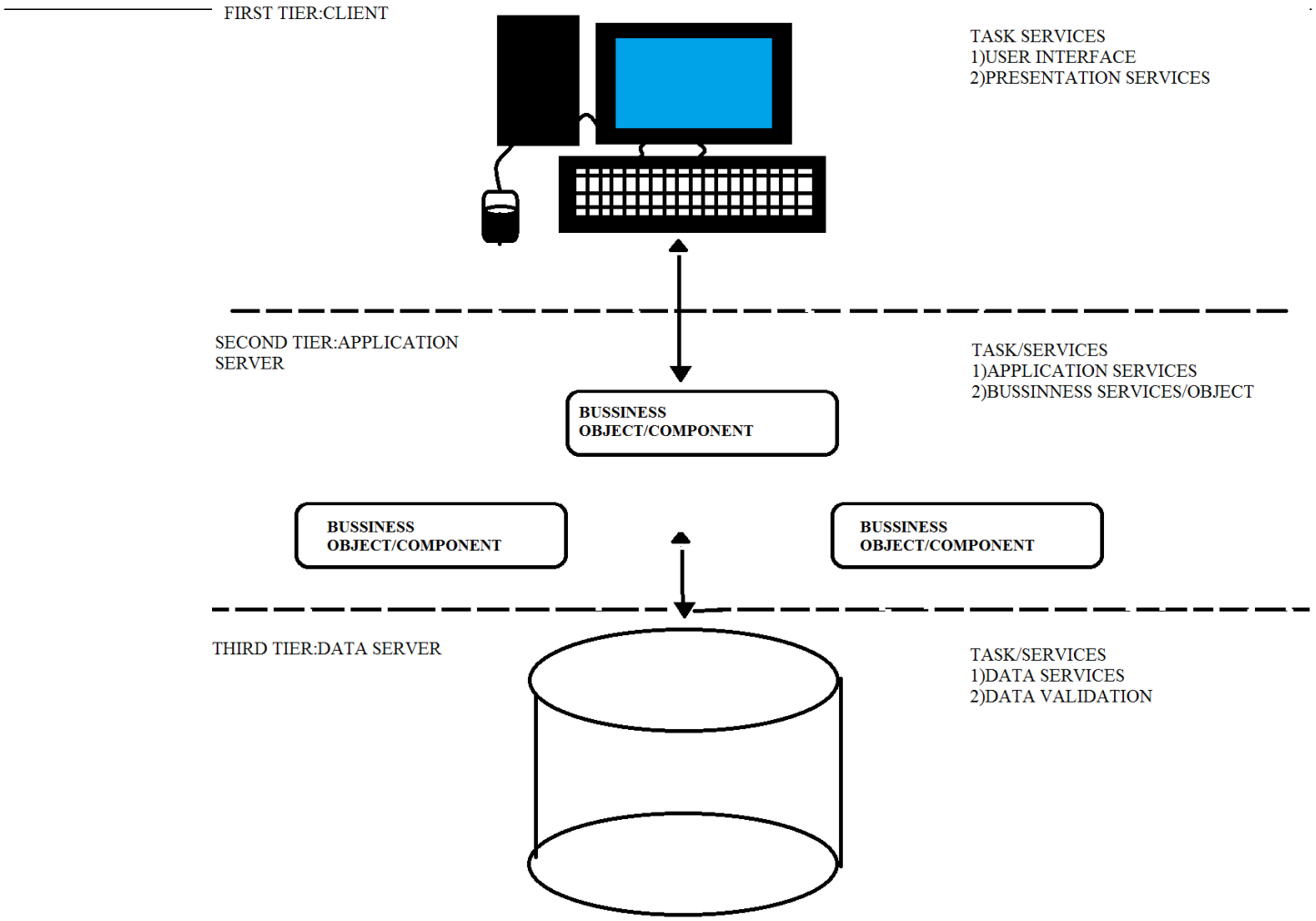

Figure 5.1 Represents the Three Tier Architecture of the system

6.Conclusion

We have introduced a dynamic proof of retrievability scheme for cloud storage systems. The erasure codes are adopted to encode the data blocks to achieve in server and supporting the efficient data recovery. By using the improved base function for encryption, our construction can support efficient data dynamic while defending against data reply attack and pollution attack.We improve security by sending the mail states the user login time and device IP. In this work, we are investing in diversity in a given cloud storage system, where for every abstract service in the architecture, there exist numbers of concrete cloud services

7 References

Dynamic Proofs of Retrievability for Coded Cloud Storage Systems
Zhengwei Ren, Lina Wang, Qian Wang, Member, IEEE, Rongwei Yu, and Ruyi Deng

Y. Zhu, H. Wang, Z. Hu, G.J. Ahn, and H. Hu, "Zero-knowledge Proofs of Retrievability,", Science China: Information Sciences, vol. 54, no. 8, pp. 1608-1617, 2011.

Z. Mo, Y. Zhou, and S. Chen. A dynamic proof of retrievability (por) scheme with o(log n) complexity. In ICC'12, pages 912–916, 2012

E. Shi, E. Stefanov, and C. Papamanthou. Practical dynamic proofs of retrievability.Technical report, 2013.

Q. Zheng and S. Xu. Fair and dynamic proofs of retrievability.In CODASPY, 2011.

Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Trans. Parallel Distrib. Syst., 22(5):847–859, 2011