International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 05, March 2016
Available at http://internationaljournalofresearch.org

Verification in Multi-Cloud Storage Using Provable Data Possession

Somesh Sondhiya[1*]; Kanchan agrakar[2*]; Shubham Wahane[3]& Neeraj Telrandhe[4]

[1, 2,3] Students, Computer Science & Engineering, GNIET, Nagpur, India.
[4] Assistant Professor Department of Computer Science & Engineering, GNIET, Nagpur, India.
[*]Email: someshsondhiya666@gmail.com ; agarkar502@gmail.com

ABSTRACT: *Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. In this paper, we address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. We present a cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. We prove the security of our scheme based on multi-prover zero-knowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties. In addition, we articulate performance optimization mechanisms for our scheme, and in particular present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. Our experiments show that our solution introduces lower computation and communication overheads in comparison with non-cooperative approaches.*

Keywords: Storage Security; Provable Data Possession; Interactive Protocol; Zero-knowledge; Multiple Cloud; Cooperative.

I.INTRODUCTION

In recent years, cloud storage service has become a faster profit growth point by providing a comparably low-cost, scalable, position-independent platform for clients' data. Since cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a *multi-Cloud* (or *hybrid cloud).* Often, by using virtual infrastructure management (VIM) , a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2. There exist various tools and technologies for multicloud, such as Platform VM Orchestrator, VMware vSphere, and Ovirt. These tools help cloud providers construct a distributed cloud storage platform (DCSP) for managing clients' data. However, if such an important platform is vulnerable to security attacks, it would bring irretrievable losses to the clients.

For example, the confidential data in an enterprise may be illegally accessed through a remote interface provided by a multi-cloud, or relevant data and archives may be lost or tampered with when they are stored into an uncertain storage pool outside the enterprise. Therefore, it is indispensable for cloud service providers (CSPs) to provide security techniques for managing their storage services. Provable data possession (PDP) (or proofs of retrievability (POR) is such a probabilistic proof technique for a storage provider to prove the integrity and ownership of clients' data without downloading data. The proof-checking without downloading makes it especially important for large-size files and folders (typically including many clients' files) to check whether these data have been tampered with or deleted without downloading the latest version ofdata. Thus, it is able to replace traditional hash and signature functions in storage outsourcing. Various PDP schemes have been recently proposed, such as Scalable PDP and Dynamic PDP. However,these schemes mainly focus on PDP issues at untrusted servers in a *single* cloud storage provider and are not suitable for a multi-cloud environment.

II.MOTIVATION

Existing System

There exist various tools and technologies for multi cloud, such as Platform VM Orchestrator, VMware, vSphere,and Ovirt. These tools help cloud providers construct a distributed cloud storage platform for managing clients' data. However, if such an important platform is vulnerable to security attacks, it would bring irretrievable losses to the clients. For example, the confidential data in an enterprise may be illegally accessed through a remote interface provided by a multi-cloud, or relevant data and archives may be lost or tampered with when they are stored into an • uncertain storage pool outside the enterprise.

Therefore, it is indispensable for cloud service providers to provide security techniques for managing their storage services.

Proposed System

To check the availability and integrity of outsourced data in cloud storages, researchers have proposed two basic approaches called Provable Data Possession and Proofs of Retrievability.Ateniese et al. first proposed the PDP model for ensuring possession of files on untrusted storages and provided an RSA-based scheme for a static case that achieves the communication cost. They also proposed a publicly verifiable version, which allows anyone, not just the owner, to challenge the server for data possession..They proposed a lightweight PDP scheme based on cryptographic hash function and symmetric key encryption, but the servers can deceive the owners by using previous metadata or responses due to the lac of randomness in the challenges. The numbers of updates and challenges are limited and fixed in advance and users cannot perform block insertions anywhere.

Definition of Cooperative PDP

In order to prove the integrity of data stored in a multi-cloud environment, we define a framework for CPDP based on interactive proof system (IPS) and multi prove zero-knowledge proof system (MPZKPS).

Hash Index Hierarchy For CPDP

To support distributed cloud storage, we illustrate a representative architecture used in our cooperative PDP scheme. Our architecture has a hierarchy structure which resembles a natural representation of file storage. This hierarchical structure consists of three layers to represent relationships among all blocks for stored resources. They are described as follows:

(1) Express Layer: offers an abstract representation of the stored resources;

(2) Service Layer: offers and manages cloud storage services; and

(3) Storage Layer: realizes data storage on many physical devices.

We make use of this simple hierarchy to organize data blocks from multiple CSP services into a large size file by shading their differences among these cloud storage systems. For example the Resource in Express Layer are split and stored into three CSPs, that are indicated by different colors, in Service Layer. In turn, each CSP fragments and stores the assigned data into the storage servers in Storage Layer. We also make use of colors to distinguish different CSPs. Moreover, we follow the logical order of the data blocks to organize the Storage Layer. This architecture also provides special functions for data storage and management, e.g., there may exist overlaps among data blocks (as shown in dashed boxes) and discontinuous blocks but these functions may increase the complexity of storage management.

III.LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things are satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

IV.SYSTEM ANALYSIS & DESIGN

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Modules:

Multi cloud storage

Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow some of their computer's processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks . the cloud user upload the data into multi cloud. cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a *multi-Cloud* .A multi-cloud allows clients to easily access his/her resources remotely through interfaces.

Cooperative PDP

Cooperative PDP (CPDP) schemes adopting zero-knowledge property and three-layered index hierarchy, respectively. In particular efficient method for selecting the optimal number of sectors in each block to minimize the computation costs of clients and storage service providers. Cooperative PDP (CPDP) scheme without compromising data privacy based on modern cryptographictechniqu

Data Integrity

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

Third Party Auditor

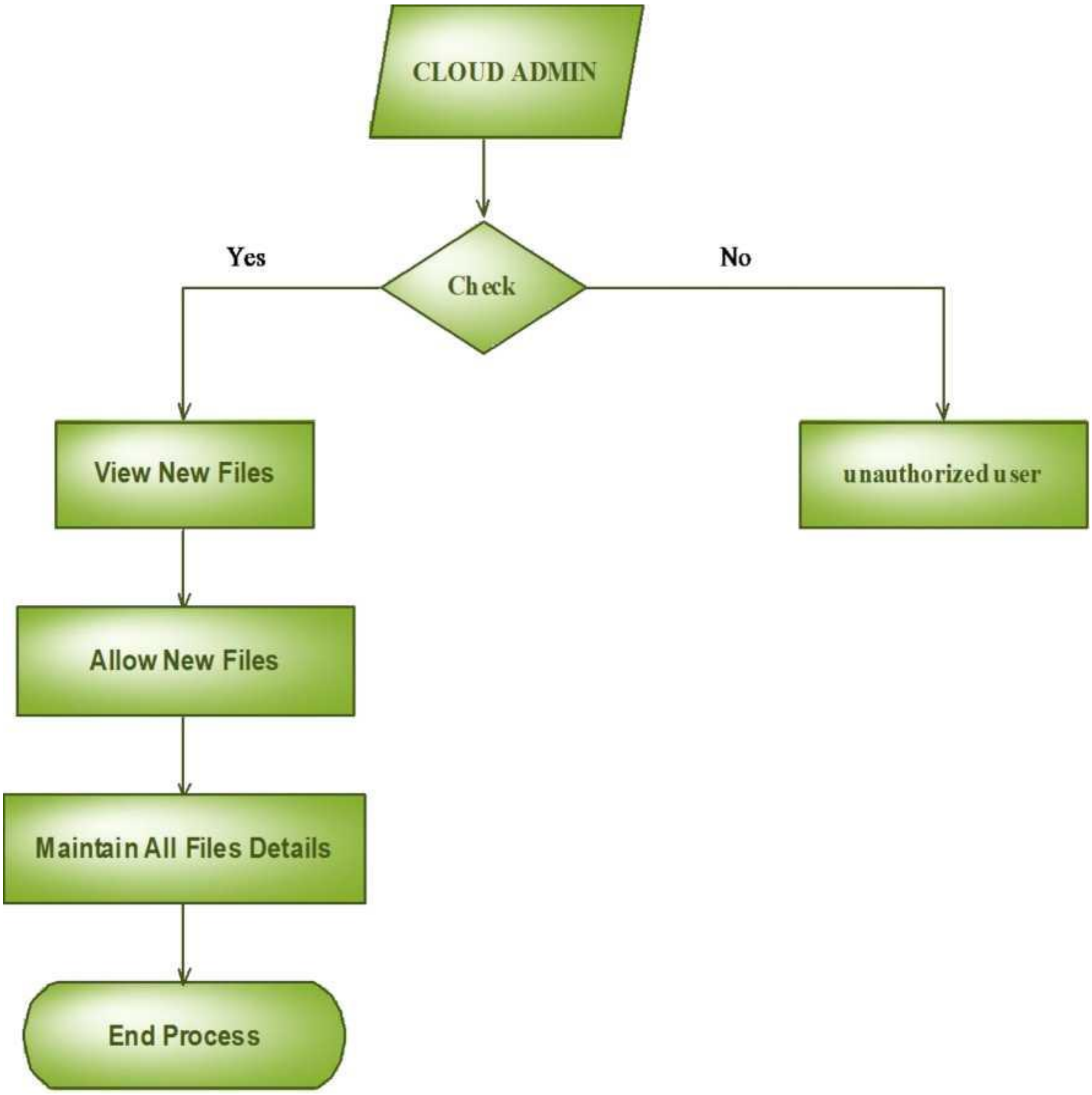
Trusted Third Party (TTP) who is trusted to store verification parameters and offe rpublic query services for these parameters. In our system the Trusted Third Party, view the user data blocks and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data blocks. If any odification tried by cloud owner a alert is send to the Trusted Third Party.

Cloud User

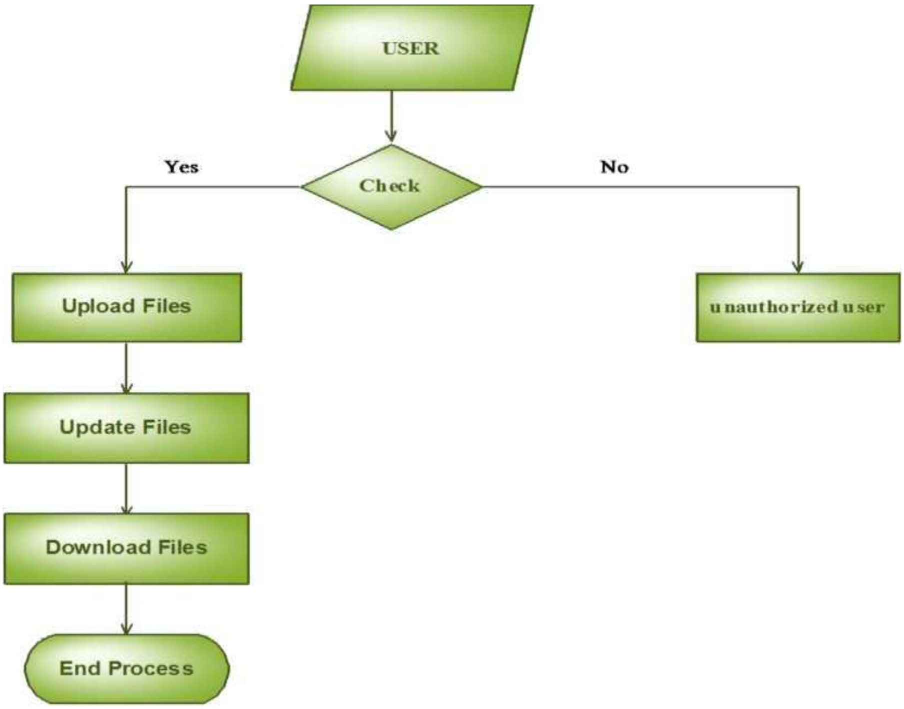
The Cloud User who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data.the User’s Data is converted into data blocks . the data blocks is uploaded to the cloud. The TPA view the data blocks and Uploaded in multi cloud. The user can update the uploaded data. If the user wants to download their files, the data’s in multi cloud is integrated and downloaded.

SYSTEM DESIGN

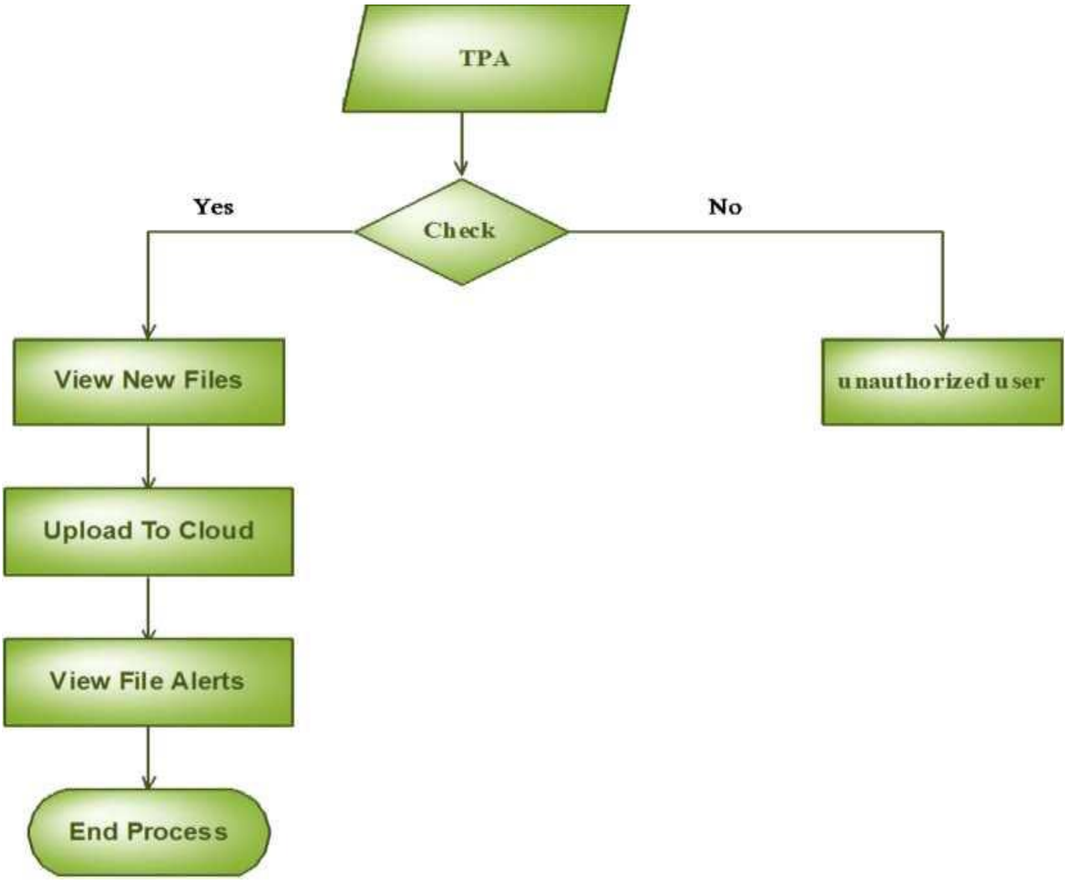
I)Admin



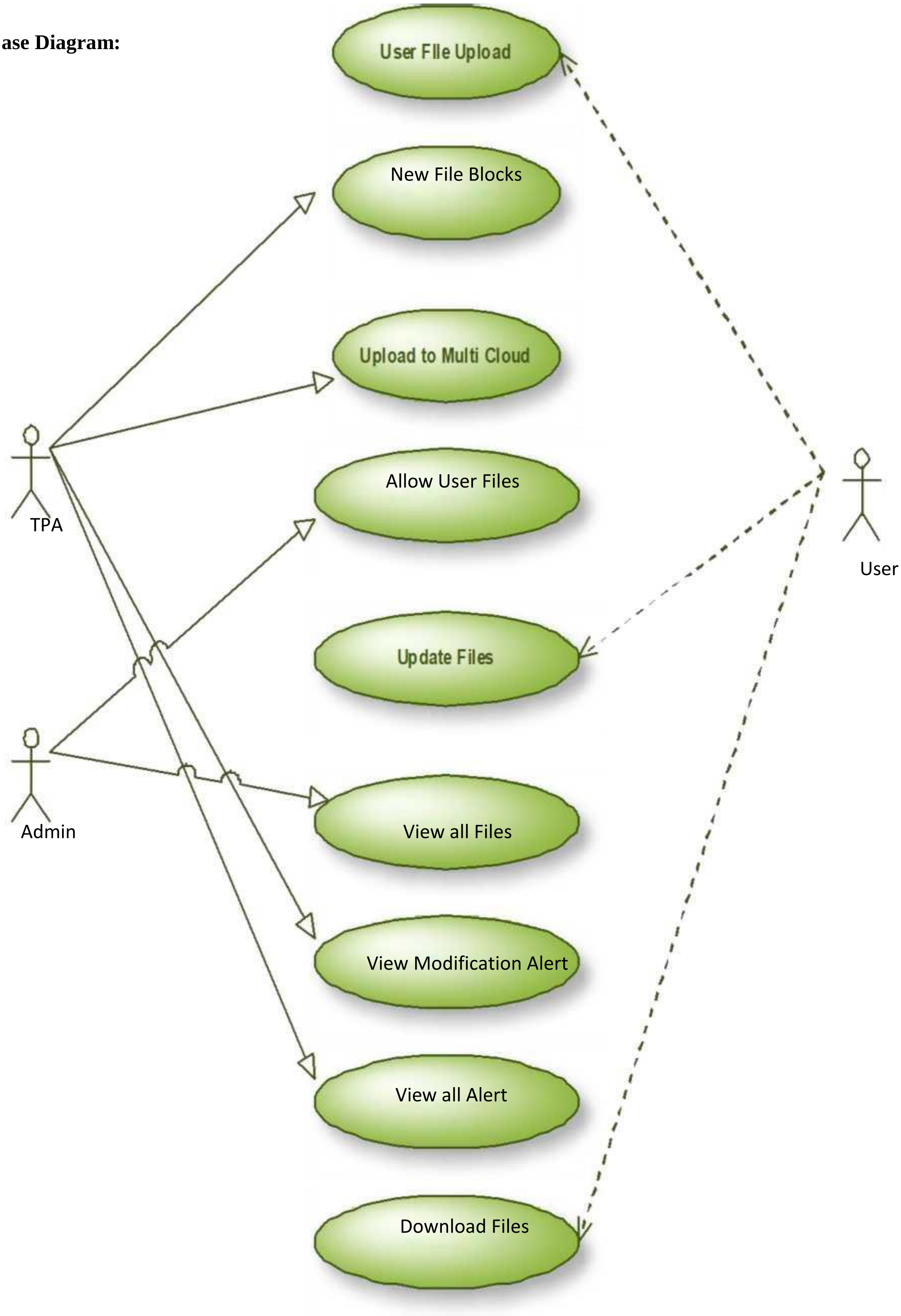
ii)User



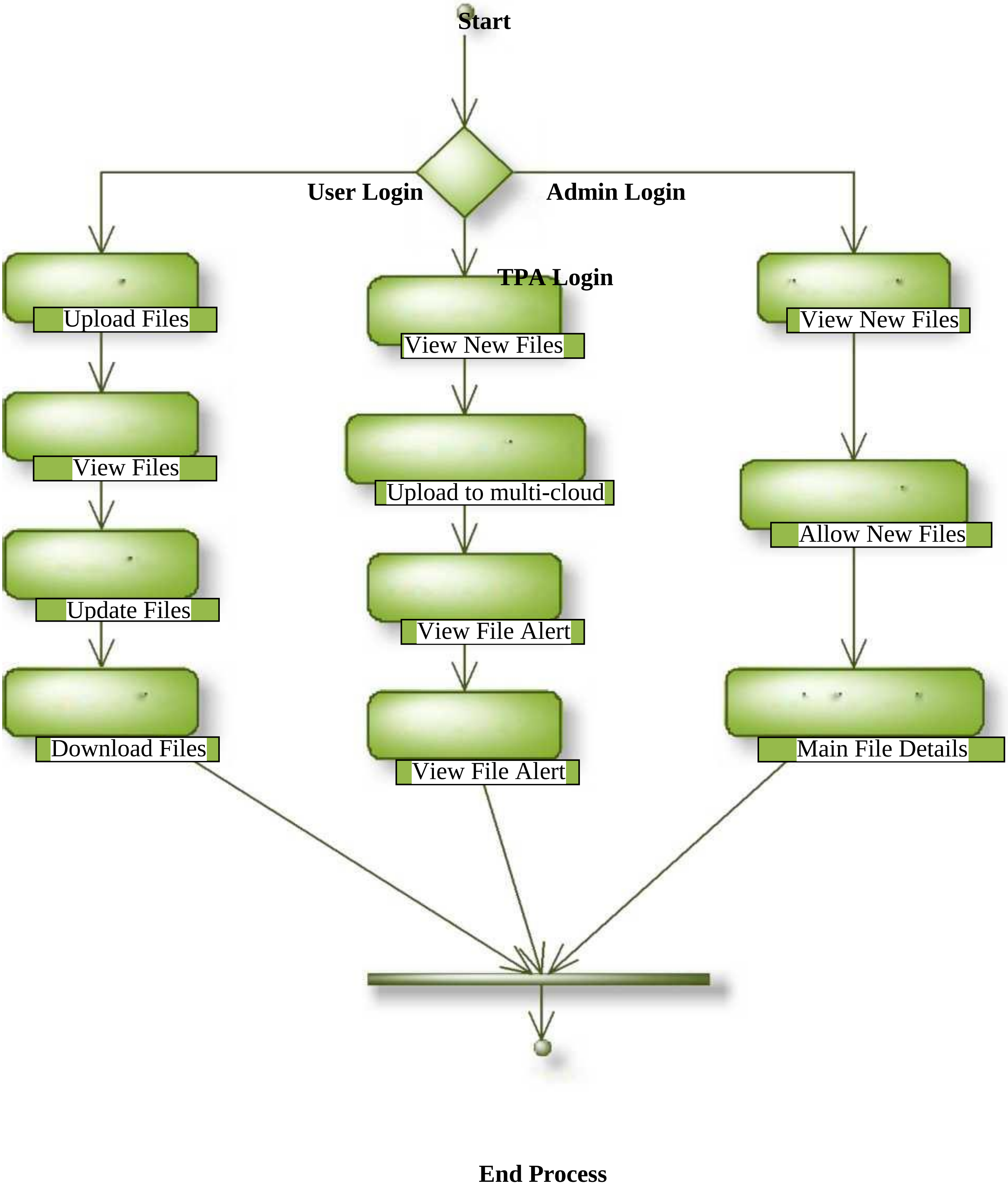
iii)Third Party Auditor:

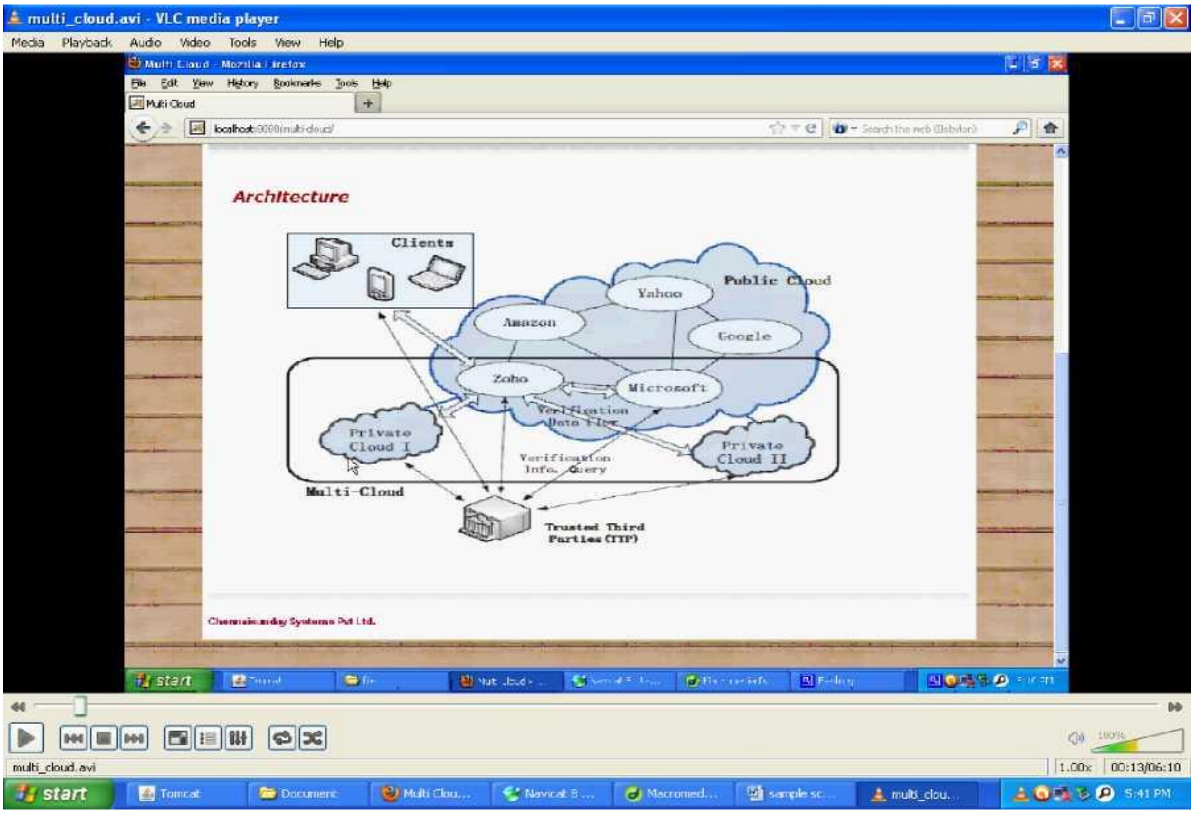


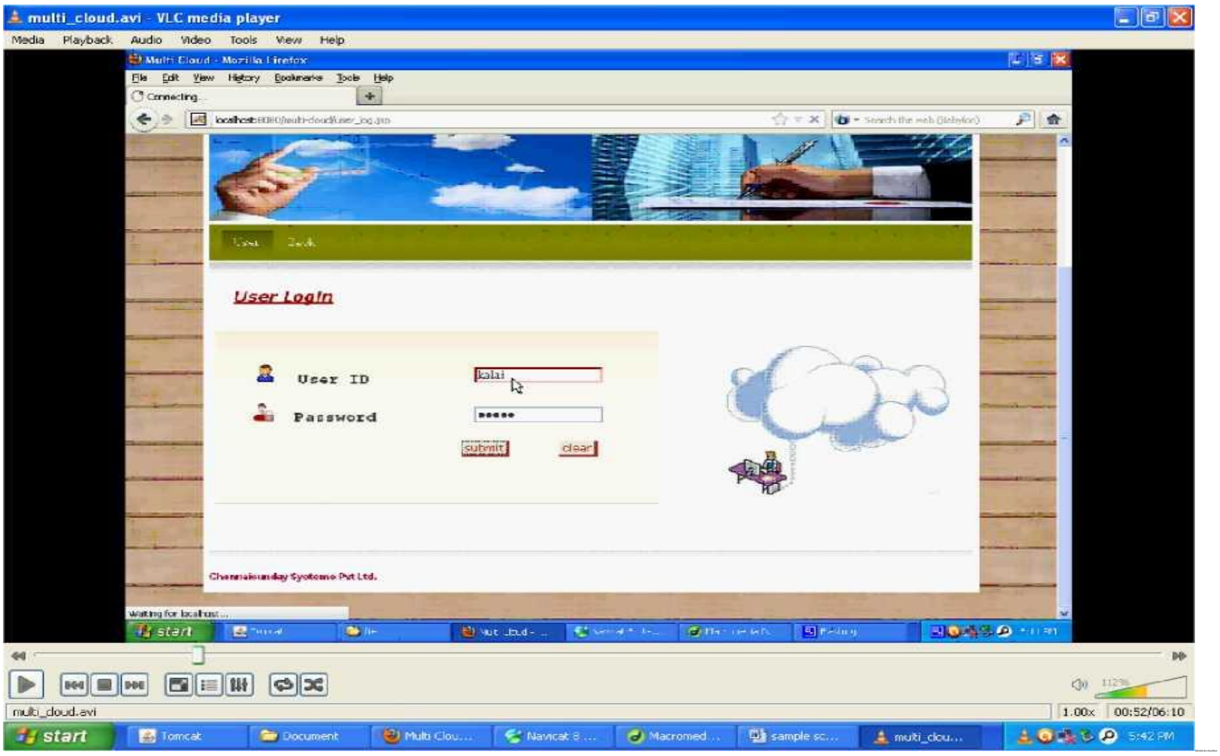
iv)User Case Diagram:



Activity Diagram:

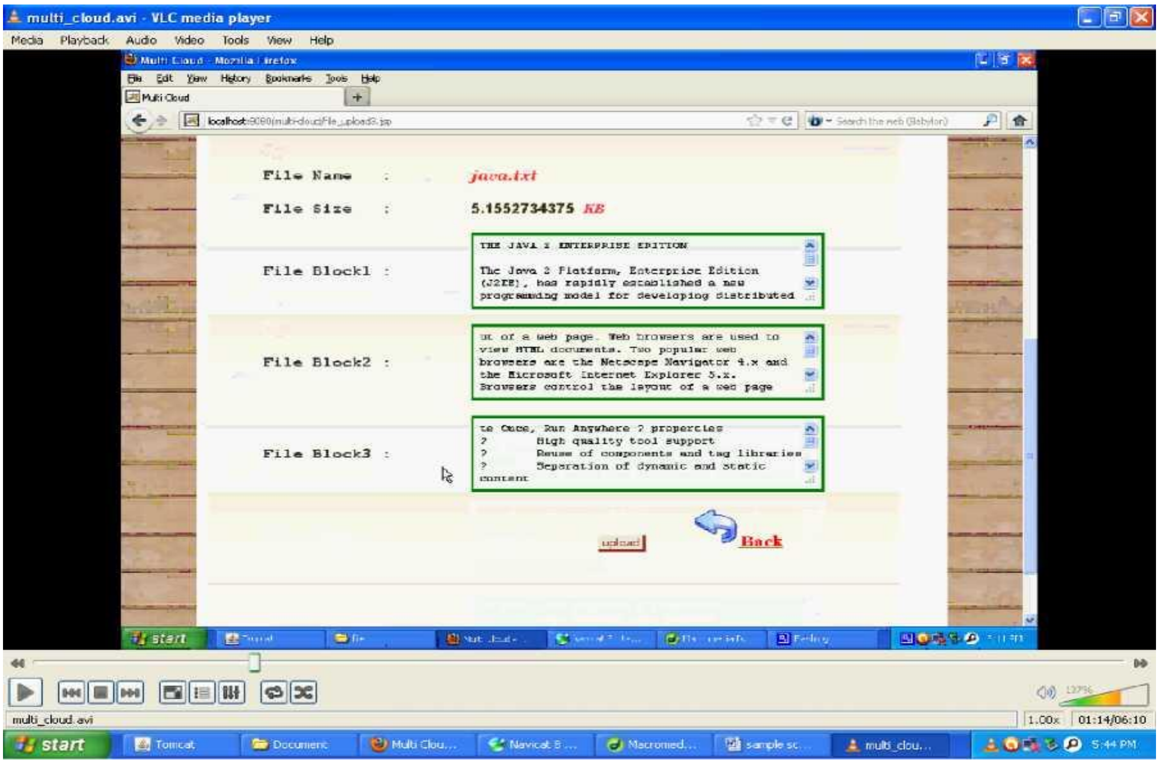





multi_cloud.avi - VLC media player
Media Playback Audio Video Tools View Help
Multi Cloud - Mozilla Firefox
Connecting...
User Login
submit
clear
Chennaisunday Systems Pvt Ltd.
Waiting for localhost...
start
multi_cloud.avi
1.00x
00:52/06:10
5:42 PM

User ID kalai

Password •••••


multi_cloud.avi - VLC media player
Media Playback Audio Video Tools View Help
Multi Cloud - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Multi Cloud
localhost:8080/multi-cloud/File_upload3.jsp
upload
Back
start
multi_cloud.avi
1.00x
01:14/06:10
Tomcat
Document
Multi Clou...
Navicat 8 ...
Macromed...
sample sc...
multi_clou...
5:44 PM

File Name : java.txt

File Size : 5.1552734375 KB

File Block1 :

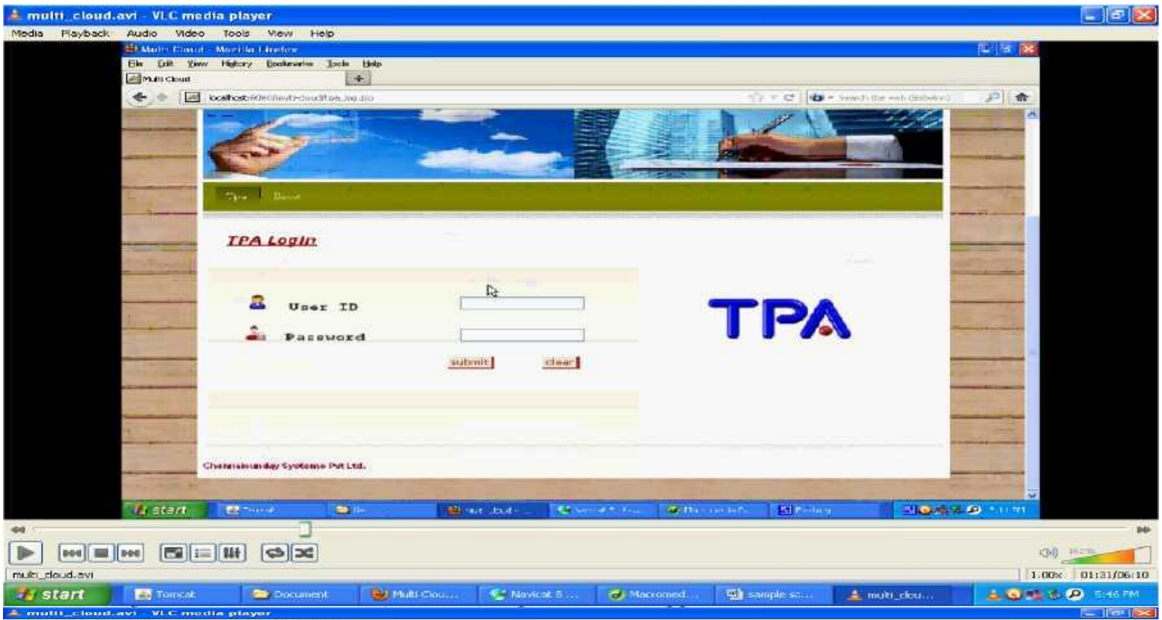
```
THE JAVA 2 ENTERPRISE EDITION

The Java 2 Platform, Enterprise Edition
(J2EE), has rapidly established a new
programming model for developing distributed
```

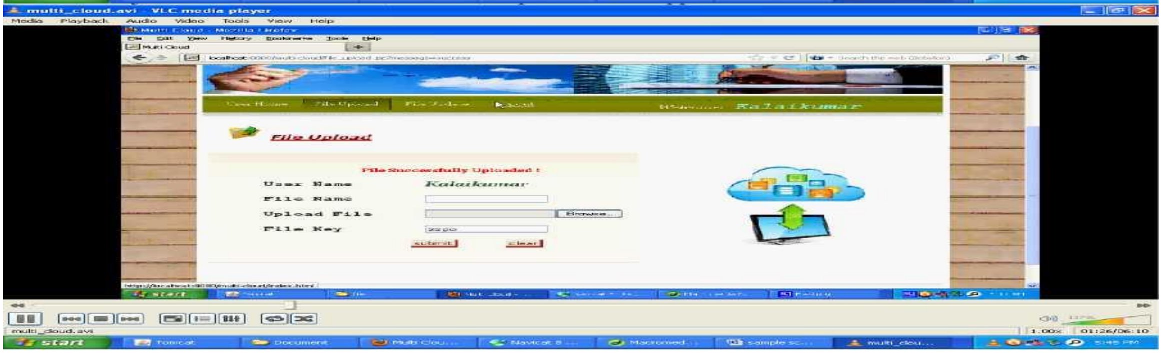
File Block2 :

```
ut of a web page. Web browsers are used to
view HTML documents. Two popular web
browsers are the Netscape Navigator 4.x and
the Microsoft Internet Explorer 5.x.
Browsers control the layout of a web page
```

File Block3 :

```
te Once, Run Anywhere ? properties
?       High quality tool support
?       Reuse of components and tag libraries
?       Separation of dynamic and static
content
```


multi_cloud.avi - VLC media player
Media Playback Audio Video Tools View Help
Multi Cloud - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Multi Cloud
TPA Login
User ID
Password
submit
clear
TPA
Chennaisunday Systems Pvt Ltd.
start
multi_cloud.avi
1.00x
01:31/06:10
Tomcat
Document
Multi Clou...
Navicat 8 ...
Macromed...
sample sc...
multi_clou...
5:46 PM


multi_cloud.avi - VLC media player
Media Playback Audio Video Tools View Help
Multi Cloud - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Multi Cloud
File Upload
Browse...
submit
clear
Tomcat
Document
Multi Clou...
Navicat 8 ...
Macromed...
sample sc...
multi_clou...

Welcome... Kalaikumar

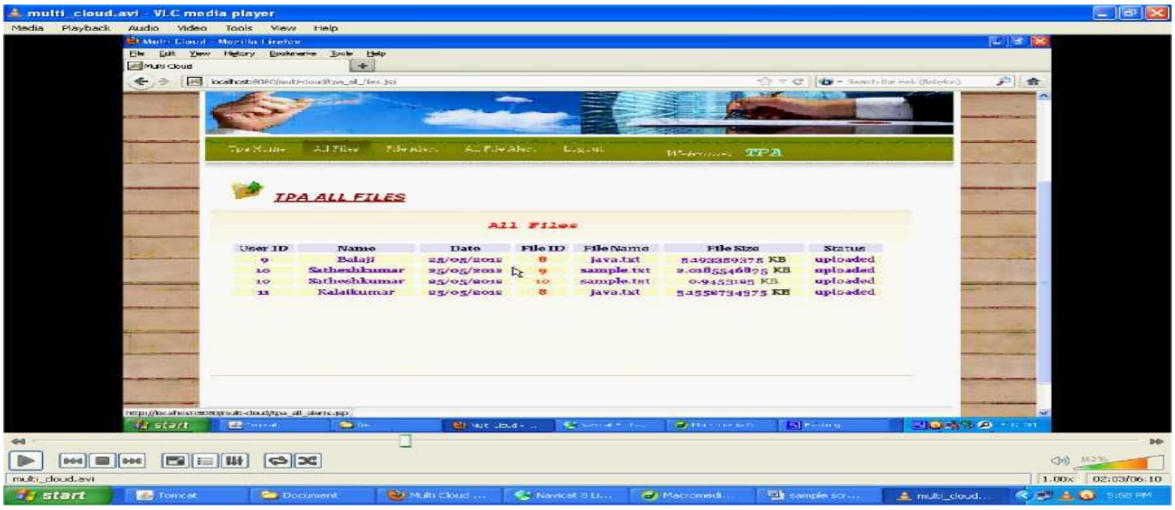
File Successfully Uploaded !

User Name Kalaikumar

File Name

Upload File

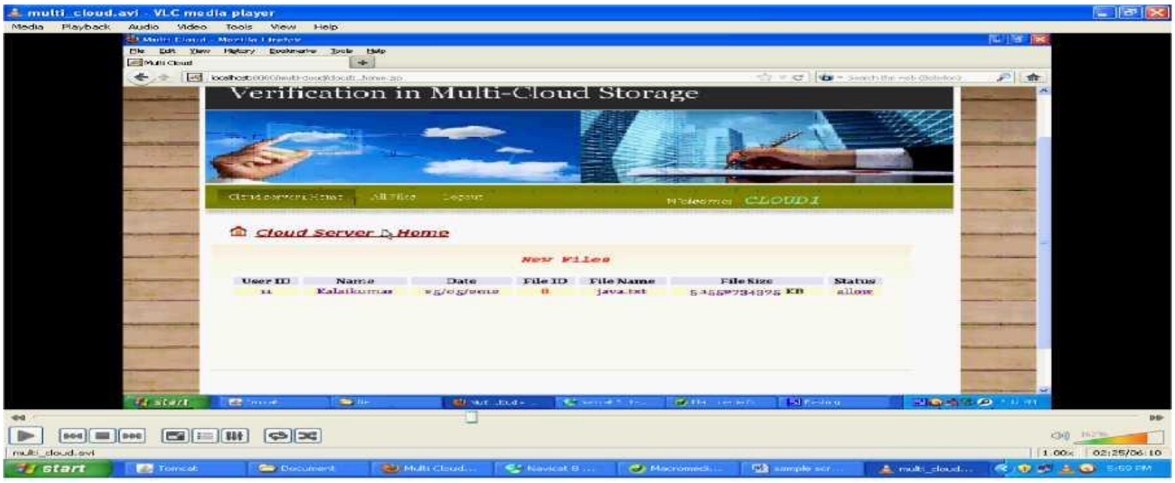
File Key zzpo


multi_cloud.avi - VLC media player
Media Playback Audio Video Tools View Help
Multi Cloud - Mozilla Firefox
localhost:8080/multi-cloud/tpa_all_files.jsp
Tpa Home
All Files
File Alert
All File Alert
Logout
Welcome TPA
start
Tomcat
Document
Multi Cloud ...
Navicat 8 Li...
Macromedi...
sample scr...
multi_cloud...

TPA ALL FILES

All Files

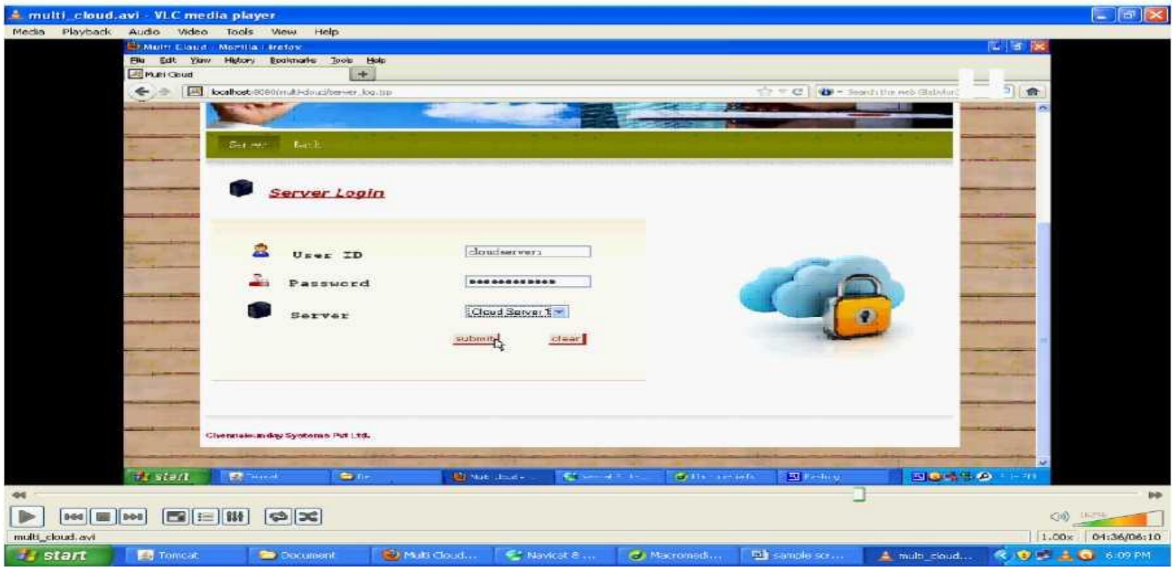
User ID	Name	Date	File ID	File Name	File Size	Status
9	Balaji	25/05/2012	8	java.txt	5.193359375 KB	uploaded
10	Satheeshkumar	25/05/2012	9	sample.txt	2.0185546875 KB	uploaded
10	Satheeshkumar	25/05/2012	10	sample.txt	0.9453125 KB	uploaded
11	Kalaikumar	25/05/2012	8	java.txt	5.1552734375 KB	uploaded


multi_cloud.avi - VLC media player
Media Playback Audio Video Tools View Help
Multi Cloud - Mozilla Firefox
Verification in Multi-Cloud Storage
Cloud server1 Home
All Files
Logout
Welcome CLOUD1
start
Tomcat
Document
Multi Cloud...
Navicat 8 ...
Macromedi...
sample scr...
multi_cloud...

Cloud Server Home

New Files

User ID	Name	Date	File ID	File Name	File Size	Status
11	Kalaikumar	25/05/2012	8	java.txt	5.1552734375 KB	allow


multi_cloud.avi - VLC media player
Media Playback Audio Video Tools View Help
Multi Cloud - Mozilla Firefox
localhost:8080/multi-cloud/server_log.jsp
Server
Back
submit
clear
start
Tomcat
Document
Multi Cloud...
Navicat 8 ...
Macromedi...
sample scr...
multi_cloud...

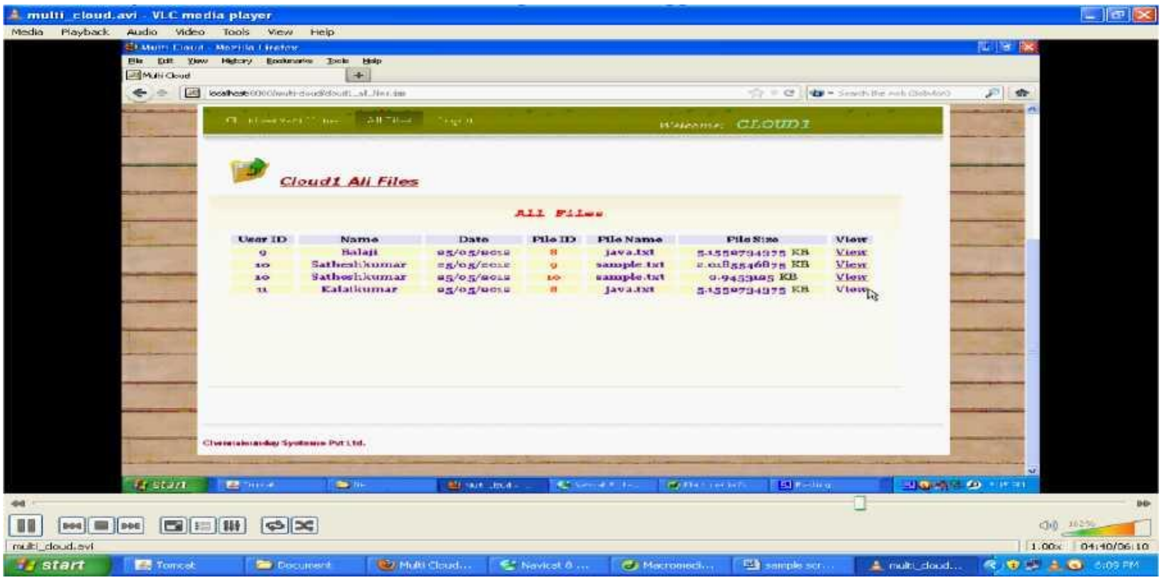
Server Login

User ID: cloudserver1

Password: ●●●●●●●●●●●●

Server: Cloud Server 1

Chennaisunday Systems Pvt Ltd.

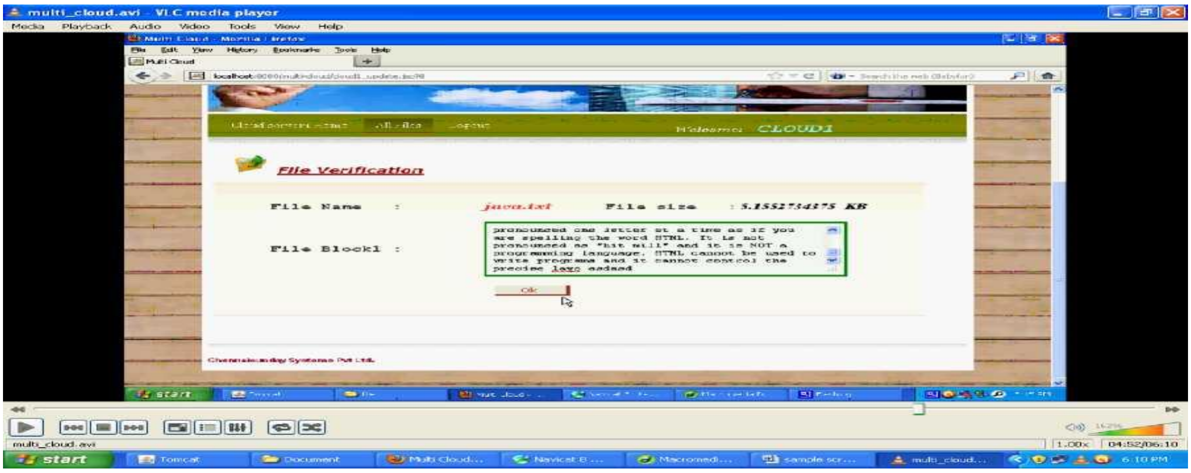


Cloud1 All Files

All Files

User ID	Name	Date	File ID	File Name	File Size	View
9	Balaji	05/05/2012	8	java.txt	5.1552734375 KB	View
10	Satheshkumar	05/05/2012	9	sample.txt	2.0185546875 KB	View
10	Satheshkumar	05/05/2012	10	sample.txt	0.9453125 KB	View
11	Kalaikumar	05/05/2012	8	java.txt	5.1552734375 KB	View

Chennaisunday Systems Pvt Ltd.

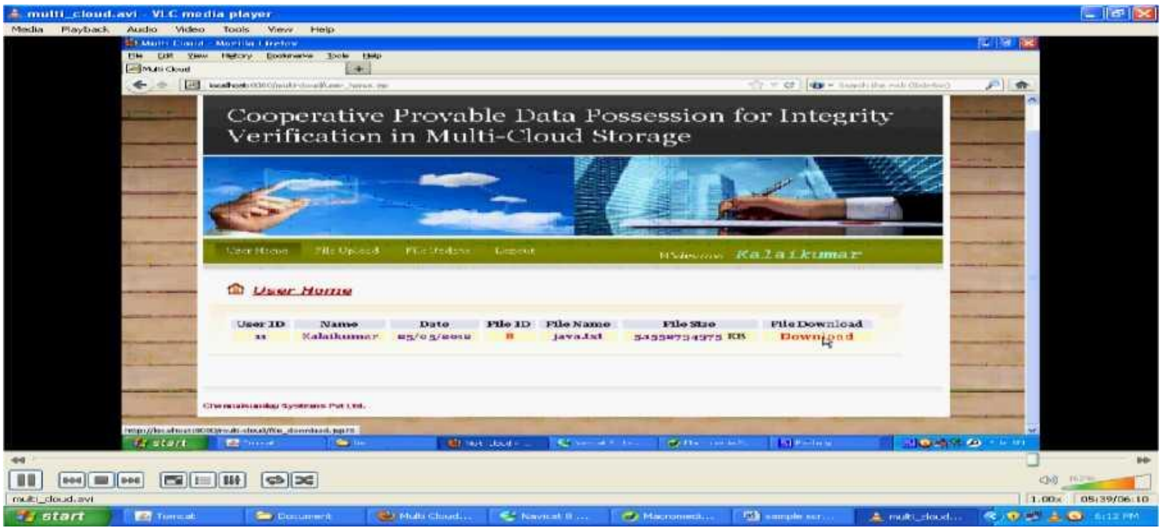


File Verification

File Name : java.txt File size : 5.1552734375 KB

File Block1 : pronounced one letter at a time as if you are spelling the word HTML. It is not pronounced as "hit mill" and it is NOT a programming language. HTML cannot be used to write programs and it cannot control the precise layo aadsad

Chennaisunday Systems Pvt Ltd.

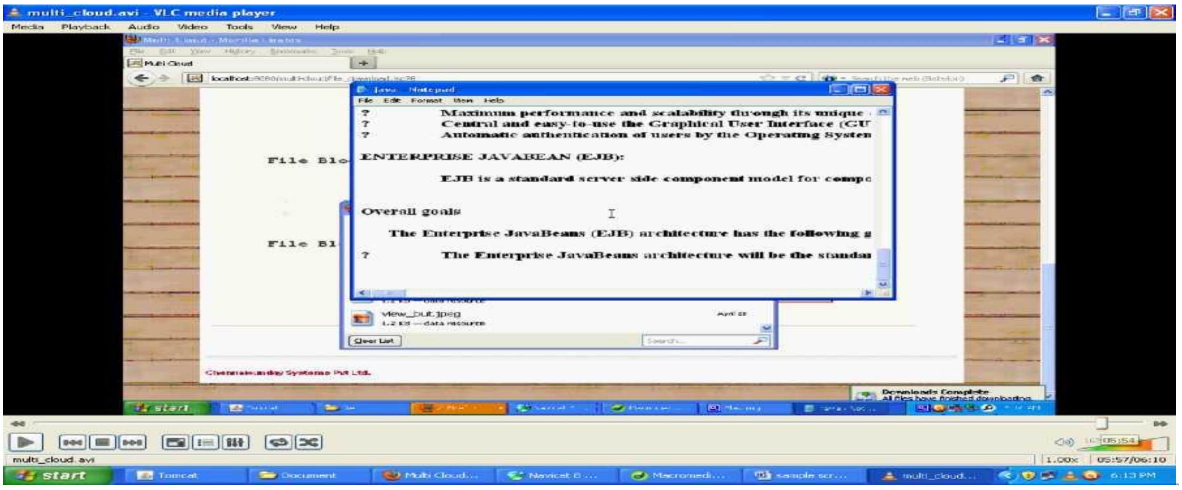


Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage

User Home

User ID	Name	Date	File ID	File Name	File Size	File Download
11	Kalaikumar	05/05/2012	8	java.txt	5.1552734375 KB	Download

Chennaisunday Systems Pvt Ltd.



? Maximum performance and scalability through its unique
? Central and easy-to-use the Graphical User Interface (GU
? Automatic authentication of users by the Operating Systen

ENTERPRISE JAVABEAN (EJB):

EJB is a standard server side component model for compo

Overall goals

The Enterprise JavaBeans (EJB) architecture has the following g

? The Enterprise JavaBeans architecture will be the standar

VI. CONCLUSION

We presented the construction of an efficient PDP scheme for distributed cloud storage. Based on homomorphic verifiable response and hash index hierarchy, we have proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers. We also showed that our scheme provided all security properties required by zero knowledge interactive proof system, so that it can resist various attacks even if it is deployed as a public audit service in clouds. Further more. we optimized the probabilistic query and periodic verification to improve the audit performance. Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems. As part of future work, we would extend our work to explore more effective CPDP constructions. Finally, it is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such a issue to provide the support of variable-length block verification.

VII. ACKNOWLEDGMENT

We would like to express my sincere thanks to my Guide for their consistence support and valuable suggestions.

VIII. REFERENCES

[1] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster, Virtual infrastructure management in private and hybrid clouds," IEEE Internet Computing, vol. 13, no. 5, pp. 14-22,2009.

[2] G. Ateniese, R. C. Bums, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598-609.

[3] A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584-597.

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm, 2008, pp. 1-10.

[5] C. C. Erway, A. K"upc, "u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213-222.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90-107.

[7] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355-370.

[8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Dynamic audit services for integrity verification of outsourced storages in clouds,” in SAC, W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550-1557.

[9] K. D. Bowers, A. Juels, and A. Oprea, “Hail: a high-availability and integrity layer for cloud storage,” in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 187-198.

[10] Y. Dodis, S. P. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” in TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109-127.

[11] L. Fortnow, J. Rompel, and M. Sipser, “On the power of multiprover interactive protocols,” in Theoretical Computer Science, 1988, pp. 156-161.

[12] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, “Collaborative integrity verification in hybrid clouds,” in IEEE Conference on the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom, Orlando, Florida, USA, October 15-18, 2011, pp. 197-206.

[13] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep., Feb 2009.

[14] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in Advances in Cryptology (CRYPTO’2001), vol. 2139 of LNCS, 2001, pp. 213-229.

[15] O. Goldreich, Foundations of Cryptography: Basic Tools. Cambridge University Press, 2001.