Ensuring Distributed Accountability for Data Sharing in the Cloud Network

Mr. Alhat Rajendra Y, Mr.Kedari Dattatray B, Mr.Sangale Bharat G, Prof. Nilesh N.Thorat
B.E computer engineering, Institute of Knowledge College of engineering, Pune 412 208

***Abstract* - Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. A major feature of the cloud services is that user's data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. To address this problem, in this paper, we propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users data in the cloud. In particular, we propose an object-centered approach that enables enclosing our logging mechanism together with users data and policies. We leverage the JAR programmable capabilities to both create a dynamic and traveling object and to ensure that any access to users data will trigger authentication and automated logging local to the JARs. To strengthen users control, we also provide distributed auditing mechanisms. We provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches.**

Keywords:
1. Cloud service provider (CSP)
2. Cloud Information Accountability (CIA)
3. Java Running Environment (JRE).
4. Identity-Based Encryption (IBE)
5. Proof-Carrying authentication (PCA)

1. INTRODUCTION

Cloud computing is a technology which uses internet and remote servers to store data and
Application. In cloud there is no need to install particular hardware, software on user machine, so user can get the required infrastructure on his machine in cheap charges/rates. Cloud computing is an infrastructure which provides useful, on demand network services to use various resources with less effort. Features of cloud computing are huge access of data, application, resources and hardware without installation of any software, user can access the data from any machine or anywhere in the world, business can get resource in one place, that means cloud computing provides scalability in on demand services to the business users. To date, there are a number of notable commercial and individual cloud computing services, including Amazon, Google, Microsoft, Yahoo, and Sales force. Clouds in general provide services at three different levels (IaaS, PaaS, and Saas) as follows, although some providers can choose to expose services at more than one level. Everyone kept their data in cloud, as
Everyone kept their data in cloud so it becomes public so security issue increases towards private data. Data usage in cloud is very large by users and businesses, so data security in cloud is very important issue to solve. Many users want to do business of his data through cloud, but users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying
about losing control of their own data. Under the Database as a service, this is having four parts which are as per mentioned below,

1. *Encryption and Decryption* - For security purpose of data stored in cloud, encryption
Seems to be perfect security solution.

2. *Key Management*- If encryption is necessary to store data in the cloud, encryption keys can′t be store there, so user requires key management.

3. *Authentication* - For accessing stored data in cloud by authorized users.

4. *Authorization* - Rights given to user as as cloud provider.

To solve the security issues in cloud; other user can't read the respective user's data
Without having access. Data owner should not bother about his data, and should not get fear about damage of his data by hacker; there is need of security mechanism which will track usage of data in the cloud. Accountability is necessary for monitoring data usage, in this all actions of users like sending of file are cryptographically linked to the server, that performs them and server maintain secured record of all the actions of past and server can use the past records to know the correctness of action. It also provides reliable information about usage of data and it observes all the records, so it helps in make trust, relationship and reputation. So accountability is for verification of authentication and authorization. It is powerful tool to check the authorization policies .Accountability describes authorization requirement for data

IJERT

usage policies. Accountability mechanisms, which rely on after the fact verification, are
an attractive means to enforce authorization policies.

There are 7 phases of accountability

1. Policy setting with data
2. Use of data by users
3. Logging
4. Merge logs
5. Error correctness in log
6. Auditing
7. Rectify and improvement.

2. EXISTING SYSTEM

To allay user′s concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in
distributed environments, are not suitable, due to the following features characterizing cloud environments.

2.1 Problem on Existing System

First data handling can be outsourced by the Direct cloud service provider(CSP) to the other entities in the cloud and these entities can also delegate the task to other and so on. Second entities are allowed to join and leave the cloud in a flexible manner. As a result data handling in the cloud goes through a complex and difficult.

3. PROPOSE SYSTEM

In this paper, we propose a novel highly decentralized information accountability framework to keep track of the actual usage of the user′s data in the cloud. In particular, we propose an object-centered approach that enables enclosing our logging mechanism together with user′s data and policies. We leverage the JAR programmable capabilities to both create a dynamic and traveling object, and to ensure that any access to user′s data will trigger authentication and automated logging local to the JARs. To strengthen user′s control, we also provide distributed auditing mechanisms. We provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches.

4. PROBLEM STATEMENT

We use cloud for uploading data owner's data. Data Owner who has uploaded his data on cloud he is not ensure about his data, so we have to store his data on the cloud by encrypting his data and then that data is wrapped into jar file along with the access policies and then that jar file is stored at the cloud. Then user can access the data. The Aim of our system is, in addition to the Ensuring Distributed Accountability for Data Sharing in the Cloud.

5. SYSTEM REQUIREMENT

5.1 H/W Specification

Processor	PIV 500 MHz to 3.0 GHz
RAM	1GB/above
Hard Disk	20 GB
Monitor	SVGA

5.2 S/W Requirement

Operating System	Windows XP/Windows Vista/Windows 7
Application Server	Tomcat5.0/6.X
Front End	HTML,JAVA,JSP
Data Base	MYSQL 5.0
Scripts	JAVA Script
Database Connectivity	JDBC

5.3 JAVA

Java is an object-oriented programming language developed by Sun Microsystems a company best known for its high end UNIX workstations. Java language was designed to be small, simple, and portable across platforms, operating systems, both at the source and at the binary level, which means that Java programs (applet and application) can run on any machine that has the Java virtual machine (JVM) installed.

5.4 J2EE

Java Platform, Enterprise Edition or Java EE is a widely used platform for server programming in the Java programming language. The Java platform (Enterprise Edition) differs from the Java Standard Edition Platform (Java SE) in that it adds libraries which provide functionality to deploy fault-tolerant, distributed, multi-tier Java software, based largely on modular components running on an application server.

5.5 Tomcat Sever

A Number of servlet containers are available today. The most popular one & the one recognized as the official servlet/JSP container is Tomcat originally designed by Sun Micro Systems Tomcat by itself is a web server this means that you can use Tomcat to service HTTP request for servlets as well as static files(HTML, image files & so on). Tomcat 5.5 uses the Jasper 2 JSP Engine to implement the Java Server Pages 2.0 specification.

IJERT

- **JSP Custom Tag Pooling** - The java objects instantiated for JSP Custom Tags can now be pooled and reused. This significantly boosts the performance of JSP pages which use custom tags.
- **Background JSP compilation** - If you make a change to a JSP page which had already been compiled Jasper 2 can recompile that page in the background. The previously compiled JSP page will still be available to serve requests. Once the new page has been compiled successfully it will replace the old page. This helps improve availability of your JSP pages on a production server.

5.4 Development Tools

Eclipse Tool is an integrated development environment (IDE) for visually designing, constructing, testing, and deploying Web services, portals, and Java (J2EE) applications.

5.4.1 Eclipse

In computer programming Eclipse does a multi-language integrated development environment (IDE) comprise a base workspace and an extensible plug-in system for customizing the environment? It is written mostly in Java It can be used to develop applications in Java and, by means of various plug-ins, other programming language including Ada, C, C++, COBOL, Fortran, Haskell, JavaScript, Lasso, Perl, PHP, Python, Ruby, Scala, Clojure, Groovy, Sch eme, and Erlang. It can also be used to develop packages for the software Mathematical. Development environments include the Eclipse Java development tools (JDT) for Java and Scala, Eclipse CDT for C/C++ and Eclipse PDT for PHP, among others. The initial codebase originated from IBM Visual Age. The Eclipse software development kit (SDK), which includes the Java development tools, is meant for Java developers. Users can extend its abilities by installing plug-ins written for the Eclipse Platform, such as development toolkits for other programming languages, and can write and contribute their own plug-in modules. Released under the terms of the Eclipse Public License, Eclipse SDK is free and open source software (although it is incompatible with the GNU General Public License). It was one of the first IDEs to run under GNU Class path and it runs without problems under Iced Tea.

6. NON FUNCTIONAL REQUIREMENT

Performance Requirements

Performance details the way the system will perform for users.

Think about:

What is the response time for reports, queries, and updates?

What is the total number of user sessions open for the entire application?

What is the total number of concurrent sessions that can be opened by a single user?

What is the total amount of idle time before the user session is forced to terminate?

Safety Requirements:

For these requirements we are using antivirus in our machine to machine crash. Also we are
going to use login registration for the new user.

Software Quality Attributes:

Our system will be user friendly, good performance and time consuming.

Security Requirements:

We are going to use login registration for the new user

7. PRODUCT PERSPECTIVE

Here you need to explain the how our project will be looking, so you can explain here System Flow of the project.

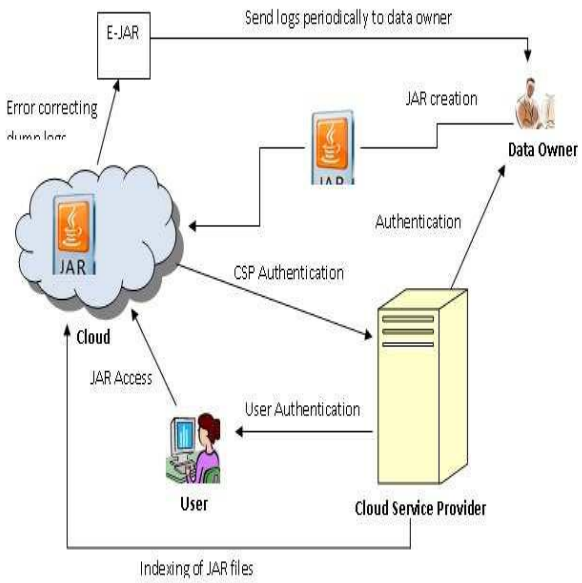


Figure System Diagrams

Project Summary

1. Jar Creation using RSA key.
2. Making Jar Access.
3. Making Authentication request to the cloud service provider.

IJERT

4. In the Authentication request cloud service provider will give authentication response.
5. Then encrypted logging will be done.
6. After that Certificate Revocation List (CRL) verification will be done with certificate authorities.

8. LITERATURE SURVEY

Survey 1

1. **Paper Title:** M. Atallah, and S. Prabhakar, Rights Protection for Relational Data, Proc. ACM SIGMOD, pp. 98-109, 2003.

Paper Discussion
Protecting rights over relational data is of ever increasing interest, especially considering areas where sensitive, valuable content is to be outsourced. A good example is a data mining application, where data is sold in pieces to parties specialized in mining it. Differ- ent avenues for rights protection are available, each with its own advantages and drawbacks. Enforcement by legal means is usually ineffective in preventing theft of copyrighted works, unless augmented by a digital counter-part, for example watermarking.
Recent research of the authors introduces the issue of digital watermarking for generic number sets.

Advantages:
(a) This paper concentrates on areas where sensitive and valuable content lies.
(b) Prevents data loss nearly about 50 Percent and above.

Disadvantages:
(a) Uses watermarking technique makes data partially visible.
(b) Fails to detest guilty agent.
(c) System is unable to protect 100 percent Data

Survey 1

1. **Paper Title:** Achieving K-Anonymity Privacy Protection Using Generalization and
Suppression, 2002

Paper Discussion This paper provides a formal presentation of combining generalization and suppression to achieve k-anonymity. Generalization involves replacing (or recoding) a value with a less specie but semantically consistent value. Suppression involves not releasing a value at all. The Preferred Minimal Generalization Algorithm (MinGen), which is a theoretical algorithm presented herein, combines these
Techniques to provide k-anonymity protection with minimal distortion.

Advantages:

(a) Uses k-anonymity algorithm.

(b) Leads to minimal distortion.

Disadvantages:

(a) Fails to provide adequate protection.

(b) Does not detect the guilty agent.

10. WORKFLOW OF SYSTEM

Usecase Diagram

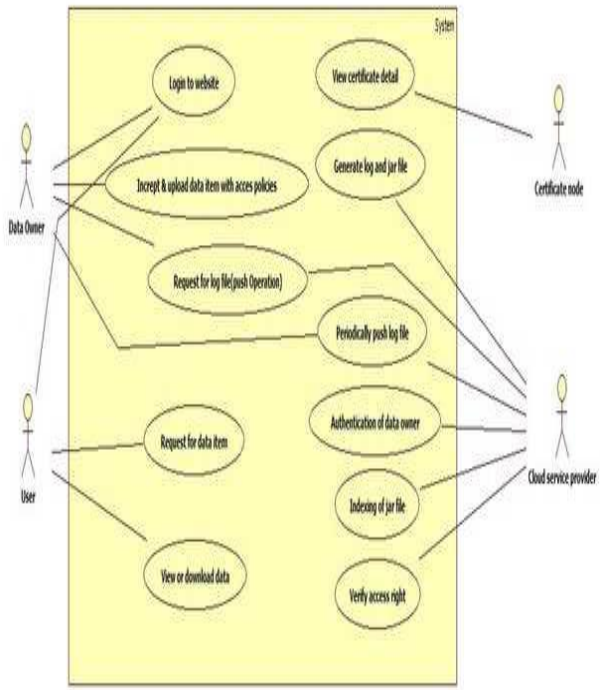
Data Owner Login to website, incrept and upload data item with access policy.

User Logins and Verify user into the system. Then request for data and view or download data

Certificate node View certificate detail.

Cloud service provider Periodically push log file to the data owner.Authentication
of data owner.Indexing of jar file. Verify access right

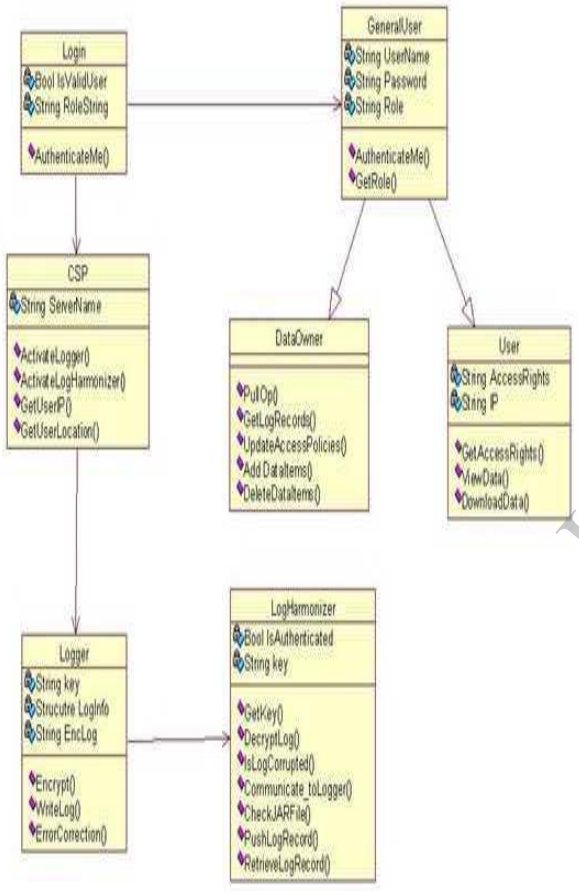
IJERT



Usecase Diagram

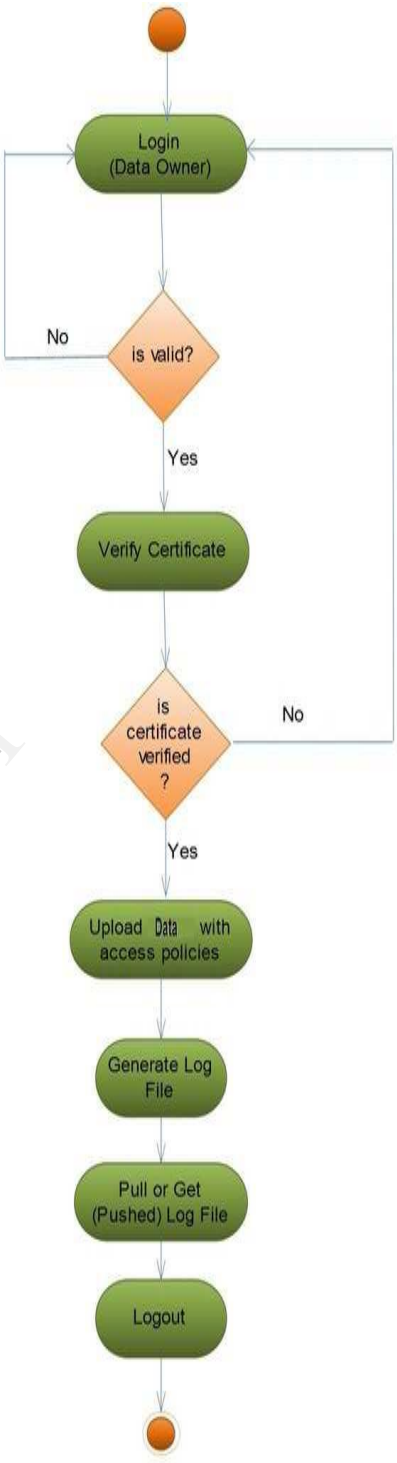
Class Diagram

There are following four main classes inside the system;
1. Login
2. GeneralUser
3. Cloud service provider(csp).
4. dataowner
5. User
6. Logger
7. LogHarmonizer



Class Diagram

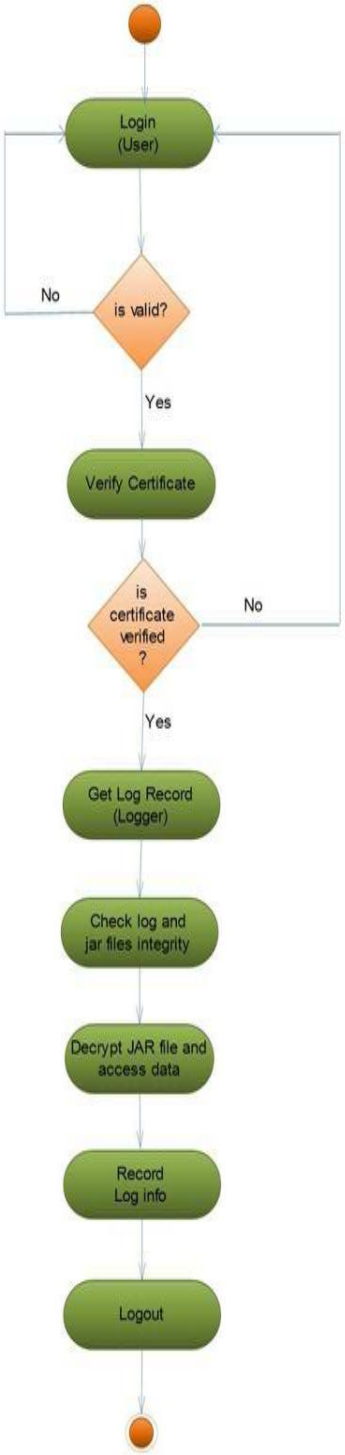
Activity Diagram for Data Owner



Activity Diagram for Data Owner

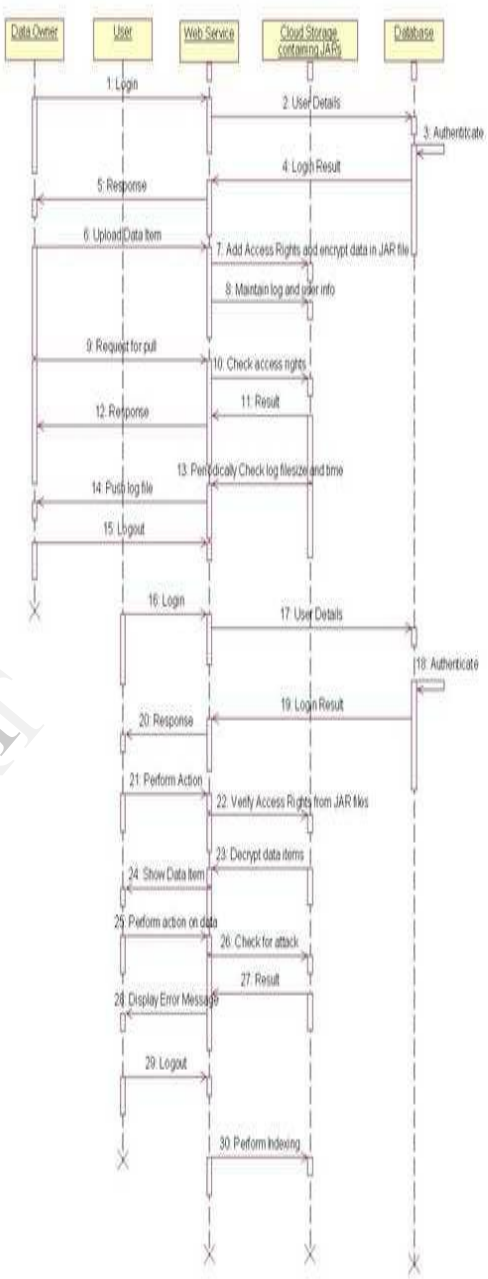
IJERT

Activity Diagram for User



Activity Diagram for User

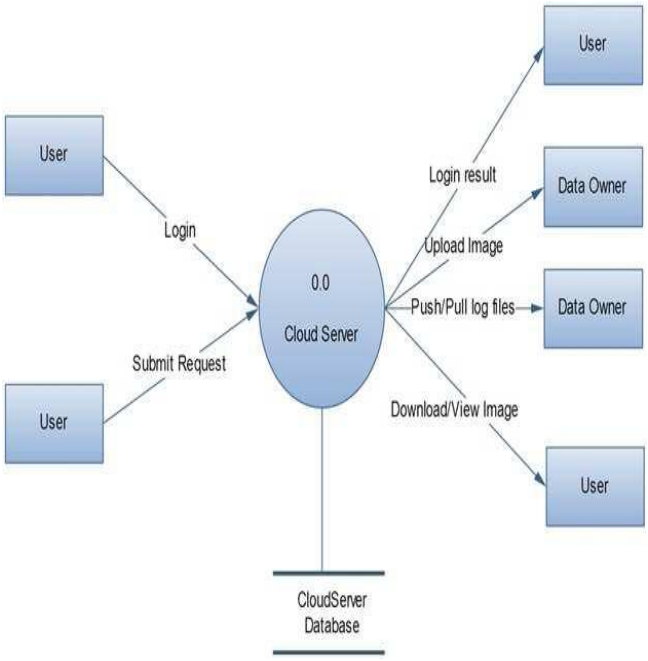
Sequence Diagram



Sequence diagram

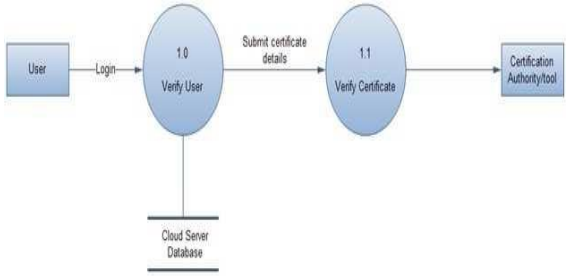
IJERT

DFD Level 0



DFD Level 0

DFD Level 1



DFD Level 1

11. CONCLUSION AND FUTURE SCOPE

Conclusion

We proposed innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism. Our approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge.

In the long term, we plan to design a comprehensive and more generic object-oriented approach to facilitate autonomous protection of traveling content. We would like to support a variety of security policies, like indexing policies for text files, usage control for executables, and generic accountability and provenance controls.

Future Scope

In the future, we plan to refine our approach to verify the integrity of the JRE and the authentication of JARs. For example, we will investigate whether it is possible to leverage the notion of a secure JVM being developed by IBM. This research is aimed at providing software tamper resistance to Java applications. In the long term, we plan to design a comprehensive and more generic object-oriented approach to facilitate autonomous protection of traveling content. We would like to support a variety of security policies, like indexing policies for text files, usage control for executables, and generic accountability and provenance Controls.

IJERT

References

[1] Suk-Ju Kang, Member, Ieee, Sung In Cho, Student Member, Ieee, Sungjoo Yoo, Member, Ieee, And Young Hwan Kim, Member,"*Scene Change Detection Using Multiple Histograms For Motion-Compensated Frame Rate Up-Conversion*", Ieee Journal Of Display Technology, Vol. 8, No. 3, March 2012

[2] Hyun-Seokmin, Jae Young Choi, Wesley De Neve, And Yongman Ro, Seniormember, Ieee ,"*Near-Duplicate Video Clip Detection Using Model-Free Semantic Concept Detection And Adaptive Semantic Distance Measurement*", Ieee Transactions On Circuits And Systems For Video Technology, Vol. 22, No. 8, August 2012

[3] Partha Pratim Mohanta, Sanjoy Kumar Saha, Member, Ieee, And Bhabatosh Chanda,"*A Model-Based Shot Boundary Detection Technique Using Frame Transition Parameters*" , Ieee Transactions On Multimedia, Vol.14, No. 1, February 2012.

[4] Abdelati Malek Amel, Ben Abdelali Abdessalem And Mtibaa Abdellatif,"*Video Shot Boundary Detection Using Motion Activity Descriptor*", Journal Of Telecommunications, Volume 2, Issue 1, April 2010.

[5] Yuzhen Niu And Feng Liu," *What Makes A Professional Video? A Computational Aesthetics Approach"*, Ieee Transactions On Circuits And Systems For Video Technology, Vol. 22, No. 7, July 2012.

[6] Bo Han, Yichuan Hu, Guijin Wang, Weiguo

[7] Soo-Chang Pei And Fan Chen , "*Semantic Scenes Detection And Classification In Sports Videos*", Ieee Transactions On Circuits And Systems For Video Technology, Vol. 22, No. 7, July 2012

[8] Wu, And Takayuki Yoshigahara,
" *Enhanced Sports Video Shot Boundary Detection Based On Middle Level Features And A Unified Model*", Ieee Transactions On Consumer Electronics, Vol. 53, No. 3, August 2007

IJERT