Providing Key Exposure to Enabling the Cloud Data Service Security

P.Bhargavi*, D.Murali, M.V. Ramesh

Brahmaiah College of Engineering, Nellore, INDIA

A B S T R A C T

With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments.

Keywords: Cloud computing, data security, lightweight data sharing scheme

1. Introduction

Distributed storage evaluating is seen as an essential administration to check the honesty of the data publically cloud. Current evaluating conventions territory unit all bolstered the customer's mystery key for examining is totally secure. In any case, such suspicion may not persistently be charge, because of the probably frail feeling that all is well with the world and additionally low security settings at the shopper. We formalize the definition and along these lines the security model of examining convention with key-presentation versatility and propose such a convention. In our style, we tend to utilize the parallel tree structure and in this manner prearrange traversal strategy to refresh the key keys for the shopper.

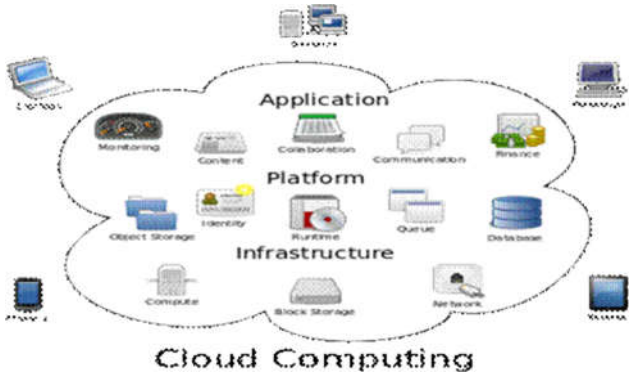

Fig: 1.1 Cloud Computing Architecture.

* *Corresponding author.*
E-mail address: pbhargavirevathi@gmail.com

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

Characteristics and Services Models: The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

2. System Analysis

2.1 Existing System

Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the cipher text, and non-revoked users periodically received private keys for each time period from the key authority. Boldyreva, Goyal and Kumar introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users. Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme. Chen et al. constructed a RIBE scheme from lattices.

2.2 Proposed System

It seems that the concept of revocable identity-based encryption (RIBE) might be a promising approach that fulfills the aforementioned security requirements for data sharing. RIBE features a mechanism that enables a sender to append the current time period to the cipher text such that the receiver can decrypt the cipher text only under the condition that he/she is not revoked at that time period. A RIBE-based data sharing system works as follows:

3. Preliminary Investigation

3.1 A break in the clouds: towards a cloud definition

This paper discusses the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20 definitions have been studied allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches.

3.2 A vision for socially motivated resource sharing

Online relationships in social networks are often based on real world relationships and can therefore be used to infer a level of trust between users. We propose leveraging these relationships to form a dynamic "Social Cloud," thereby enabling users to share heterogeneous resources within the context of a social network. In addition, the inherent socially corrective mechanisms (incentives, disincentives) can be used to enable a cloud-based framework for long term sharing with lower privacy concerns and security overheads than are present in traditional cloud environment(TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. We propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently.

4. System Study

4.1 Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential. Three key considerations involved in the feasibility analysis are

4.2 Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited.

5. System Specification

Hardware System Configuration:-

- Processor - Pentium–IV
- RAM - 4 GB (min)
- Hard Disk - 40 GB
- Keyboard - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

Software Requirements:

- Operating System — Windows XP/7
- Coding Language — Java/J2EE
- Tool — NetBeans 7.2.1
- Back End — MySQL

6. System Design And Development

6.1 Input Design

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.

6.2 Output Design

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing

The key client server idea is that client as user is essentially insulated from the physical location and formats of the data needs for their application. With the proper middleware, a client input from or report can transparently access and manipulate both local database on the client machine and remote databases on one or more servers. An added bonus is the client server opens the door to multi-vendor database access indulging heterogeneous table joins.

6.3 User Interface Design and Front End

The entire user interface is planned to be developed in browser specific environment with a touch of Intranet-Based Architecture for achieving the Distributed Concept. The browser specific components are designed by using the HTML standards, and the dynamism of the designed by concentrating on the constructs of the Java Server Pages.

Overall Description

Fig: 6.4.1 Picture showing the development process of JAVA Program

Java programming uses to produce byte codes and executes them. The first box indicates that the Java source code is located i n a. Java file that is processed with a Java compiler called java. The Java compiler produces a file called a. class file, which contains the byte code. The Class file is then loaded across the network or loaded locally on your machine into the execution environment is the Java virtual machine, which interprets and executes the byte code.

Java Architecture: Java architecture provides a portable, robust, high performing environment for development. Java provides portability by compiling the byte codes for the Java Virtual Machine, which is then interpreted on each platform by the run-time environment. Java is a dynamic system, able to load code when needed from a machine in the same room or across the planet.

Compilation of code: When you compile the code, the Java compiler creates machine code (called byte code) for a hypothetical machine called Java Virtual Machine (JVM).Java was designed to be easy for the Professional programmer to learn and to use effectively. If you are an experienced C++ programmer, learning Java will be even easier. Because Java inherits the C/C++ syntax and many of the object oriented features of C++. Most of the confusing concepts from C++ are either left out of Java or implemented in a cleaner, more approachable manner. In Java there are a small number of clearly defined ways to accomplish a given task.

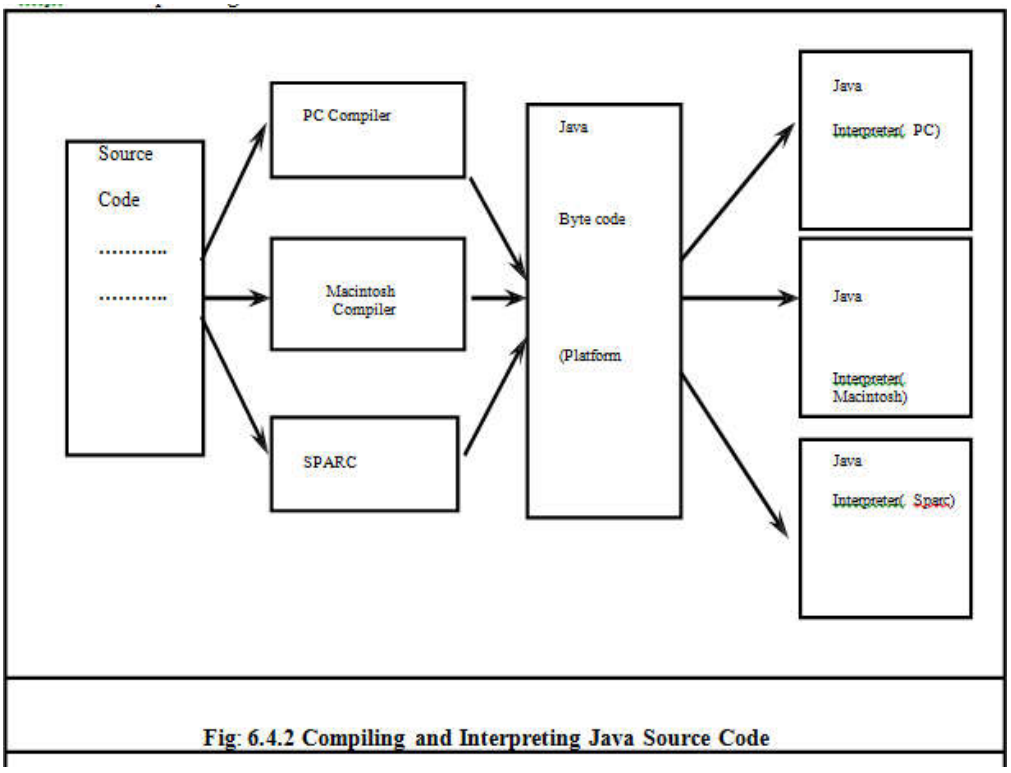

Fig: 6.4.2 Compiling and Interpreting Java Source Code

almost as easy to learn as HTML, and JavaScript statement can be including in HTML document by enclosing the Statement between a pair of scripting tags.

<SCRIPTS>..</SCRIPT>.

<SCRIPT LANGUAGE = “JavaScript”>

JavaScript statements

</SCRIPT>

Here are a few things we can do with JavaScript:

- Validate the contents of a form and make calculations.
- Add scrolling or changing messages to the Browser’s status line.
- Animate images or rotate images that change when we move the mouse over them.
- Detect the browser in use and display different content for different browsers.
- Detect installed plug-ins and notify the user if a plug-in is required.

Basic HTML Tags:

<!-- -->	Specifies comments
<A>…….</A>	Creates hypertext links
<B>…….</B>	Formats text as bold
<BIG>…….</BIG>	Formats text in large font.
<BODY>…</BODY>	Contains all tags and text in the HTML document
<CENTER>...</CENTER>	Creates text
<DD>…</DD>	Definition of a term
<DL>...</DL>	Creates definition list
<FONT>…</FONT>	Formats text with a particular font
<FORM>...</FORM>	Encloses a fill-out form
<FRAME>...</FRAME>	Defines a particular frame in a set of frames
<H#>…</H#>	Creates headings of different levels
<HEAD>...</HEAD>	Contains tags that specify information about a document
<HR>...</HR>	Creates a horizontal rule
<HTML>…</HTML>	Contains all other HTML tags
<META>...</META>	Provides meta-information about a document
<SCRIPT>…</SCRIPT>	Contains client-side or server-side script
<TABLE>…</TABLE>	Creates a table
<TD>…</TD>	Indicates table data in a table
<TR>…</TR>	Designates a table row
<TH>…</TH>	Creates a heading in a table

Advantages:

- A HTML document is small and hence easy to send over the net. It is small because it does not include formatted information.
- HTML is platform independent.
- HTML tags are not case-sensitive.

JDBC connectivity:

The JDBC provides database-independent connectivity between the J2EE platform and a wide range of tabular data sources. JDBC technology allows an Application Component Provider to:

Perform connection and authentication to a database server

- Manager transactions
- Move SQL statements to a database engine for preprocessing and execution
- Execute stored procedures
- Inspect and modify the results from Select statements.

Tomcat 6.0 web server

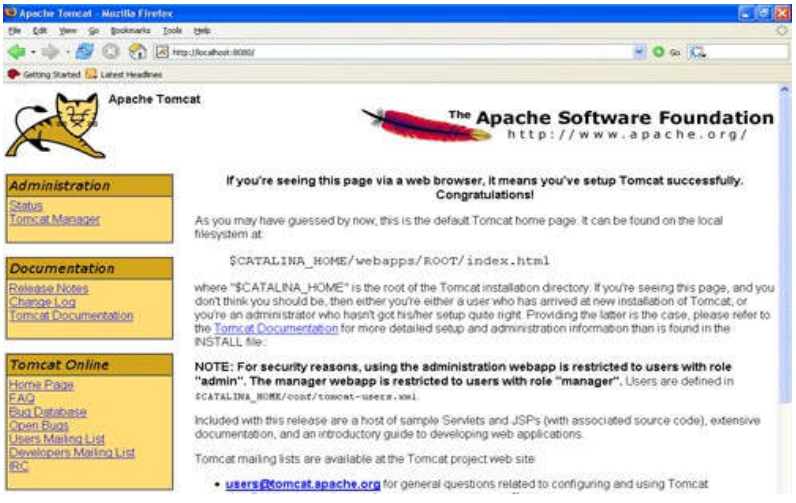

Fig 6.5 Tomcat 6.0 web server

Tomcat is an open source web server developed by Apache Group. Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and Java Server Pages technologies. The Java Servlet and Java Server Pages specifications are developed by Sun under the Java Community Process. Web Servers like Apache Tomcat support only web components while an application server supports web components as well as business components (BEAs WebLogic, is one of the popular application server).To develop a web application with jsp/servlet install any web server like JRun, Tomcat etc to run your application.

7. System Design

7.1 Architecture Diagram:

We evaluated our algorithms using synthetic, measured and real topology. The framework comprises of modules and risk modules.

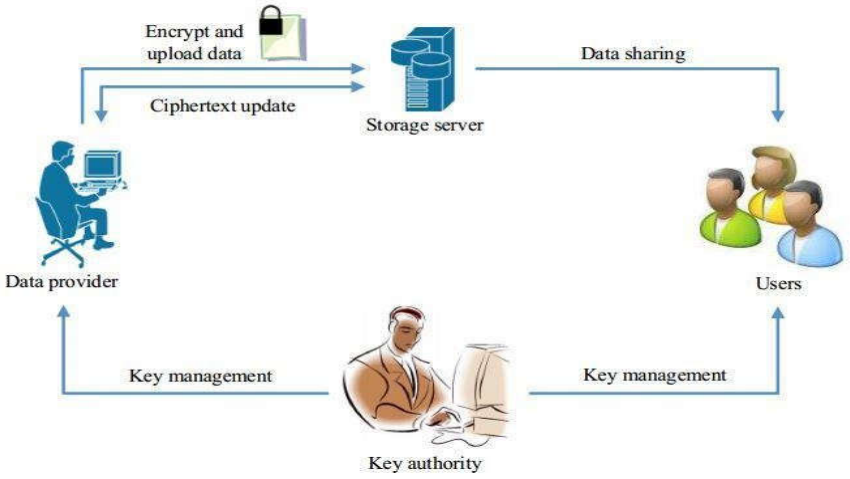

Fig: 7.1 System Architecture. Module

Explanations:

7.1.1 Public key & Secret key: In this Module open mystery's created for confirmation for the client to deliver the client determination work. The mystery's the private produced for each hopeful all through enrollment.

7.1.2 File storage: The File Storage module the record keeps for the any use of the purchaser and consequently the docu ment is given the decision to take a gander at and exchange upheld the timeframe keys.

7.1.3 Generate period of time key: The timeframe mystery's produced such to utilize the document or to perform task on that u pheld time.

7.1.4 Indexing of the files: The combination of the documents is such determined to take a gander at the exchange or to think of key or to exchange or play out the activity on the record.

7.1.5 View and transfer files: The documents will be seen or exchange upheld the time of time key confirmation of the client.

7.1.6 Auditor public key: The examiner open mystery's produced to play out all the activity with one key on every one of the modules.

7.2 DATA FLOW DIAGRAM:

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system. The data flow diagram (DFD) is one of the most important modeling tools. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from
input to output.

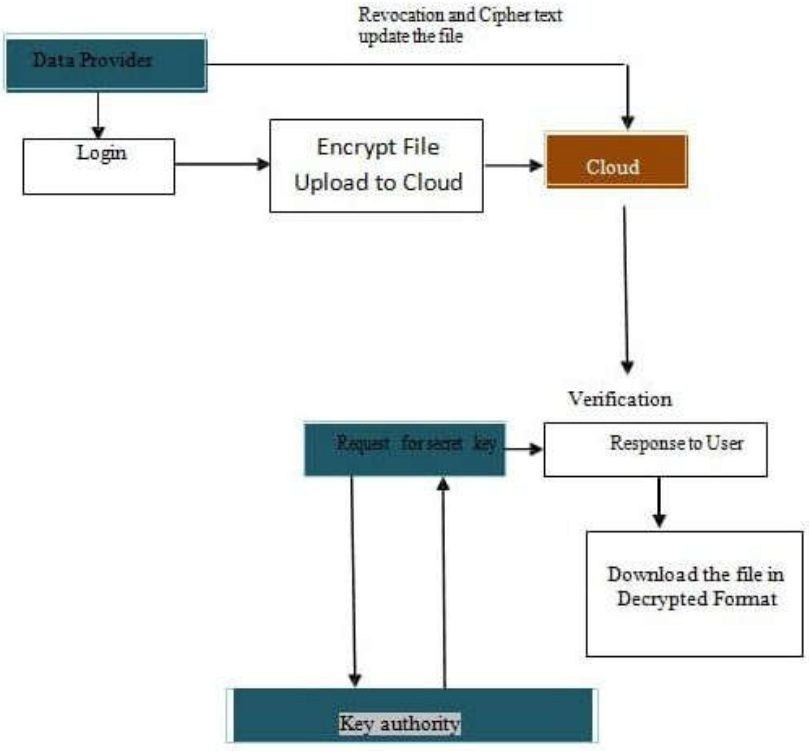

Fig: 7.2 Data Flow Diagram

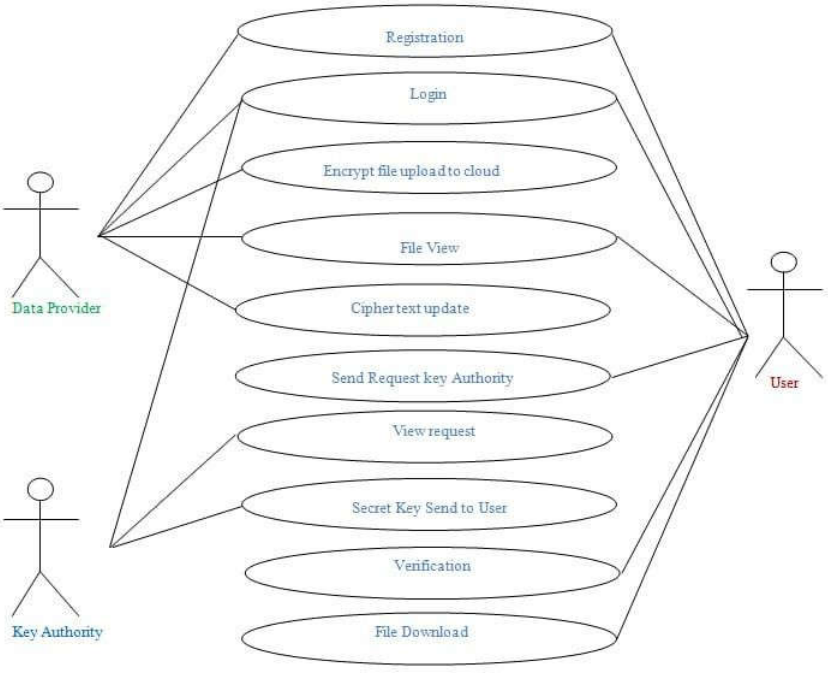

Fig: 7.3 Use Case Diagram

8. Implementation

System Construction Module:
In the first module, we develop the proposed system with the required entities for the evaluation of the proposed model. The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the cipher text of the shared data to the cloud server. When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding cipher text.

Data Provider:
In this module, we develop the Data Provider module. The data provider module is developed such that the new users will Signup initially and then Login for authentication. The data provider module provides the option of uploading the file to the Cloud Server. The process of File Uploading to the cloud Server is undergone with Identity-based encryption format. Data Provider will check the progress status of the file upload by him/her. Data Provider provided with the features of Revocation and cipher text update the file.

Cloud User:
In this module, we develop the Cloud User module. The Cloud user module is developed such that the new users will Signup initially and then Login for authentication. The Cloud user is provided with the option of file search. Then cloud user feature is added up for send the Request to Auditor for the File access. After getting decrypt key from the Auditor, he/she can access to the File.

Key Authority (Auditor)
Auditor Will Login on the Auditor's page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt. After complete the process, the Auditor logout the session.

9. System Testing

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration.

Functional test Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.
Invalid Input : identified classes of invalid input must be rejected.
Functions : identified functions must be exercised.
Output : identified classes of application outputs must be exercised. Systems/Procedures: interfacing systems or procedures must be invoked.

9.1 Unit Testing:

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format

- No duplicate entries should be allowed
- All links should take the user to the correct page.

9.2 Integration Testing

Fig 9.1 Home Page.

Description: This is the Home page, in the Home page admin, data owner, user, and about the project. Then home page can be di splayed the total Home menu icons.

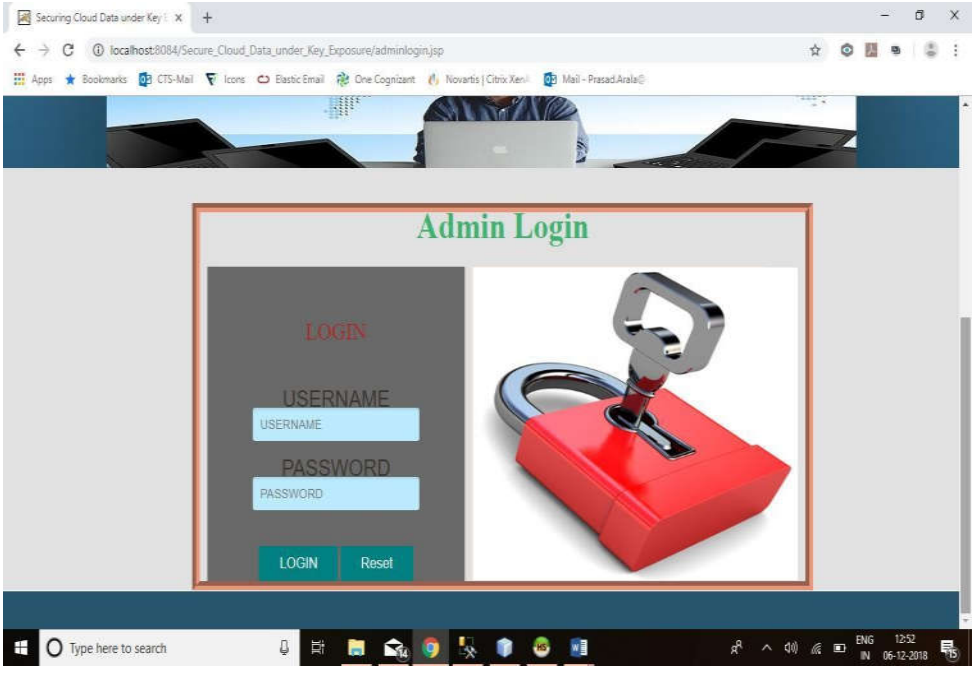

Fig 9.2 Admin Login Page

Description: This is the Admin Login page, in the admin page admin can login and check the user details and data owner details and file request details

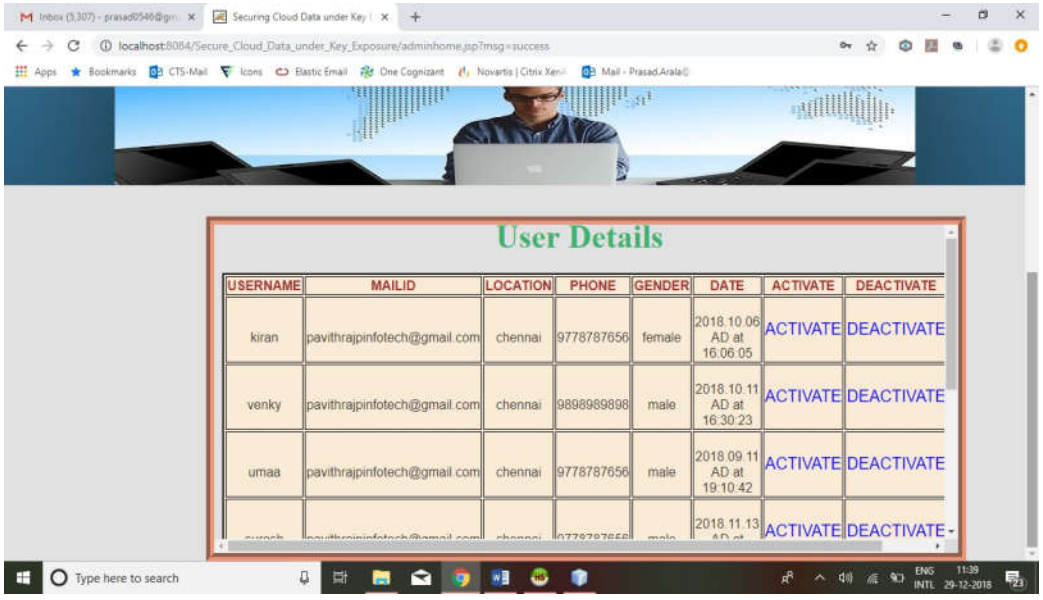

Fig 9.3 Admin – User Details

Description: This is the Admin Home page, in the admin page admin can login and check the user details and data owner details and file request details

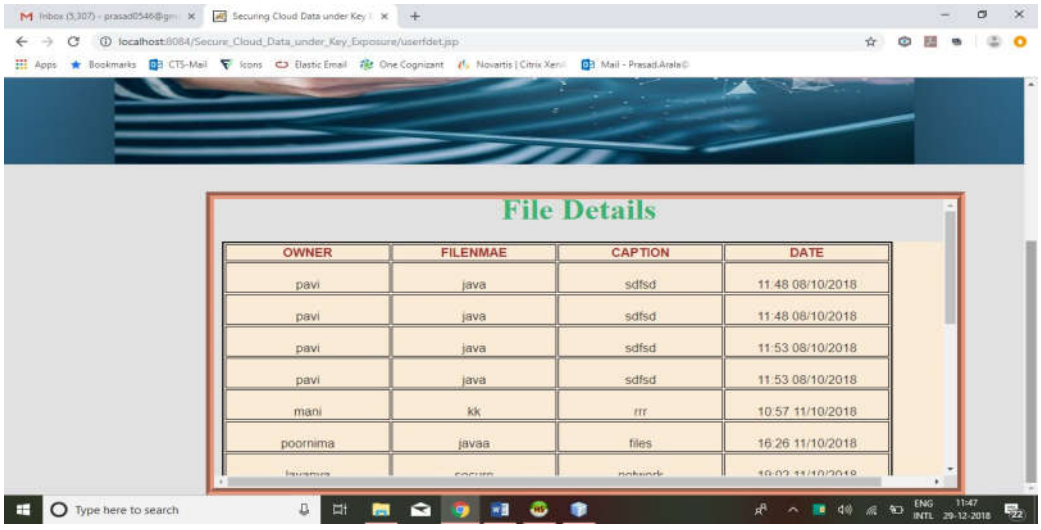

Fig 9.4 User – File Details

Description: This is the User page, in the user page user can login and check the user details and download or view file details.

10. Conclusion

We formalize the definition thus the assurance model of inspecting convention with key- presentation versatility and propose such a convention. In our vogue, we've a slant to utilize the parallel tree structure thus pre-arrange traversal procedure to refresh the key keys for the supporter. We tend to together build up a particular appraiser development to help the forward security thus the property of square less certainty. The security verification thus the execution examination demonstrates that our anticipated convention is secure and prudent. All through this paper, we've a slant to represent considerable authority in this new part of distributed storage evaluating.

REFERENCES

[1] J. Carter and K. Rajamani, "Designing energy-efficient servers and data centers,"Computer, vol. 43, no. 7, pp. 76–78, Jul. 2010.

[2] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[3] Cloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[4] Azure. (2014) Azure storage service. Available: http://www.windowsazure.com/

[5] Amazon. (2014) Amazon simple storage service (Amazon s3).[Online]. Available: http://aws.amazon.com/s3/

[6] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[7] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp.362–375, 2013.

[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

[12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003.

[15] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

[16] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.

[17] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Advances in Cryptology– CRYPTO 2001. Springer, 2001, pp. 41–62.

[18] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in Advances in Cryptology–EUROCRYPT 2003. Springer, 2003, pp. 272–293.