A

MINI PROJECT REPORT ON

Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud

Submitted in partial fulfilment of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

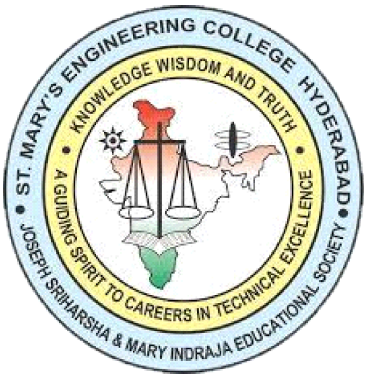
Submitted by

M. Sai Darshan Balaji	**[18BH1A05F8]**
M. Jaya Krishna Sai	**[18BH1A05F9]**
T. Amarnath Goud	**[18BH1A05E2]**
Md Ali Ahmad Khurshid	**[18BH1A05J7]**

Under the guidance of

Dr. V. SAMBASIVA RAO **M.Tech., Ph.D.**

CSE DEPARTMENT



ST. MARY'S ENGINEERING COLLEGE

(AFFILIATED TO JNTUH, APPROVED BY AICTE, ACCREDITED BY NAAC)

NEAR RAMOJIFILM CITY, DESHMUKHI (V), YADADRI, BHUVANGIRI DIST-508284

[2018-2022]

DECLARATION

A project titled, **"SECURE DATA GROUP SHARING AND DISSEMINATION WITH ATTRIBUTE AND TIME CONDITIONS IN PUBLIC CLOUD"** submitted to the Department of **Computer Science and Engineering**, **St. Mary's Engineering College** in fulfilment of degree for the award of Bachelor of technology, is a bonafide work done by us. No part of this report is copied from Internet and wherever the portion is taken; the same has been duly referred in the text. The reported results are based on the project work entirely done by us and not copied from any other sources. Also, we declare that the matter embedded in this report has not been submitted by us in full or partially therefore the award of any degree of any other institution or university previously.

By

M. Sai Darshan Balaji [18BH1A05F8]

M. Jaya Krishna Sai [18BH1A05F9]

T. Amarnath Goud [18BH1A05E2]

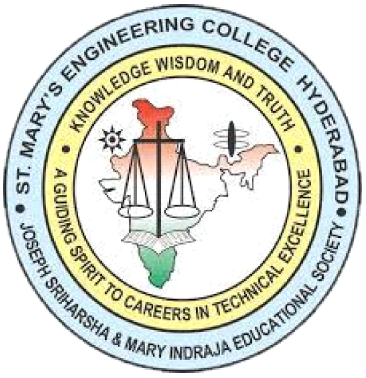
Md. Ali Ahmad Khurshid [18BH1A05J7]

ST. MARY'S ENGINEERING COLLEGE

(AFFILIATED TO JNTUH, APPROVED BY AICTE, ACCREDITED BY NAAC)

NEAR RAMOJIFILM CITY, DESHMUKHI(V), YADADRI, BHUVANGIRI DIST-508284

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



CERTIFICATE

This is to certify that the project report as "**SECURE DATA GROUP SHARING AND DISSEMINATION WITH ATTRIBUTE AND TIME CONDITIONS IN PUBLIC CLOUD**" has carried out and being submitted by **M. Sai Darshan Balaji (18BH1A05F8) M. Jaya Krishna Sai (18BH1A05F9) T. Amarnath Goud (18BH1A05E2) Md. Ali Ahmad Khurshid (18BH1A05J7)** have done this project in our institution for the partial fulfilment of award of Degree of in "**BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE & ENGINEERING"** in the department of **"COMPUTER SCIENCE AND ENGINEERING"** to the **Jawaharlal Nehru Technological University**, Hyderabad is a record of bonafide work carried out under our guidance and supervision.

Internal Guide

Dr. V. SAMBASIVA RAO M.TECH., Ph.D.

Asst. Professor

Department of CSE

HEAD OF THE DEPATMENT

K. HARISH KUMAR M.TECH.,Ph.D.

Asst. Professor

Department of CSE

External Examiner

ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of this project would be incomplete without the mention of the people who made it possible. We consider it as a privilege to express our gratitude and respect to all those who guided us in the completion of the project.

We are thankful to our internal guide**, Dr. V. SAMBASIVA RAO, Assistant professor, Department of Computer Science and Engineering, St. Mary's Engineering College** for having been of a source encouragement and for insisting us to do this project work.

We are obliged to **Mr. K. Harish Kumar, Assistant professor, Head of the Department of Computer Science and Engineering, St. Mary's Engineering College** for his guidance and suggestion throughout project work.

We take this opportunity to express a deep sense of gratitude to **Sri Dr. T G ARUL, Principal of St. Mary's Engineering College** for allowing us to do this seminar and for this affectionate encouragement in presenting this project work.

We convey our sincere thanks to **Sri Dr. Rev. K.V.K RAO, Chairman** of **St. Mary's Engineering College** for giving us learning environment to grow out self personally as well as professionally.

We would like to express our thanks to all staff members who have helped us directly and indirectly in accomplishing this project work. We also extended our sincere thanks to our parents and friends for their moral support throughout the project work. Above all we thank God almighty for his manifold mercies in carrying out this project work successfully.

M. Sai Darshan Balaji **[18BH1A05F8]**

M. Jaya Krishna Sai **[18BH1A05F9]**

T. Amarnath Goud **[18BH1A05E2]**

Md. Ali Ahmad Khurshid **[18BH1A05J7]**

ABSTRACT

Cloud computing has become increasingly popular among users and businesses around the world. Although cryptographic techniques can provide data protection for users in public cloud, several issues also remain problematic, such as secure data group dissemination and fine-grained access control of time-sensitive data. In this project, we propose an identity-based data group sharing and dissemination scheme in public cloud, in which data owner could broadcast encrypted data to a group of receivers at one time by specifying these receivers' identities in a convenient and secure way. In order to achieve secure and flexible data group dissemination, we adopt attribute-based and timed-release conditional proxy re-encryption to guarantee that only data disseminators whose attributes satisfy the access policy of encrypted data can disseminate it to other groups after the releasing time by delegating a re-encryption key to cloud server. The re-encryption conditions are associated with attributes and releasing time, which allows data owner to enforce fine-grained and timed-release access control over disseminated ciphertexts. The experimental results show our proposed scheme makes a tradeoff between computational overhead and expressive dissemination conditions

INDEX

FIGURE INDEX

LIST OF PLATES

INTRODUCTION

Cloud computing is regarded as such a computing paradigm in which resources in the computing infra- structure are provided as services over the Internet. The cloud computing benefits individual users and enterprises with convenient access, increased operational efficiencies and rich storage resources by combining a set of existing and new techniques from research areas such as service-oriented architectures and virtualization. Although the great benefits brought by cloud computing are exciting for users, security problems may somehow impede its quick development. Currently, more and more users would outsource their data to cloud service provider (CSP) for sharing. However, the CSP which deprives data owners' direct control over their data is assumed to be honest-but-curious, that may prompt security concerns. These security matters existing in public cloud motivate the requirement to appropriately keep data confidential. Several schemes exploiting cryptographic mechanisms to settle the security problems have been proposed. In order to guarantee secure data group sharing, identity-based broadcast encryption (IBBE) scheme is employed in public cloud. The data owners could broadcast their encrypted data to a group of receivers at one time and the public key of the user can be regarded as email, unique id and username. Hence, by using an identity, data own- er can share data with other group users in a convenient and secure manner. Attribute-based encryption (ABE) is one of new cryptographic mechanisms used in cloud to reach flexible and fine-grained secure data group sharing. Especially, ciphertext-policy ABE (CP-ABE) allows data owners to encrypt data with an access policy such that only users whose attributes satisfy the access policy can decrypt the data.

Except for being able to allow users to share data with others in public cloud, there is another requirement of data dissemination. For example, when Bob views a photo which is owned by Alice and hopes to share this photo with others, he can specify policies to authorize others to see this photo. In this case, Bob is a disseminator of the photo. The proxy re-encryption (PRE) scheme in a manner could achieve efficient data dissemination in cloud by re-encrypting the ciphertext to other users. However, it may not meet the requirements when data owner doesn't expect all the authorized users who can view his data to disseminate data or allow the disseminators to disseminate all of his data. For example, Alice authorizes Bob and Carol to access her data, but she only allows Bob to disseminate some specific photos or videos to his space. The conditional PRE (CPRE) scheme could address this issue by allowing a user to

generate a re-encryption key associated with a condition, and only the encrypted data meeting the condition can be re- encrypted. However, conditions in traditional CPRE which are only keywords may not well match situations in cloud because data owner may have a large number of requirements for different disseminators to disseminate his different data, such as photos taken in home only for families to disseminate and travelling photos allowed to be disseminated by friends. Thus, fine-grained conditions are inevitably needed in data group dissemination situation in public cloud.

Simultaneously, time-sensitive data such as a business plan and a tender, is a special data in cloud which re- quires time-based exposing. It means that data owner may want different users to disseminate data after different time. For instance, data owner may share sensitive business plan with directors, and he hopes these directors only can disseminate business plan to managers at an early time and then to other employees at last. Simply, the directors can manually release data owner's time- sensitive data, which requires data owner to formulate encrypted data only can be disseminated by directors to managers, and then be disseminated to other employees when the corresponding time arrives. However, this solution forces the directors to repeatedly disseminate different versions of the same data, which brings unnecessary burden. From the perspective of cryptography, this goal of time-based exposing can be achieved by timed-release encryption (TRE). Currently, some TRE-based systems incorporate the concept of time into a combination of CP-ABE or PRE to support fine-grained and time-based data exposing, whereas these approaches are failure to meet the above scenario of data dissemination.

Our Contribution

In this project, we propose a secure data group sharing and dissemination scheme with attribute and time conditions in public cloud. The main contributions of our scheme are as follows:

We employ IBBE technique to achieve secure data group sharing in public cloud, which allows data owner to outsource encrypted data to semi-trusted cloud and share it with a group of receivers at one time. It is more convenient that email and username could be used as public keys for users.

We design an access policy embedding releasing time and take the advantages of attribute-based CPRE, to achieve fine-grained and timed-release data group dis- semination. The CSP can re-encrypt initial ciphertexts for data disseminator after the designate time if his attributes associated with the re-encryption key satisfy the access policy in the ciphertexts.

We analyse the security of our proposed scheme, and conduct a detailed theoretical and experimental analysis. The results show that our scheme makes a trade-off between computational overhead and expressive dissemination conditions, and performs significantly better in data group sharing and dissemination in public cloud.

Application Scenario

Benefits brought by the proposed scheme are evident especially in public cloud storage systems. Our scheme is suitable for the scenarios where data can be shared and disseminated with time conditions in a group of users. Let's consider an application scenario. Suppose that company A uses the cloud storage service, in which the pro- posed scheme is being utilized. Some employees in company A usually share some important time-sensitive data

with different intended workmates, and these workmates can access the data stored in the cloud with sufficient authorization, but gain their disclosure privilege at different time points. Specially speaking, since the business plan of this company may contain some business secrets, executive officer shares this plan with directors to discuss and improve the business plan at an early time, while others cannot access this plan. Then, only executive director can gain disclosure privilege to disseminate the business plan in the cloud to managers of some relevant departments at a later time point, when they take responsibility for the plan execution. At last, all the directors can disseminate the business plan in the cloud to make other employees in the company to have the access privilege after specific secrecy period.

SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

1. In general, we upload file to the public cloud and it can be accessed by many users with many to many relationships.
2. Here the data owner shares, uploads data file to a Cloud service Provider (CSP) with key and this key can be used while accessing the file.
3. The file and the key both will be with the CSP.

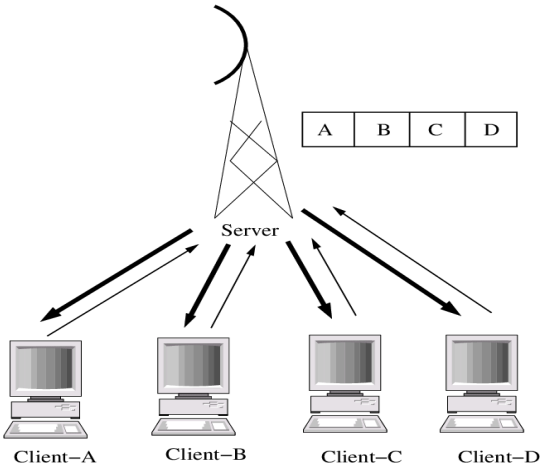


Figure 2.1 Existing system

Disadvantages of Existing System

1. These schemes do not support the scenario where the access privilege of data is required to be respectively released to different groups of users after different time points.
2. These schemes lack fine-grained access control.
3. It introduces heavy extra overhead since the authority needs to generate update keys for all potential attributes each time to implement the time-related function, and the computational complexity increases with the amount of involved attributes.
4. This scheme does not consider the data owner's requirement and his encrypted data may be re-encrypted for other group users after different releasing time.

2.2 PROPOSED SYSTEM

1. We employ IBBE technique to achieve secure data group sharing in public cloud, which allows data owner to outsource encrypted data to semi-trusted cloud and share it with a group of receivers at one time. It is more convenient that email and username could be used as public keys for users.

2. We design an access policy embedding releasing time and take the advantages of attribute-based Conditional Proxy Re-encryption (CPRE), to achieve fine-grained and timed-release data group dissemination.

The results show that our scheme makes a tradeoff between computational overhead and expressive dissemination conditions. significantly better in data group sharing and dissemination in public cloud.

2.3 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

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

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. The expenditures must be justified. Thus, the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

SYSTEM DESIGN

3.1 DEFINITION

System design is the process of defining the components, modules, interfaces, and data for a system to satisfy specified requirements. System development is the process of creating or altering systems, along with the processes, practices, models, and methodologies used to develop them.

Architectural design

The architectural design of a system emphasizes the design of the system architecture that describes the structure, behaviour and more views of that system and analysis.

Logical design

The logical design of a system pertains to an abstract representation of the data flows, inputs and outputs of the system. This is often conducted via modelling, using an over-abstract (and sometimes graphical) model of the actual system. In the context of systems, designs are included. Logical design includes ER diagrams.

Physical design

The physical design relates to the actual input and output processes of the system. This is explained in terms of how data is input into a system, how it is verified/authenticated, how it is processed, and how it is displayed. In physical design, the following requirements about the system are decided.

- Input requirement,
- Output requirements,
- Storage requirements,
- Processing requirements,
- System control and backup or recovery

Processing within the CPU, and output via a monitor, printer, etc. It would not concern the actual layout of the tangible hardware, which for a PC would be a monitor, CPU, motherboard, hard drive, modems, video/graphics cards, USB slots, etc. It involves a detailed design of a

user and a product database structure processor and a control processor. The H/S personal specification is developed for the proposed system.

3.2 OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- Select methods for presenting information.
- Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the
- ❖ Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

3.3 INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus, the objective of input design is to create an input layout that is easy to follow.

3.4 SYSTEM ARCHITECTURE

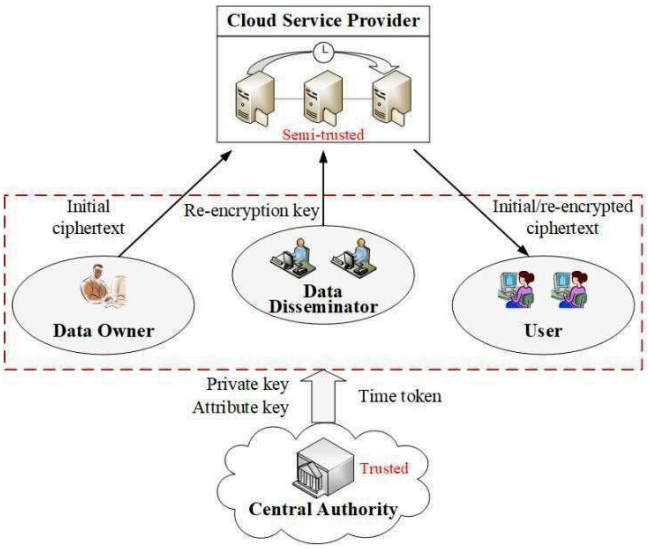


Fig.3.4 System Architecture

System Model

The primary goal of our scheme is to achieve fine-grained and timed-release data group dissemination. Fig. 1 shows the system model of our scheme, which consists of the following system entities.

The central authority (CA) is a fully trusted authority running on trusted cloud platform with flexibility and scalability that manages and distributes public/secret keys in the system, including generates system parameters to initialize system and generates private keys and attribute keys with users' identity and attributes. In addition, it acts as a trusted time agent to publish time token at each pre-defined time.

The CSP is a semi-trusted entity that has abundant storage capacity and computation power to pro- vide data sharing services in public cloud. It is in charge of controlling the accesses from outside users to the stored data and providing corresponding services. When it receives the request of data re-encryption, it is responsible for generating a re- encrypted ciphertext with re-encryption key from data disseminator. Hence, CSP stores not only initial cipher texts, but also re-encrypted ciphertexts.

The data owner wishes to outsource the data into cloud for convenience of group sharing and dissemination. The data owner is in charge of encrypting data for a set of receivers. If the data owner has the requirement to limit his data to be disseminated by some specific people after

some specific time, the data owner is able to define at- tribute-based and timed-release access policy, and enforce it on his own data by encrypting the data under the policy before outsourcing it.

- The data disseminator is the person who wishes to share data owner's data with other people (e.g., his friends, family members, colleagues). For security and access control considerations, data disseminator must be one of intended receivers defined by the data owner, who could decrypt the initial cipher texts. The data disseminator can generate re- encryption keys, and then send data re-encryption requests with these keys to the CSP to disseminate data owner's data to others. Only the attributes of data disseminator satisfy access policy and the pre- determined time arrives, data re-encryption request can be successfully executed by CSP.
- The user is the ciphertexts receiver who can access the outsourced data. The user is able to decrypt the initial and re-encrypted ciphertexts if he is the in- tended receiver defined by the data owners or data disseminators.

Security Model

In our scheme, we assume the CA running on the trusted cloud platform to be fully trusted, which means it would not be compromised by malicious attackers, or collude with other malicious entities. However, we assume the CSP is honest but curious, which means it executes the tasks and may collude to get unauthorized data. Specifically, security requirements cover the following aspects.

Data confidentiality. The unauthorized users who are not the intended receivers defined by data owner should be prevented from accessing the data. Additionally, unauthorized access from CSP which is not fully trusted should also be prevented.

Re-encryption secrecy. The data disseminator whose attributes could not satisfy the access policy in ciphertexts alone, or who tries to disseminate the ciphertext before specified releasing time, should be prevented from disseminating the cipher texts.

Flexible dissemination conditions. The data owner can custom fine-grained and timed-release conditions so that the data only can be disseminated by the user attributes satisfy these conditions after the releasing time.

Collusion resistance. The unauthorized data disseminators cannot collude with each other to generate the re- encryption key, thus the re-encryption of ciphertext should not be successful.

3.5 DATA FLOW DIAGRAM

The DFD is also called as bubble chart. The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system

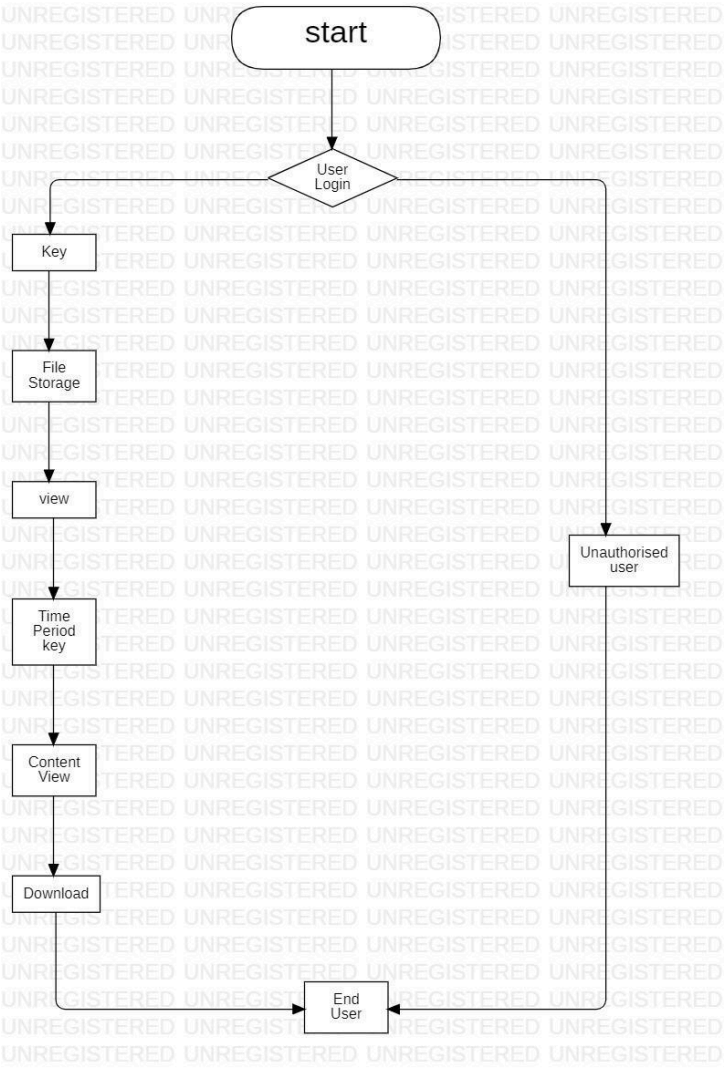


Figure 3.5.1 Data Flow Diagram- USER

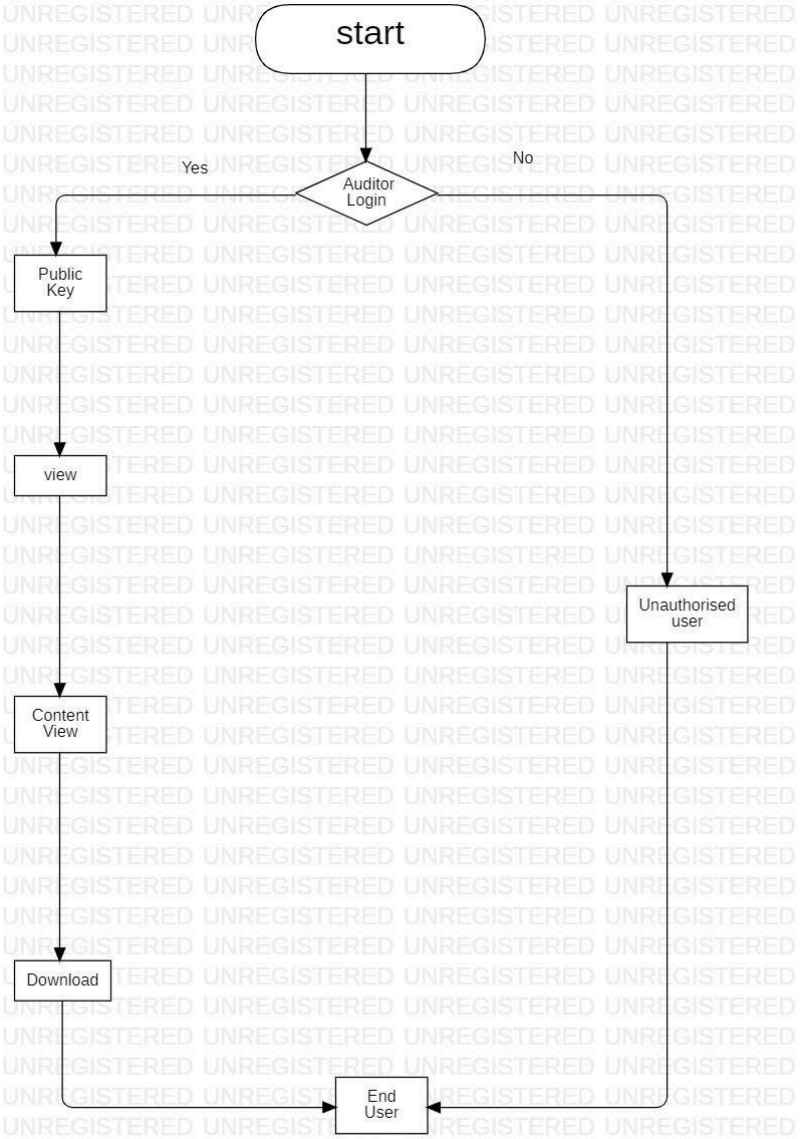


Figure 3.5.2 Data Flow Diagram – AUDITOR

3.6 USE CASE DIAGRAM

• A use case diagram in the Unified Modelling Language (UML) is a type of behavioural diagram defined by and created from a Use-case analysis.

• Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.

• The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

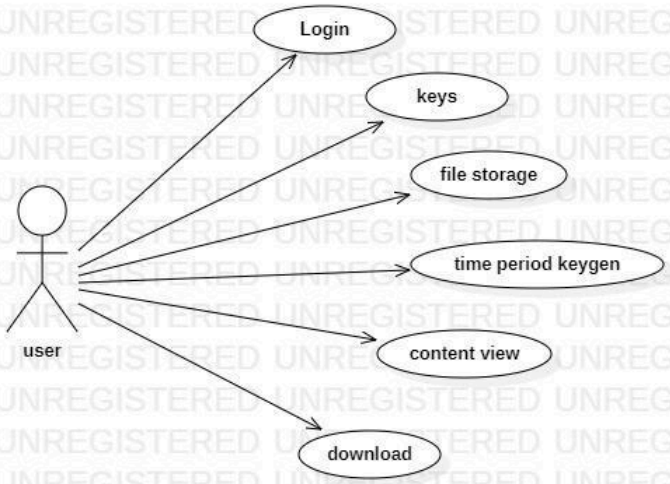


Figure 3.6.1 Use case diagram – USER

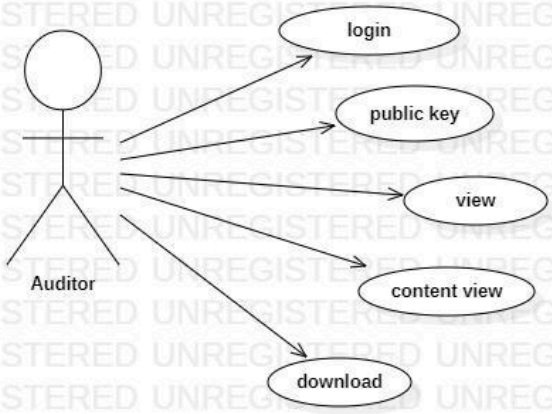


Figure 3.6.2 Use Case Diagram – AUDITOR

SEQUENCE DIAGRAM:

A sequence diagram in Unified Modelling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

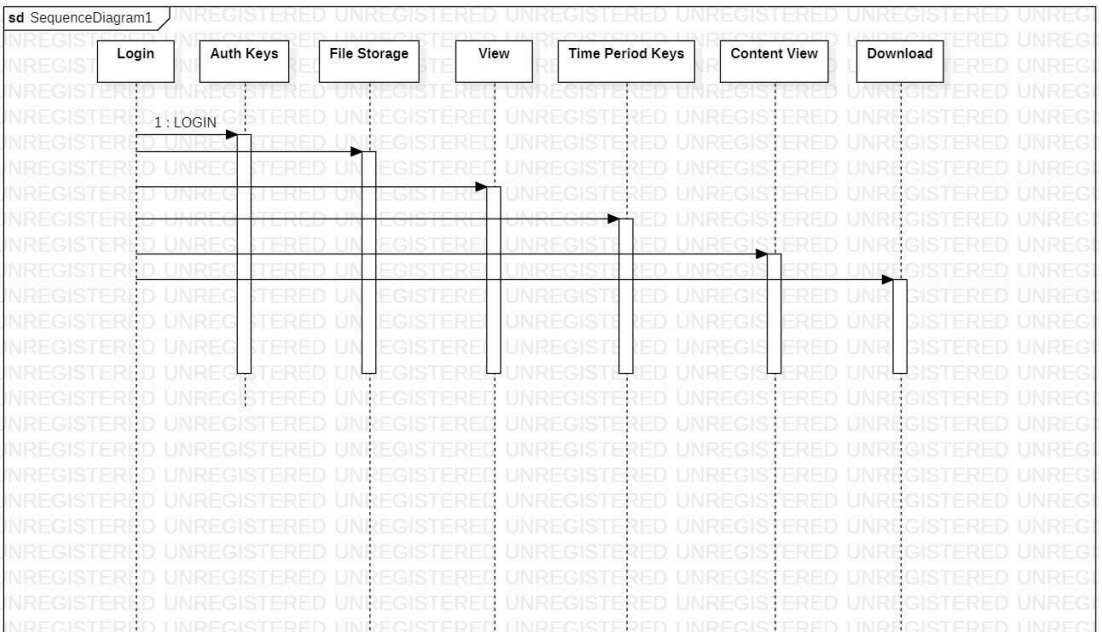


Figure 3.6.3 Sequence diagram- USER

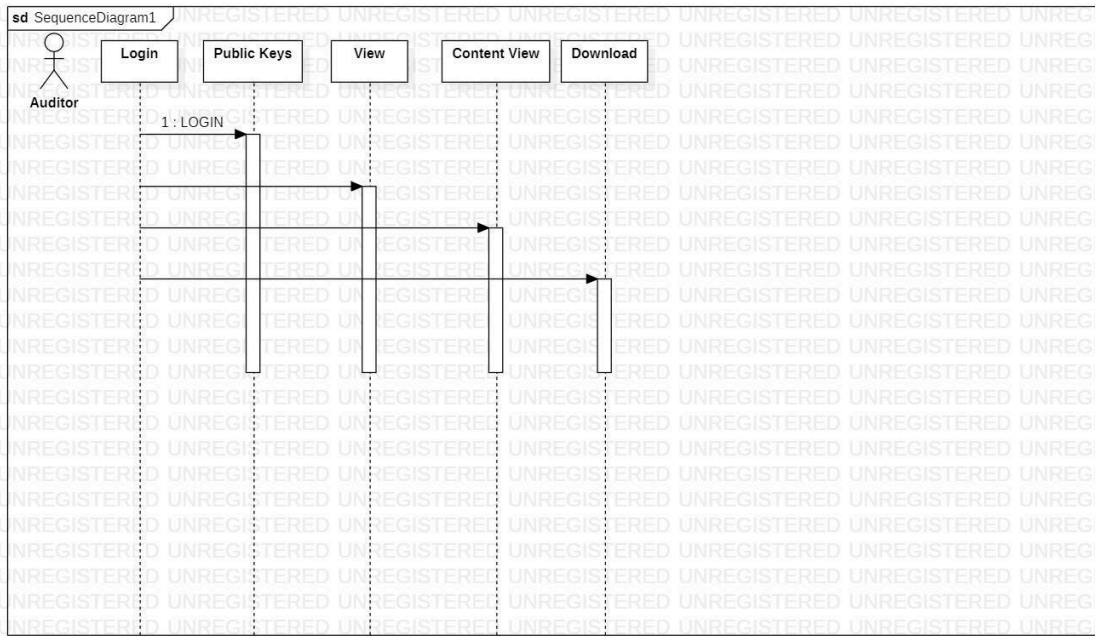


Figure 3.6.4 Sequence diagram- AUDITOR

3.7 E-R DAIGRAMS

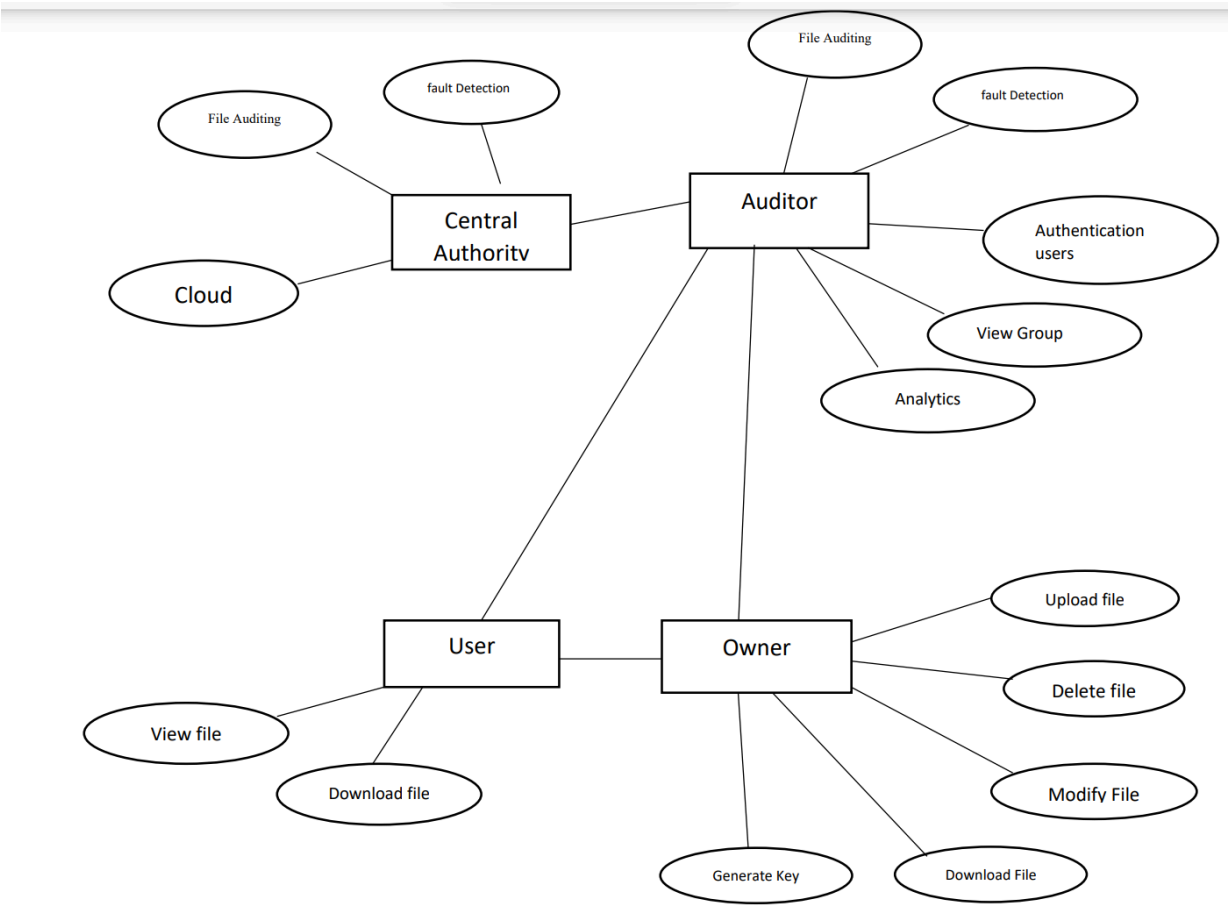


Figure 3.7.1 E-R DIAGRAM

3.8 DATA DICTIONARY

USER REGISTER:

FIELD NAME	DATA TYPE	DATA SIZE	DESCRIPTION
User Id	Int	10	User Id, Auto Generated
User Name	Varchar	45	Name Of the User
User Email id	Varchar	45	User Email Id
User Password	Varchar	10	Login Password For user
User Mobile	Varchar	10	Landline Or Mobile Number

AUDITOR LOGIN:

FIELD NAME	DATA TYPE	DATA SIZE	DESCRIPTION
Auditor id	Int	10	Auditor Id, Auto Generator
Auditor Name	Varchar	45	Name Of the Auditor
Auditor Password	Varchar	10	Login Password for Auditor

USER LOGIN:

FIELD NAME	DATA TYPE	DATA SIZE	DESCRIPTION
Use id	Int	10	User Id, Auto Generator
User Name	Varchar	45	Name Of the User
User Password	Varchar	10	Login Password for User

4 SYSTEM SPECIFICATIONS

4.1HARDWARE SPECIFICATIONS

1. Hardware	:	Pentium Dual Core
2. Speed	:	2.80 GHz
3. RAM	:	1GB
4. Hard Disk	:	20 GB

4.2SOFTWARE SPECIFICATIONS

1. Operating System	:	Windows 7, 8, 10
2. Technology	:	Java7 and J2EE
3. Web Technologies	:	Html, JavaScript, CSS
4. IDE	:	NetBeans IDE 8.2
5. Web Server	:	Tomcat
6. Database	:	My SQL
7. Java Version	:	J2SDK1.5

5 OVER VIEW OF LANGUAGE

5.1 FRONTEND OR USER INTERFACE DESIGN

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.

5.2 COMMUNICATION OR DATABASE CONNECTIVITY TIER:

The Communication architecture is designed by concentrating on the Standards of Servlets and Enterprise Java Beans. The database connectivity is established by using the Java Data Base Connectivity. The standards of three-tier architecture are given major concentration to keep the standards of higher cohesion and limited coupling for effectiveness of the operations.

5.3 ABOUT JAVA:

Initially the language was called as “oak” but it was renamed as “Java” in 1995. The primary motivation of this language was the need for a platform-independent (i.e., architecture neutral) language that could be used to create software to be embedded in various consumer electronic devices. Java is a programmer’s language. Java is cohesive and consistent. Except for those constraints imposed by the Internet environment, Java gives the programmer, full control.

Finally, Java is to Internet programming where C was to system programming.

Features Of Java:

Security:

Every time you that you download a “normal” program, you are risking a viral infection. Prior to Java, most users did not download executable programs frequently, and those who did scanned them for viruses prior to execution. Most users still worried about the possibility of infecting their systems with a virus. In addition, another type of malicious program exists that must be guarded against. This type of program can gather private information, such as credit card numbers, bank account balances, and passwords.

Java answers both these concerns by providing a “firewall” between a network application and your computer. When you use a Java-compatible Web browser, you can safely download Java applets without fear of virus infection or malicious intent.

Portability:

For programs to be dynamically downloaded to all the various types of platforms connected to the Internet, some means of generating portable executable code is needed. As you will see, the same mechanism that helps ensure security also helps create portability. Indeed, Java’s solution to these two problems is both elegant and efficient.

The Byte code:

The key that allows the Java to solve the security and portability problems is that the output of Java compiler is Byte code. Byte code is a highly optimized set of instructions designed to be executed by the Java run-time system, which is called the Java Virtual Machine (JVM). That is, in its standard form, the JVM is an interpreter for byte code.

Translating a Java program into byte code helps makes it much easier to run a program in a wide variety of environments. The reason is, once the run-time package exists for a given system, any Java program can run on it. Although Java was designed for interpretation, there is technically nothing about Java that prevents on-the-fly compilation of byte code into native code. Sun has just completed its Just In Time (JIT) compiler for byte code. When the JIT compiler is a part of JVM, it compiles byte code into executable code in real time, on a piece-by-piece, demand basis. It is not possible to compile an entire Java program into executable code all at once, because Java performs various run-time checks that can be done only at run time. The JIT compiles code, as it is needed, during execution.

Java, Virtual Machine (JVM):

Beyond the language, there is the Java virtual machine. The Java virtual machine is an important element of the Java technology. The virtual machine can be embedded within a web browser or an operating system.

Once a piece of Java code is loaded onto a machine, it is verified. As part of the loading process, a class loader is invoked and does byte code verification makes sure that the code that’s has been generated by the compiler will not corrupt the machine that it’s loaded on. Byte code verification takes place at the end of the compilation process to make sure that is all

accurate and correct. So, byte code verification is integral to the compiling and executing of Java code.

Overall Description:

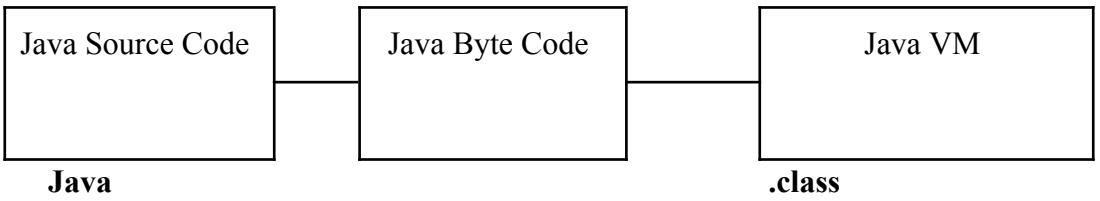


Figure 5.3 Picture Showing the Development Process of Java Program

Java programming uses to produce byte codes and executes them. The first box indicates that the Java source code is located in a. Java file that is processed with a Java compiler called javac. 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.

5.4 JAVASCRIPT:

JavaScript is a script-based programming language that was developed by Netscape Communication Corporation. JavaScript was originally called Live Script and renamed as JavaScript to indicate its relationship with Java. JavaScript supports the development of both client and server components of Web-based applications.

On the client side, it can be used to write programs that are executed by a Web browser within the context of a Web page. On the server side, it can be used to write Web server programs that can process information submitted by a Web browser and then updates the browser's display accordingly

Even though JavaScript supports both client and server Web programming, we prefer JavaScript at Client-side programming since most of the browsers supports it. JavaScript is almost as easy to learn as HTML, and JavaScript statements can be included in HTML documents by enclosing the statements between a pair of scripting tags

<SCRIPTS>..</SCRIPT>.

<SCRIPT LANGUAGE = “JavaScript”>

JavaScript statements

</SCRIPT>

JavaScript vs Java:

JavaScript and Java are entirely different languages.

A few of the most glaring differences are:

1. Java applets are generally displayed in a box within the web document;
2. JavaScript can affect any part of the Web document itself.
3. While JavaScript is best suited to simple applications and adding interactive features to Web pages; Java can be used for incredibly complex applications.

5.5 HYPER TEXT MARKUP LANGUAGE:

Hypertext Markup Language (HTML), the languages of the World Wide Web (WWW), allows users to produces Web pages that include text, graphics and pointer to other Web pages (Hyperlinks).

HTML is not a programming language but it is an application of ISO Standard 8879, SGML (Standard Generalized Markup Language), but specialized to hypertext and adapted to the Web. The idea behind Hypertext is that instead of reading text in rigid linear structure, we can easily jump from one point to another point. We can navigate through the information based on our interest and preference. A markup language is simply a series of elements, each delimited with special characters that define how text or other items enclosed within the elements should be displayed. Hyperlinks are underlined or emphasized works that load to other documents or some portions of the same document.

HTML can be used to display any type of document on the host computer, which can be geographically at a different location. It is a versatile language and can be used on any platform or desktop.

HTML provides tags (special codes) to make the document look attractive. HTML tags are not case-sensitive. Using graphics, fonts, different sizes, color, etc., can enhance the presentation of the document. Anything that is not a tag is part of the document itself.

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

5.6 JAVA DATABASE CONNECTIVITY:

What Is JDBC?

JDBC is a Java API for executing SQL statements. (As a point of interest, JDBC is a trademarked name and is not an acronym; nevertheless, JDBC is often thought of as standing for Java Database Connectivity. It consists of a set of classes and interfaces written in the Java programming language.

JDBC provides a standard API for tool/database developers and makes it possible to write database applications using a pure Java API.Using JDBC, it is easy to send SQL statements to virtually any relational database. One can write a single program using the JDBC API, and the program will be able to send SQL statements to the appropriate database. The combinations of Java and JDBC lets a programmer write it once and run it anywhere.

JDBC versus ODBC and other API s:

At this point, Microsoft's ODBC (Open Database Connectivity) API is that probably the most widely used programming interface for accessing relational databases. It offers the ability to connect to almost all databases on almost all platforms.

So why not just use ODBC from Java? The answer is that you can use ODBC from Java, but this is best done with the help of JDBC in the form of the JDBC-ODBC Bridge, which we will cover shortly. The question now becomes "Why do you need JDBC?" There are several answers to this question:

ODBC is not appropriate for direct use from Java because it uses a C interface. Calls from Java to native C code have a number of drawbacks in the security, implementation, robustness, and automatic portability of applications.

A literal translation of the ODBC C API into a Java API would not be desirable. For example, Java has no pointers, and ODBC makes copious use of them, including the notoriously error-prone generic pointer "void *". You can think of JDBC as ODBC translated into an object-oriented interface that is natural for Java programmers.

ODBC is hard to learn. It mixes simple and advanced features together, and it has complex options even for simple queries. JDBC, on the other hand, was designed to keep simple things simple while allowing more advanced capabilities where required.

A Java API like JDBC is needed in order to enable a "pure Java" solution. When ODBC is used, the ODBC driver manager and drivers must be manually installed on every client machine. When the JDBC driver is written completely in Java, however, JDBC code is automatically installable, portable, and secure on all Java platforms from network computers to mainframes.

Two-tier and Three-tier Models:

The JDBC API supports both two-tier and three-tier models for database access. In the two-tier model, a Java applet or application talks directly to the database. This requires a JDBC driver that can communicate with the particular database management system being accessed. A user's SQL statements are delivered to the database, and the results of those statements are sent back to the user. The database may be located on another machine to which the user is connected via a network. This is referred to as a client/server configuration, with the user's machine as the client, and the machine housing the database as the server. The network can be an Intranet, which, for example, connects employees within a corporation, or it can be the Internet.

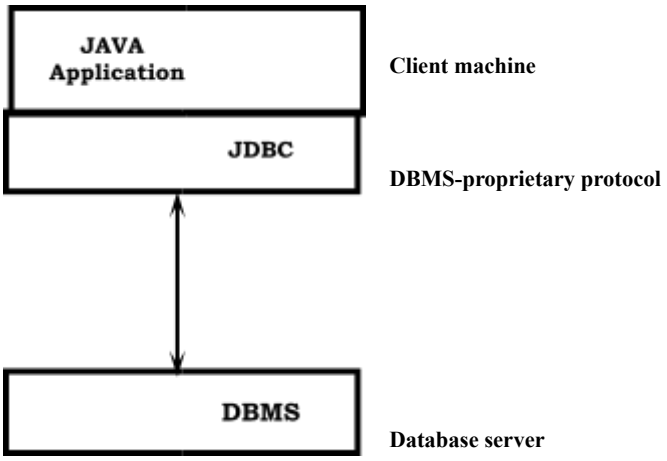


Figure 5.6.1. Two-Tier Model

In the three-tier model, commands are sent to a "middle tier" of services, which then send SQL statements to the database. The database processes the SQL statements and sends the results back to the middle tier, which then sends them to the user. MIS directors find the three-tier model very attractive because the middle tier makes it possible to maintain control over access and the kinds of updates that can be made to corporate data. Another advantage is that when

there is a middle tier, the user can employ an easy-to-use higher-level API which is translated by the middle tier into the appropriate low-level calls. Finally, in many cases the three-tier architecture can provide performance advantages.

Until now the middle tier has typically been written in languages such as C or C++, which offer fast performance. However, with the introduction of optimizing compilers that translate Java byte code into efficient machine-specific code, it is becoming practical to implement the middle tier in Java. This is a big plus, making it possible to take advantage of Java's robustness, multi-threading, and security features.

JDBC is important to allow database access from a Java middle tier.

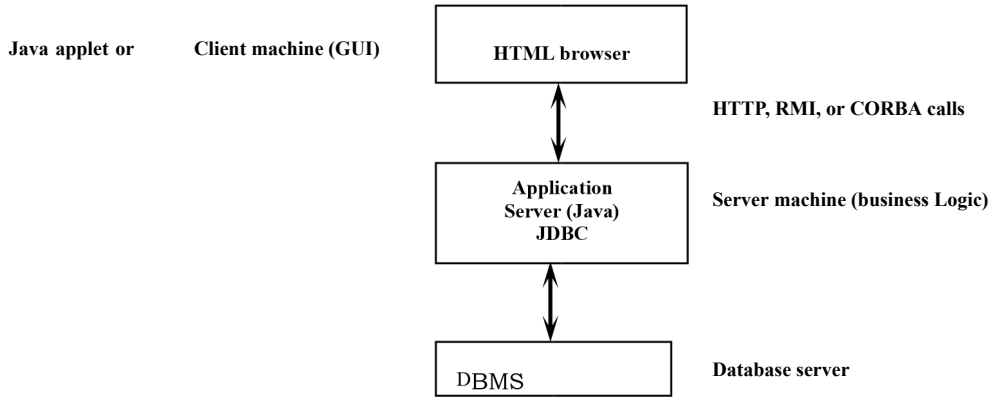


Figure 5.6 2. Three-Tier Model

5.7 JAVA SERVER PAGES (JSP):

Java server Pages is a simple, yet powerful technology for creating and maintaining dynamic-content web pages. Based on the Java programming language, Java Server Pages offers proven portability, open standards, and a mature re-usable component model. The Java Server Pages architecture enables the separation of content generation from content presentation. This separation not eases maintenance headaches, it also allows web team members to focus on their areas of expertise. Now, web page designer can concentrate on layout, and web application designers on programming, with minimal concern about impacting each other's work.

Features of JSP:

Portability:

Java Server Pages files can be run on any web server or web-enabled application server that provides support for them. Dubbed the JSP engine, this support involves recognition, translation, and management of the Java Server Page life cycle and its interaction components.

Components:

It was mentioned earlier that the Java Server Pages architecture can include reusable Java components. The architecture also allows for the embedding of a scripting language directly into the Java Server Pages file. The components current supported include Java Beans, and Servlets.

Processing:

A Java Server Pages file is essentially an HTML document with JSP scripting or tags. The Java Server Pages file has a JSP extension to the server as a Java Server Pages file. Before the page is served, the Java Server Pages syntax is parsed and processed into a Servlet on the server side. The Servlet that is generated outputs real content in straight HTML for responding to the client.

Access Models:

A Java Server Pages file may be accessed in at least two different ways.

A client's request comes directly into a Java Server Page. In this scenario, suppose the page accesses reusable Java Bean components that perform particular well-defined computations like accessing a database. The result of the Beans computations, called result sets is stored within the Bean as properties. The page uses such Beans to generate dynamic content and present it back to the client.

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:

1. Perform connection and authentication to a database server

2. Manager transactions
3. Move SQL statements to a database engine for pre-processing and execution
4. Execute stored procedures
5. Inspect and modify the results from Select statements.

5.8 TOMCAT 6.0 WEB SEVER:

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 Web logic, is one of the popular application servers). To develop a web application with jsp/servlet installs any web server like JRun, Tomcat etc to run your application.

6. IMPLEMENTATIONS

6.1 System Modules

MODULES:

- Data Owner
- Data User
- Central Authority (CA)
- Semi-Trusted (CSP)
- Data Disseminator

MODULE DESCRIPTION:

Data Owner:

The data owner wishes to outsource the data into cloud for convenience of group sharing and dissemination. The data owner is in charge of encrypting data for a set of receivers. If the data owner has the requirement to limit his data to be disseminated by some specific people after some specific time, the data owner is able to define attribute-based and timed-release access policy, and enforce it on his own data by encrypting the data under the policy before outsourcing it.

Data User:

The user is the ciphertexts receiver who can access the outsourced data. The user is able to decrypt the initial and re-encrypted ciphertexts if he is the intended receiver defined by the data owners or data disseminators.

Central Authority (CA):

The central authority (CA) is a fully trusted authority running on trusted cloud platform with flexibility and scalability that manages and distributes public/secret keys in the system, including generates system parameters to initialize system and generates private keys and attribute keys with users' identity and attributes. In addition, it acts as a trusted time agent to publish time token at each pre-defined time.

Semi-Trusted (CSP):

The CSP is a semi-trusted entity that has abundant storage capacity and computation power to provide data sharing services in public cloud. It is in charge of controlling the accesses from outside users to the stored data and providing corresponding services. When it receives the request of data re-encryption, it is responsible for generating a reencrypted ciphertext with re-encryption key from data disseminator. Hence, CSP stores not only initial ciphertexts, but also re-encrypted ciphertexts.

Data Disseminator:

The data disseminator is the person who wishes to share data owner's data with other people (e.g., his Senior, Manager, and Planning Department). For security and access control considerations, data disseminator must be one of intended receivers defined by the data owner, who could decrypt the initial ciphertexts. The data disseminator can generate reencryption keys, and then send data re-encryption requests with these keys to the CSP to disseminate data owner's data to others. Only the attributes of data disseminator satisfy access policy and the pre-determined time arrives, data re-encryption request can be successfully executed by CSP.

6.2 SOURCE CODE

USER.JSP

```
<%@ page language="java" content Type="text/html; charset=ISO-8859-1" page
Encoding="ISO-8859-1"%>

<%@ page language="java" import="java.sql. *, com. dbasecon.Databasecon" error Page=""
%>

<!DOCTYPE html>

<html>

<head>

<title>Auditor File View</title>

<link href="css/style.css" rel="stylesheet" type="text/css">
```

```
<link href="css/table.css" rel="stylesheet" type="text/css">

<link href="css/tabzoom.css" rel="stylesheet" type="text/css">

</head>

<body>

<div id="header">

<div>

 <h1 align="center"><font size="6" color="brown"> <b>Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud </font></h2>

<ul class="navigation">

<! -- <li><a href="/CloudStorageAuditKey/index.html">Home</a></li> -->

<li><a href="auditview.jsp">File View</a></li

  <li><a class="active" href="users.jsp">User Details</a>

<li><a href="graph.jsp">Graph</a></li>

<li><a href="logout.jsp">Logout</a><

</ul>

</div>

</div>

<div id="body">

<div class="content">

<div>

<div>
```

```
<p>

<div class="CSSTableGenerator">

<table>

<tr>

<td>SerNo</td>

<td>Username</td>

<td>Email</td>

<td>Mobile</td>

<td>City</td><td>Group</td>

</tr>

<%int count=1;

Connection con=Databasecon.getConnection();

String query="select * from registration";

Prepared Statement pstmt=con.prepareStatement(query);

ResultSet rs=pstmt.executeQuery();

while(rs.next())

{        %>

<tr><%-- <td><%=rs.getInt("sid")%></td> --%>

<td><%=rs. get String("id") %></td>

<td><%=rs. get String("uname")%></td>
```

```
<td><%=rs.getString("email")%></td>

<td><%=rs.getString("mobile")%></td>

<td><%=rs.getString("city")%></td>

<td><%=rs.getString("groups")%></td>

</tr>    <%}

%>

</table>

</div>

</p>

</div>

</div>

</div><div class="sidebar">

<img src="images/textview.png">

</div>

</div>

<div id="footer">

<div class="abc" align="center">

<p>&copy; Copyright 2021. All Rights Reserved</p>

</div>

</div>
```

```
</body>

</html>
```

7 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 tests. Each test type addresses a specific testing requirement.

7.1 TEST CASES

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. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components

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.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box. you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

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.

Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g., components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

TP User login:

S. No	Action	Inputs	Excepted Output	Actual Output	Test Browser	Test result	Test comments
1	Launch application	http://localhost:8084/secure data group sharing /member_login.jsp .	Login page	Login page	Chrome	Pass	Launch successful
2	Enter correct username and password and hit login button	Username: amarnath Password: amarnath	Login success	Login success	Chrome	pass	Login Successful
3	Enter incorrect username and correct password and hit login button	Username: Asdf Password: amarnath	Login failure	Login failure	Chrome	fail	Login fail
4	Enter correct username and incorrect password and hit login button	Username: Amarnath Password: asdf	Login failure	Login failure	Chrome	fail	Login fail

TP Auditor login:

S.No	Action	Inputs	Excepted Output	Actual Output	Test Browser	Test result	Test comments
1	Launch application	http://localhost:8084/secure data group sharing and /auditorlogin.jsp	Login page	Login page	Chrome	Pass	Launch sucessful
2	Enter correct username and password and hit login button	Username: Auditor Password: Auditor	Login success	Login success	Chrome	pass	Login Successful
3	Enter incorrect username and correct password and hit login button	Username: Asdf Password: Amar	Login failure	Login failure	Chrome	fail	Login fail

8 OUTPUT SCREENS

8.1 USER REGISTRATION FORM

reguser.jsp

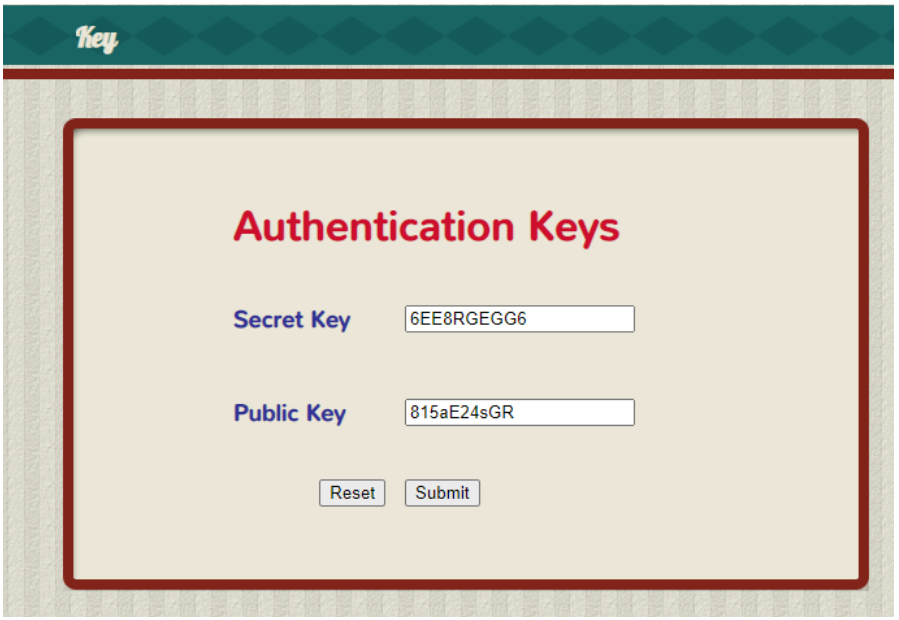
register

8.2 USER LOGIN FORM

user.jsp

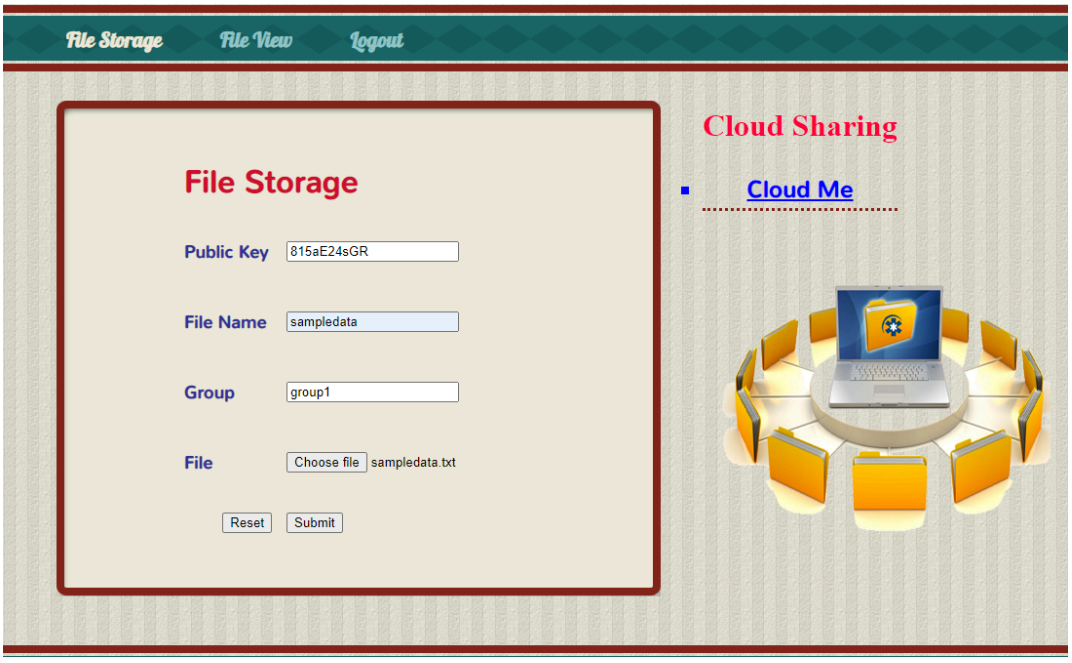
8.3 Verifying keys to login

pubkey.jsp



8.4 Uploading file to the public cloud

keyauthdb.jsp

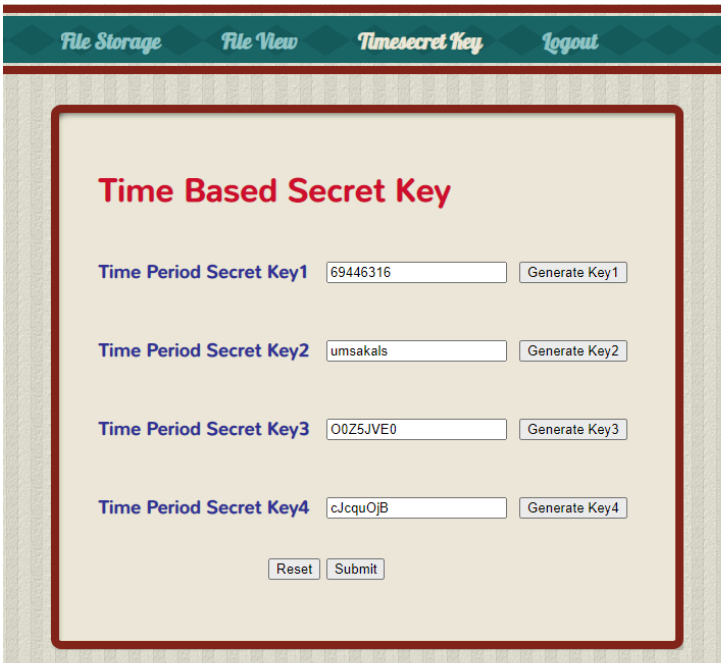


8.5 Viewing uploaded file

fileview.jsp

8.6 Generating time secret keys

timesecretkey.jsp

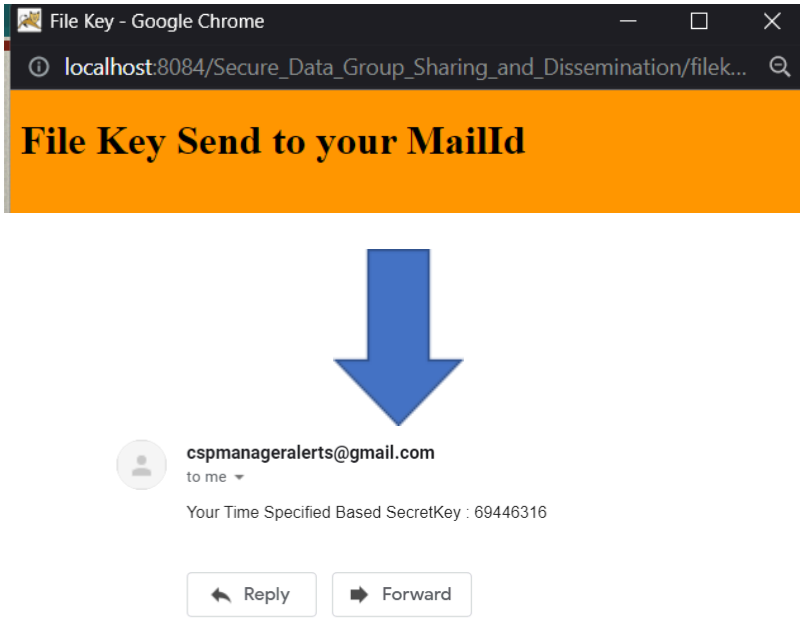


8.7 Requesting Time Secret Key

fcontview.jsp

8.8 Getting time secret key through mail

filekey.jsp



8.9 Viewing file after getting authorized with the time secret key

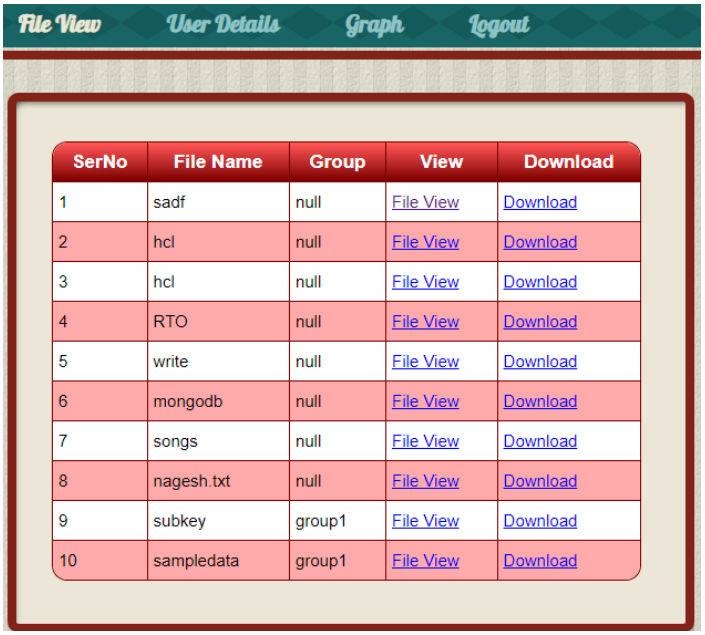
fcontview.jsp

auditor.jsp

auditorlogdb.jsp

8.10 Auditor can access all the files from all the users

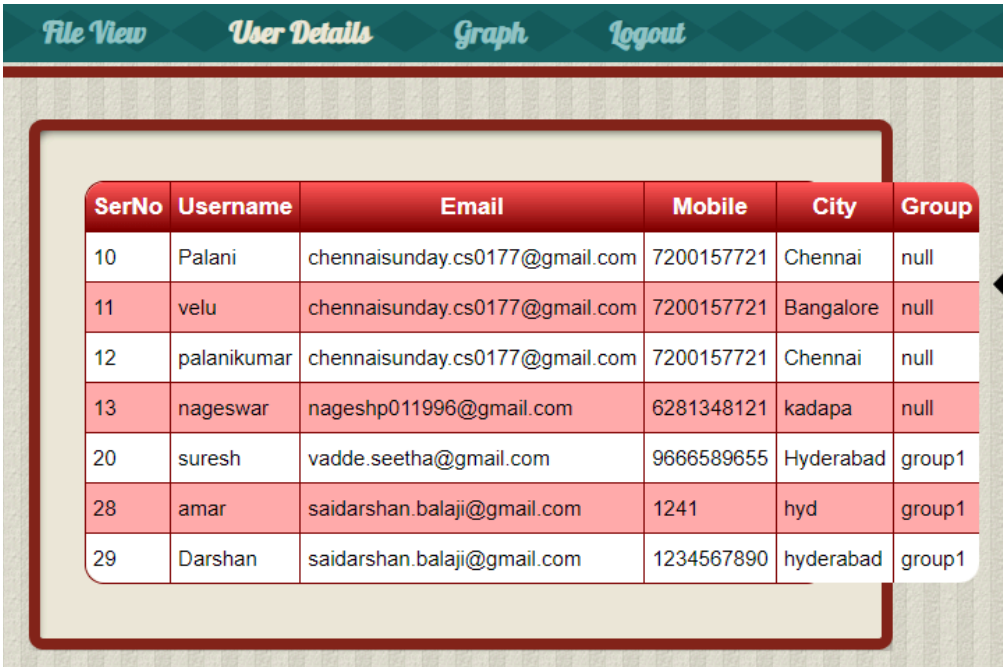
auditkeyauthdb.jsp



SerNo	File Name	Group	View	Download
1	sadf	null	File View	Download
2	hcl	null	File View	Download
3	hcl	null	File View	Download
4	RTO	null	File View	Download
5	write	null	File View	Download
6	mongodb	null	File View	Download
7	songs	null	File View	Download
8	nagesh.txt	null	File View	Download
9	subkey	group1	File View	Download
10	sampledata	group1	File View	Download

8.11 Auditor can access details of all the users

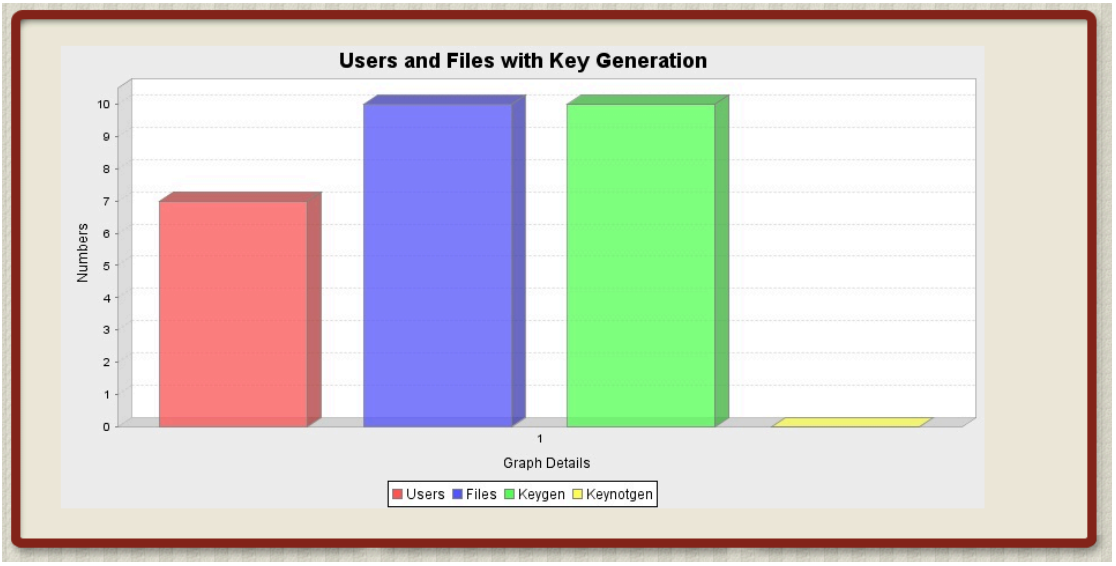
users.jsp



SerNo	Username	Email	Mobile	City	Group
10	Palani	chennaisunday.cs0177@gmail.com	7200157721	Chennai	null
11	velu	chennaisunday.cs0177@gmail.com	7200157721	Bangalore	null
12	palanikumar	chennaisunday.cs0177@gmail.com	7200157721	Chennai	null
13	nageswar	nageshp011996@gmail.com	6281348121	kadapa	null
20	suresh	vadde.seetha@gmail.com	9666589655	Hyderabad	group1
28	amar	saidarshan.balaji@gmail.com	1241	hyd	group1
29	Darshan	saidarshan.balaji@gmail.com	1234567890	hyderabad	group1

8.12 Auditor can also view data graph of all the components

graph.jsp



8.13 Auditor Table

	id	adtname	adtpwd	Pubkey
	1	auditor	auditor	auditor123
*	(NULL)	(NULL)	(NULL)	(NULL)

The above table is to store auditor details which are used login into auditor pages

8.14 User Table

	sid	pkey	fname	fcont		skey1	skey2	skey3	skey4	status	groups
	1	1235	sadf	smita.d@alchemysolutions.com	28 b...	77093248	8fgpq0wc	VPYILDRY	PdMbRViM	Generated	(NULL)
	5	12345	hcl	smita.d@alchemysolutions.com	28 b...	48345898	0kziumm5	FC43CYYF	ILpqQifg	Generated	(NULL)
	6	12345	hcl	smita.d@alchemysolutions.com	28 b...	80065791	az053k7m	037ZVJ4G	XrkJWiEG	Generated	(NULL)
	7	42342	RTO	http://btis.in/rto	18 b...	78302808	eevtdai4	P4X1X7KR	GbhpKTkR	Generated	(NULL)
	9	1234	write	http://stackoverflow.com/questions/1350742...	2 Kb...	49915723	du8u7dk5	WL2S4UQF	WUhQaTof	Generated	(NULL)
	11	1234	mongodb	http://www.webiyo.com/2011/02/install-mong...	71 b...	55614432	lmpz7x67	R7RDPBOZ	nmNkScog	Generated	(NULL)
	12	1234	songs	http://tamiltunes.com/ilayarajas-best-melo...	139 b...	91550861	172vhh2t	7XAKCOIJ	eTMJyPXq	Generated	(NULL)
	13	121E3b6411	nagesh.txt	welcome to project demonistration	33 b...	10908626	21v5h6ip	2RO1JPLD	VvlvkwQU	Generated	(NULL)
	14	2jEb3jj1k5	sampleData	Data deduplication is one of important dat...	187 b...	(NULL)	(NULL)	(NULL)	(NULL)	Key Not Gen	(NULL)
	15	3RGj18aEC5	subkey	To accomplish more reliable verification o...	236 b...	02581818	6681pebu	7BECWZDR	jkKSKXnl	Generated	group1
*	(NULL)	(NULL)	(NULL)	(NULL)	0 Kb...	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

The above database table stores user details which are used to login into the user side of the application.

8.15 Graph Table

	sid	Users	Files	Keygen	Keynotgen
	1	5	10	9	1
*	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

The above table stores graph values.

8.16 File Table with Keys

	Id	Uname	Email	Password	Mobile	City	Pubkey	Skey	groups
	10	Palani	chennaisunday.cs0177@gmail.com	123	7200157721	Chennai	j5sG148D1R	8a4GDj6EEa	(NULL)
	11	velu	chennaisunday.cs0177@gmail.com	abc	7200157721	Bangalore	(NULL)	8R666DblRa	(NULL)
	12	palanikumar	chennaisunday.cs0177@gmail.com	123	7200157721	Chennai	s3sD2682D5	lCCDsDs3ks	(NULL)
	13	nageswar	nageshp011996@gmail.com	12345678	6281348121	kadapa	b4Rb2RDCkD	8RDER4GaD3	(NULL)
	20	suresh	vadde.seetha@gmail.com	suresh	9666589655	Hyderabad	RGRk5CkG3a	b2CRG1j5C2	group1
*	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

The above stores files data including details of the user who uploaded it.

9 CONCLUSION

In this project, we proposed a secure data group sharing and dissemination scheme in public cloud based on attribute-based and timed-release conditional identity-based broadcast PRE. Our scheme allows users to share data with a group of receivers by using identity such as email and username at one time, which would guarantee data sharing security and convenience in public cloud. Besides, with the usage of fine-grained and timed-release CPRE, our scheme allows data owners to custom access policies and time trapdoors in the ciphertext which could limit the dissemination conditions when outsourcing their data. The CSP will re-encrypt the ciphertext successfully only when the attributes of data disseminator associated with the re-encryption key satisfy access policy in the initial ciphertext and the time trapdoors in the initial ciphertext are exposed. We conducted our experiments with pairing-based cryptography library. The theoretical analysis and experiment results have shown the security and efficiency of our scheme.

Future Enhancement

❖ We intent to propose time period key not to be based on operations instead strongly recommend generating time period key based on logging.

❖ Time period key should be generated with long time to avoid time consumption of frequent changing of keys

❖ The key generated should be generated automatically based on some time specification

10 BIBLIOGRAPHY

Good Teachers are worth more than thousand books, we have them in Our Department

1. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

2. G. Ateniese, R.D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. 4th International Conference on Security and Privacy in Communication Networks, 2008

3. F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data In- tegrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1-6, 2008.

4. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MRPPDP: Multiple-Replica Provable Data Possession," Proc. 28th IEEE International Conference on Distributed Computing Systems, pp. 411-420, 2008.

5. H. Shacham and B. Waters, "Compact Proofs of Retrievability," Advances in Cryptology-Asiacrypt'08, pp. 90-107, 2008.

6. C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

7. Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on Computer and Communications Security, pp. 756-758, 2010.

8. K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.

9. K. Yang and X. Jia, “An efficient and secure dynamic auditing protocol for data storage in cloud computing,” IEEE Trans. Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.

10. C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage,” IEEE Trans. Computers, Vol. 62, No. 2, pp. 362375, 2013.

Sites Referred:

www.cloudxl.com

www.cloud-computing.com

www.talkincloud.com

www.cloudcomputing.sys-con.com

www.virtualizationreview.com/Home.aspx

www.thecloudtutorial.com