A Project Report

On

A LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

Project Submitted in partial fulfillment of requirements for the Award of the Degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

JONNADA SAI TEJA

20U91A0555

Under the Esteemed guidance of

R. BHUVANESWARI M. Tech

Asst. Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SRI MITTAPALLI COLLEGE OF EGINEERING

(Approved by AICTE, New Delhi and Affiliated to JNTU Kakinada)

(An ISO 9001:2005 Certified Institution and Accredited by NAAC& NBA)

TUMMALAPALEM, NH-5, GUNTUR, 522233, A.P.

(2020-2024)

SRI MITTAPALLI COLLEGE OF ENGINEERIN

(Approved by AICTE, New Delhi and Affiliated to JNTU Kakinada)

(An ISO 9001:2005 Certified Institution and Accredited by NAAC & NBA)

TUMMALAPALEM, NH-5, GUNTUR, 522233, A.P.

CERTIFICATE

This is to certify that the project entitled **"A LIGHT WEIGHT SECURE DATA SHARING SCHEME FOR MOBLIE CLOUD COMPUTING "**is the Bonafede work of JONNADA SAI TEJA (20U91A0555), submitted in partial fulfillment of requirements for award degree of Bachelor of Technology in **COMPUTER SCIENCE AND ENGINEERING** by **JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, KAKINADA** during the year 2023-2024.

PROJECT GUIDE	**HEAD OF THE DEPARTMENT**
R. BHUVANESWARI **M. Tech**	**Dr. S. GOPI KRISHNA** **M. Tech, Ph. D**
Asst. Professor	**Professor & HOD**

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

I would like to express our utmost gratitude to our Chairman **Sri. M.V. KOTESWARA RAO** and Secretary Sri. **M.B.V. SATYANARAYANA** for providing their support and stimulating environment for the development of our project.

I express our deep sense of reverence and profound graduate **Dr. S. GOPI KRISHNA** **M.Tech, Ph.D.** Principal for providing us the great support for carrying out this project.

I extend our sincere thanks to **Dr. S. GOPI KRISHNA** **M. Tech, Ph.D,** Head of the Departmentof C.S.E for his co-operation and guidance to make this project successful.

I am also immensely thankful to our guide **Miss. R. Bhuvaneswari** **M. Tech**, for her moral support and guidance throughout the project. Our sincere thanks also go to all the teaching and non-teaching staff for their constant support and advice.

I would like to thank our friends who have helped us in the successful completion of this project, either directly or indirectly.

BY

JONNADA SAI TEJA

20U91A0555

DECLARATION

I am J. Sai Teja, declare that the contents of this project, in full or part, have not been submitted to any other university or institution for the award of any degree or diploma.

I also declare that we have adhered to all principles of academic honesty and integrity and not misrepresented or fabricated or falsified any idea/data/fact/source in our submission

I understand that any violation of the above will cause disciplinary action by the institution and can also evoke penal action for the sources which have not been properly cited or from whom proper permission has not been taken when needed.

BY

JONNADA SAI TEJA

20U91A0555

TABLE OF CONTENTS

S.NO **CHAPTER NAME** **PAGE.NO**

ABSTRACT

This paper is based on integration of the biomedical field and computer science. Paper contains the study of bone cancer and features to predict the type of the same. Related work to find cancer in human body using computer vision is discussed in this paper. Image segmentation technique like so bel, pre with, canny, K- means and Region Growing are described in this paper which can be stimulated for X-Ray and MRI image interpretation. Paper also shows the result of edge based and region-based image segmentation techniques applied on X-Ray image to detect osteosarcoma cancer present on bone using MATLAB. Finally, paper concluded by finding best suited segmentation method for grey scaled image with future aspects.

Bone tumors are abnormal growths of cells within bone tissue that can be benign or malignant, posing significant diagnostic challenges due to their diverse morphologies and locations. X-ray imaging remains one of the primary modalities for initial detection and assessment of bone tumors due to its widespread availability, cost- effectiveness, and ability to provide detailed structural information. This paper presents a comprehensive review of recent advancements in identifying bone tumors using X-ray images, focusing on various techniques, methodologies, and challenges encountered in clinical practice and research.

The review encompasses both traditional image processing approaches and modern deep learning-based methods for bone tumor detection, segmentation, classification, and characterization. It discusses the significance of feature extraction, image enhancement, and segmentation algorithms in preprocessing X-ray images to improve the accuracy and efficiency of tumor detection. Additionally, it explores the utilization of convolutional neural networks (CNNs) and other deep learning architectures for automated analysis of X-ray images, highlighting their strengths in learning discriminative features directly from raw pixel data.

CHAPTER-1

INTRODUCTION

INTRODUCTION

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.

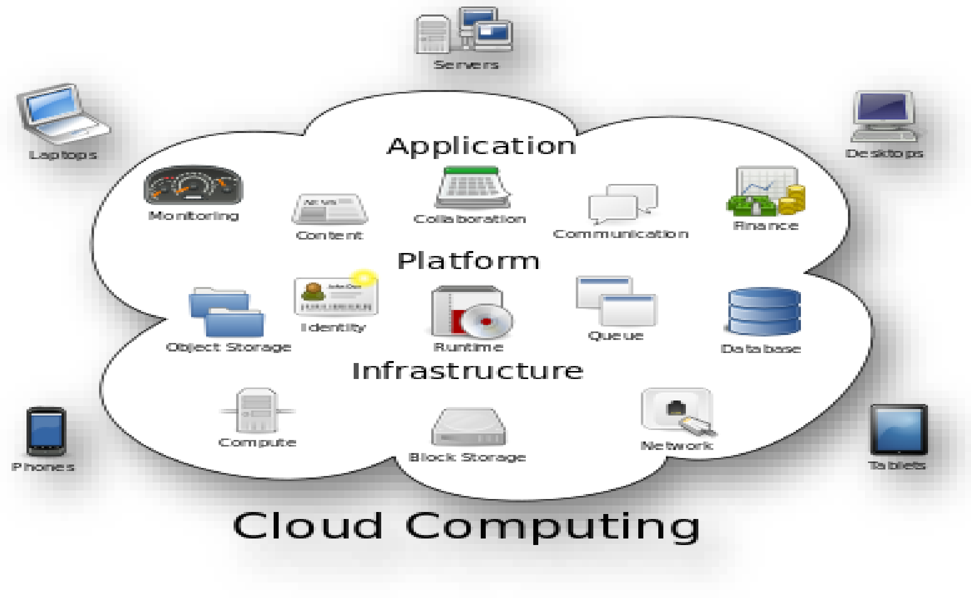


Fig: 1. Structure of cloud computing

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. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them.

1.1 CHARACTERISTICS

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

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

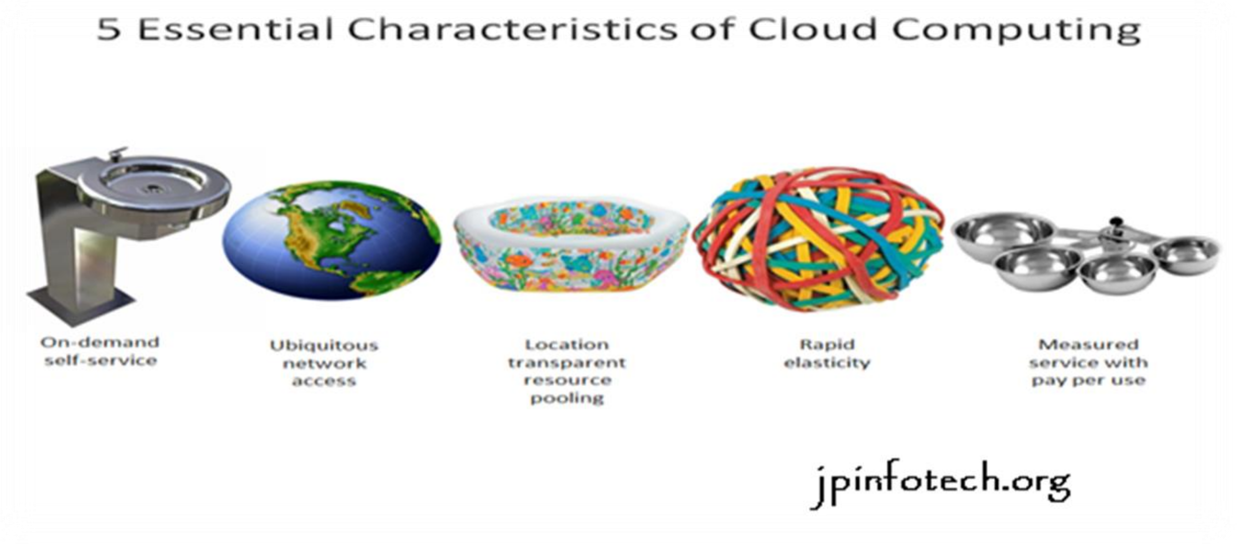

5 Essential Characteristics of Cloud Computing
On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use
jpinfotech.org

Fig: 2. Characteristics of cloud computing

1.2 SERVICES MODELS

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below.

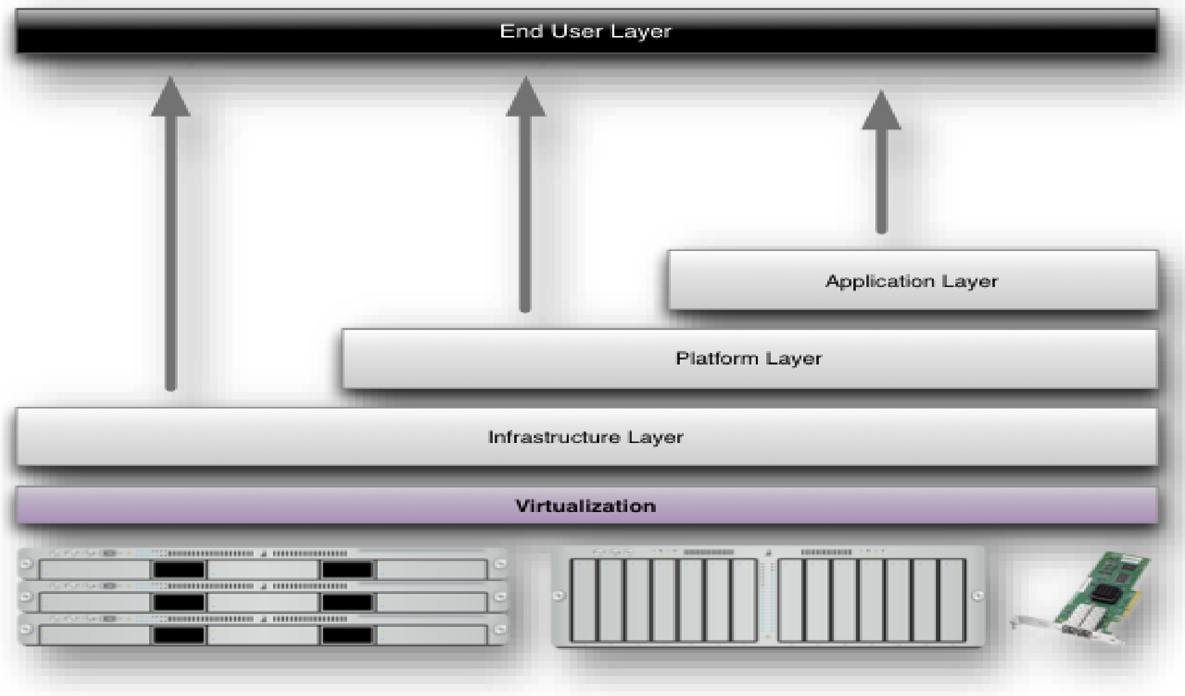


Fig: 3. Structure of service models

CHAPTER-2

LITERATURE SURVEY

LITERATURE SURVEY

1) **“Attribute-based fine-grained access control with efficient revocation in cloud storage systems”**

   A cloud storage service allows data owner to outsource their data to the cloud and through which provide the data access to the users. Because the cloud server and the data owner are not in the same trust domain, the semi-trusted cloud server cannot be relied to enforce the access policy. To address this challenge, traditional methods usually require the data owner to encrypt the data and deliver decryption keys to authorized users.

   These methods, however, normally involve complicated key management and high overhead on data owner. In this paper, we design an access control framework for cloud storage systems that achieves fine-grained access control based on an adapted Ciphertext-Policy Attribute-based Encryption (CP-ABE) approach. In the proposed scheme, an efficient attribute revocation method is proposed to cope with the dynamic changes of users' access privileges in large-scale systems.

2) **“Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data”**

   Considering the large number of on-demand data users and huge amount of outsourced data files in cloud, the problem is particularly challenging, as it is extremely difficult to meet also the practical requirements of performance, system usability, and high-level user searching experiences. In this paper, we investigate the problem of secure and efficient similarity search over outsourced cloud data. Similarity search is a fundamental and powerful tool widely used in plaintext information retrieval, but has not been quite explored in the encrypted data domain. Our mechanism design first exploits a suppressing technique to build storage-efficient similarity keyword set from a given document collection, with edit distance as the similarity metric.

3) **“Effective Data Access Control for Multiauthority Cloud Storage Systems”**

   Data access control is an effective way to ensure data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising technique for access control of encrypted data. However, due to the inefficiency of decryption and revocation, existing CP-ABE schemes cannot be directly applied to construct a data access control scheme for multiauthority cloud storage systems, where users may hold attributes from multiple authorities.

4) “Attribute based proxy re-encryption with delegating capabilities”

Attribute based proxy re-encryption scheme (ABPRE) is a new cryptographic primitive which extends the traditional proxy re-encryption (public key or identity-based cryptosystem) to the attribute-based counterpart, and thus empower users with delegating capability in the access control environment. Users, identified by attributes, could freely designate a proxy who can re-encrypt a ciphertext related with a certain access policy to another one with a different access policy.

CHAPTER-3

SYSTEM ANALYSIS

SYSTEM ANALYSIS

3.1 Existing System

In general, we can divide these approaches into four categories: simple ciphertext access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-based encryption (ABE). All these proposals are designed for non-mobile cloud environment. Tysowski et al. considered a specific cloud computing environment where data are accessed by resource-constrained mobile devices, and proposed novel modifications to ABE, which assigned the higher computational overhead of cryptographic operations to the cloud provider and lowered the total communication cost for the mobile user.

Disadvantages of existing system:

- Data privacy of the personal sensitive data is a big concern for many data owners.
- The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or not very convenient.
- They cannot meet all the requirements of data owners.
- They consume large amount of storage and computation resources, which are not available for mobile devices
- Current solutions don't solve the user privilege change problem very well. Such an operation could result in very high revocation cost. This is not applicable for mobile devices as well.

3.2 Proposed System

We propose a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment. We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over ciphertext. We use proxy servers for encryption and decryption operations. In our approach, computationally intensive operations in ABE are conducted on proxy servers, which greatly reduce the computational overhead on client-side mobile devices. Meanwhile, in LDSS-CP-ABE, in order to maintain data privacy, a version attribute is also added to the access structure.

We introduce lazy re-encryption and description field of attributes to reduce the revocation overhead when dealing with the user revocation problem. Finally, we implement a data sharing prototype framework based on LDSS.

Advantages of proposed system:

- The experiments show that LDSS can greatly reduce the overhead on the client side, which only introduces a minimal additional cost on the server side.
- Such an approach is beneficial to implement a realistic data sharing security scheme on mobile devices.
- The results also show that LDSS has better performance compared to the existing ABE based access control schemes over ciphertext.
- Multiple revocation operations are merged into one, reducing the overall overhead
- In LDSS, the storage overhead needed for access control is very small compared to data

CHAPTER-4

SYSTEM REQUIRMENTS

SYSTEM REQUIREMENT

4.1 Hardware Requirements:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

4.2 Software Requirements:

- Operating system : - Windows XP/7.
- Coding Language : JAVA/J2EE
- Data Base : M

4.3 System Study Feasibility Study

The feasibility of the project is analysed 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.

- **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.

- **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 level of acceptance by the users solely depends on the methods that are employed to educate the user about the systeand 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.

4.4 Input design and output design

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.

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.

CHAPTER – 5

SYSTEM DESIGN

SYSTEM DESIGN

5.1 SYSTEM ARCHITECTURE:

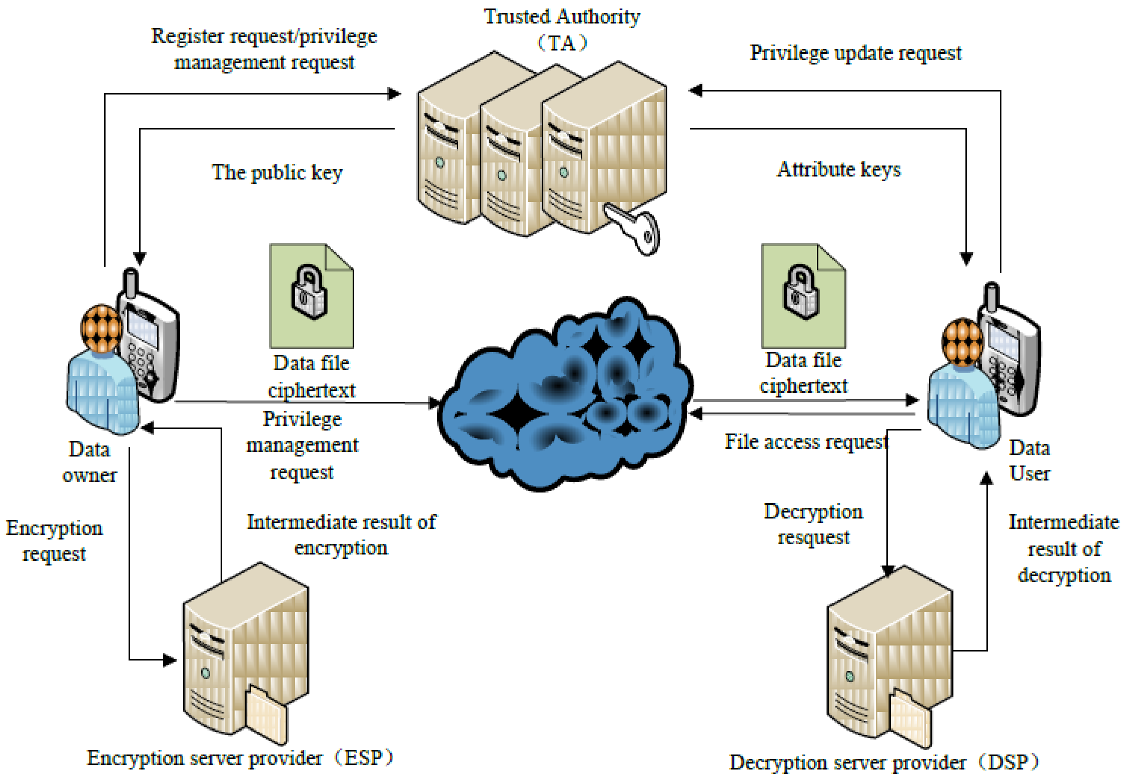

Trusted Authority
（TA）
Register request/privilege management request
Privilege update request
The public key
Attribute keys
Data file ciphertext
Data file ciphertext
Privilege management request
File access request
Data owner
Data User
Encryption request
Intermediate result of encryption
Decryption resquest
Intermediate result of decryption
Encryption server provider（ESP）
Decryption server provider（DSP）

Fig: 1 System Architecture

5.2 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 modelling tools. It is used to model the system components
- 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.

- DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional deta

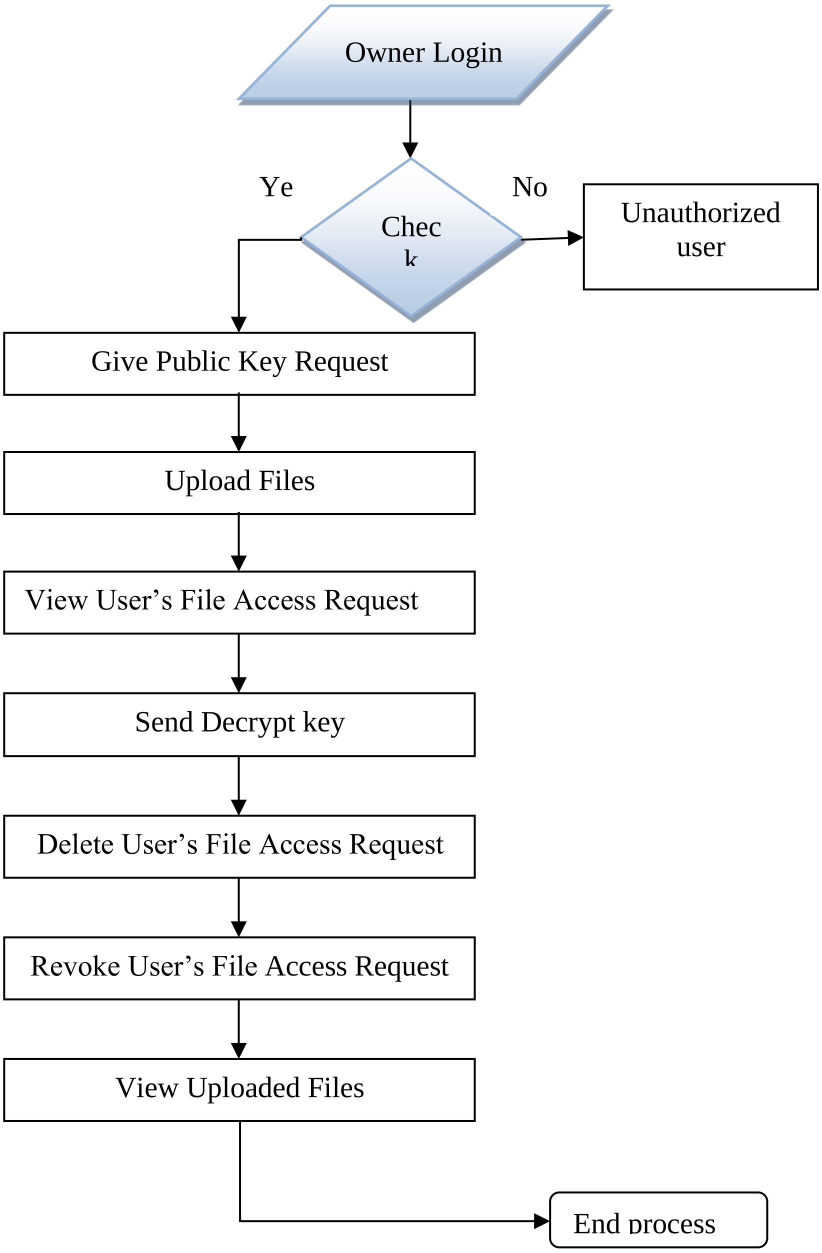


Fig 1 Data Flow

5.3 UML DIAGRAM:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of +object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML

GOALS:

- Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
- Provide extendibility and specialization mechanisms to extend the core concepts.
- Be independent of particular programming languages and development process.
- Provide a formal basis for understanding the modeling language.
- Encourage the growth of OO tools market.
- Support higher level development concepts such as collaborations, frameworks, patterns and components.
- Integrate best practices.

5.4 USE CASE DIAGRAM

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral 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.

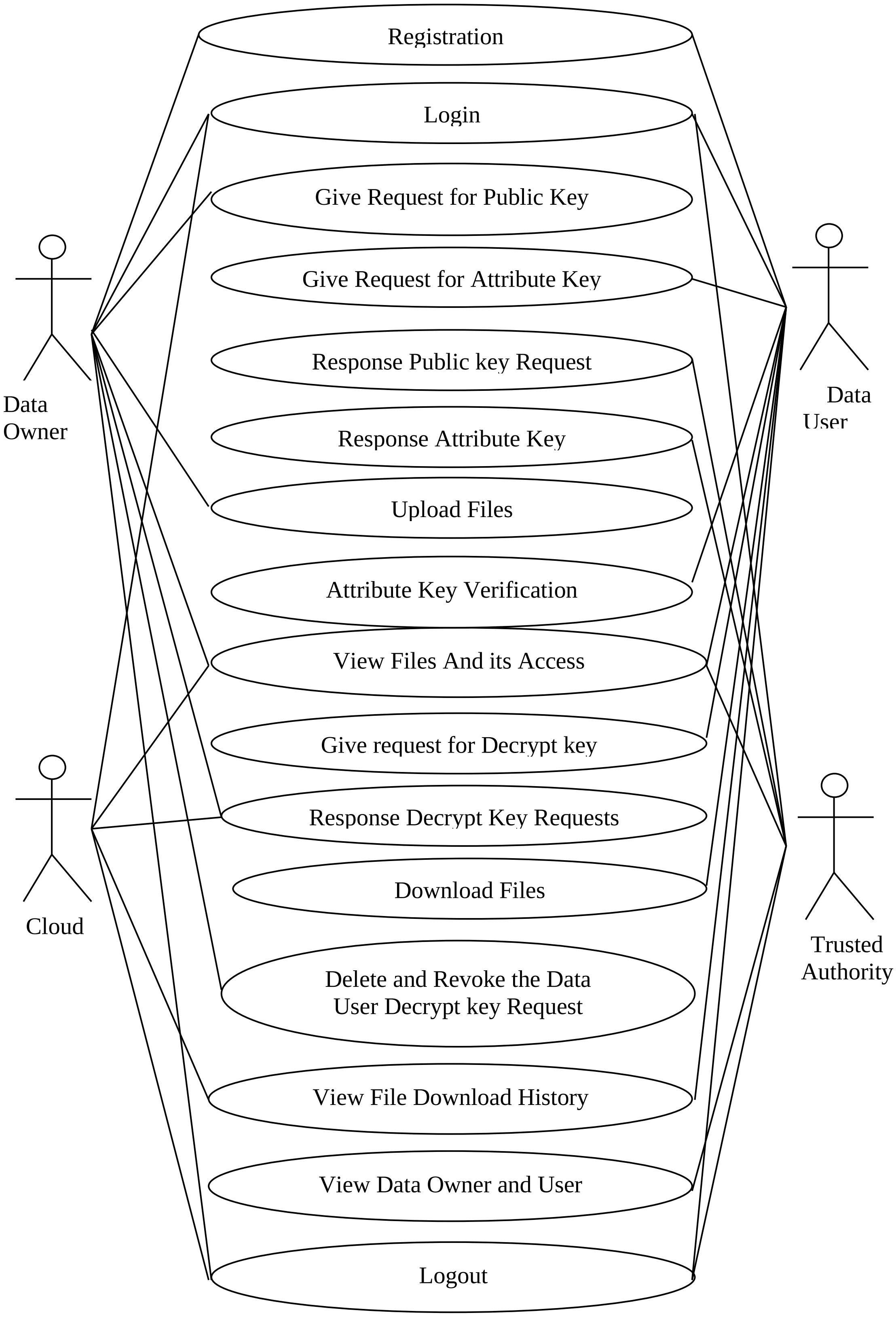
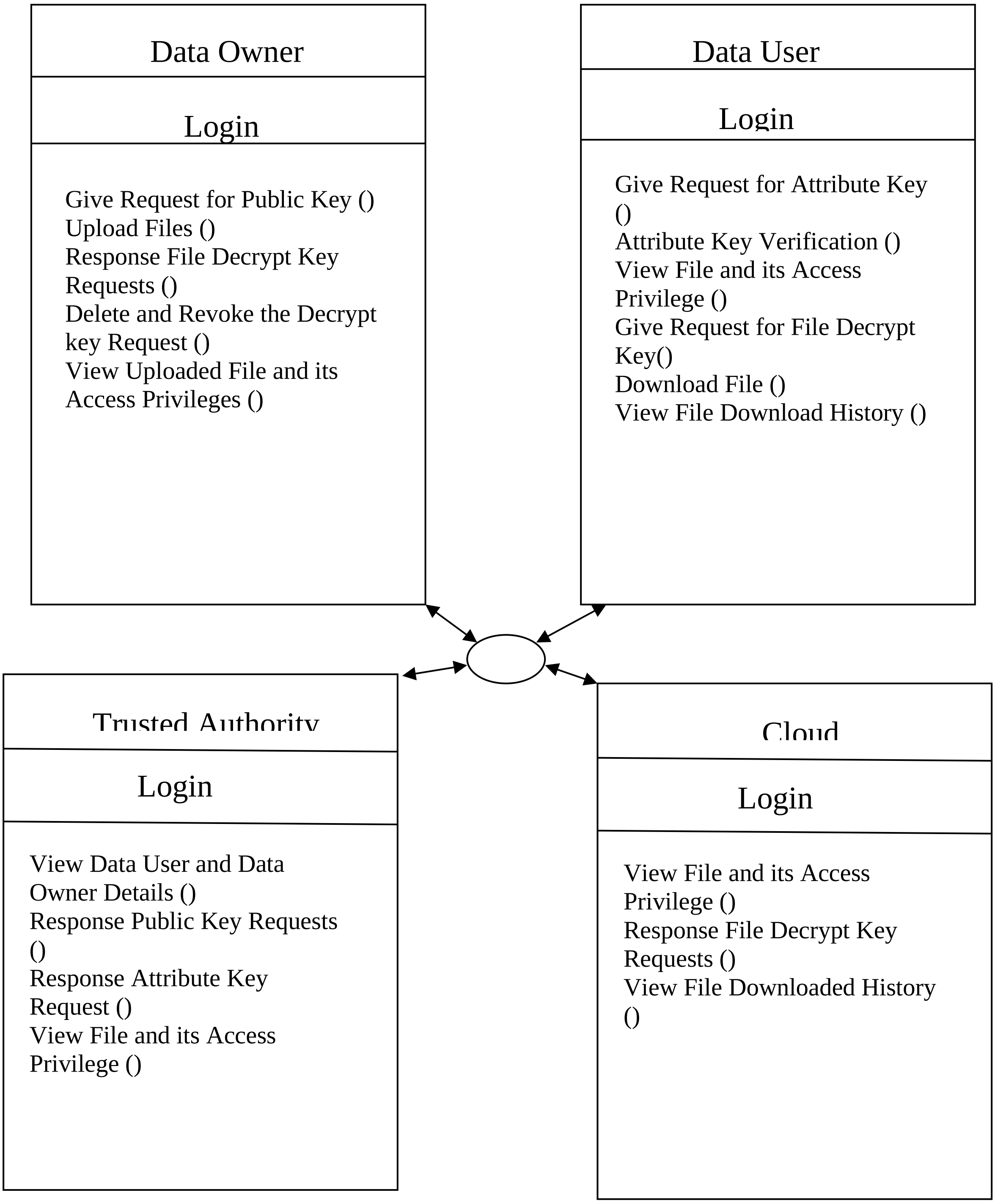

Registration
Login
Give Request for Public Key
Give Request for Attribute Key
Response Public key Request
Response Attribute Key
Upload Files
Attribute Key Verification
View Files And its Access
Give request for Decrypt key
Response Decrypt Key Requests
Download Files
Delete and Revoke the Data User Decrypt key Request
View File Download History
View Data Owner and User
Logout
Data Owner
Data User
Cloud
Trusted Authority

Fig: 3. Use Case

5.5 CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

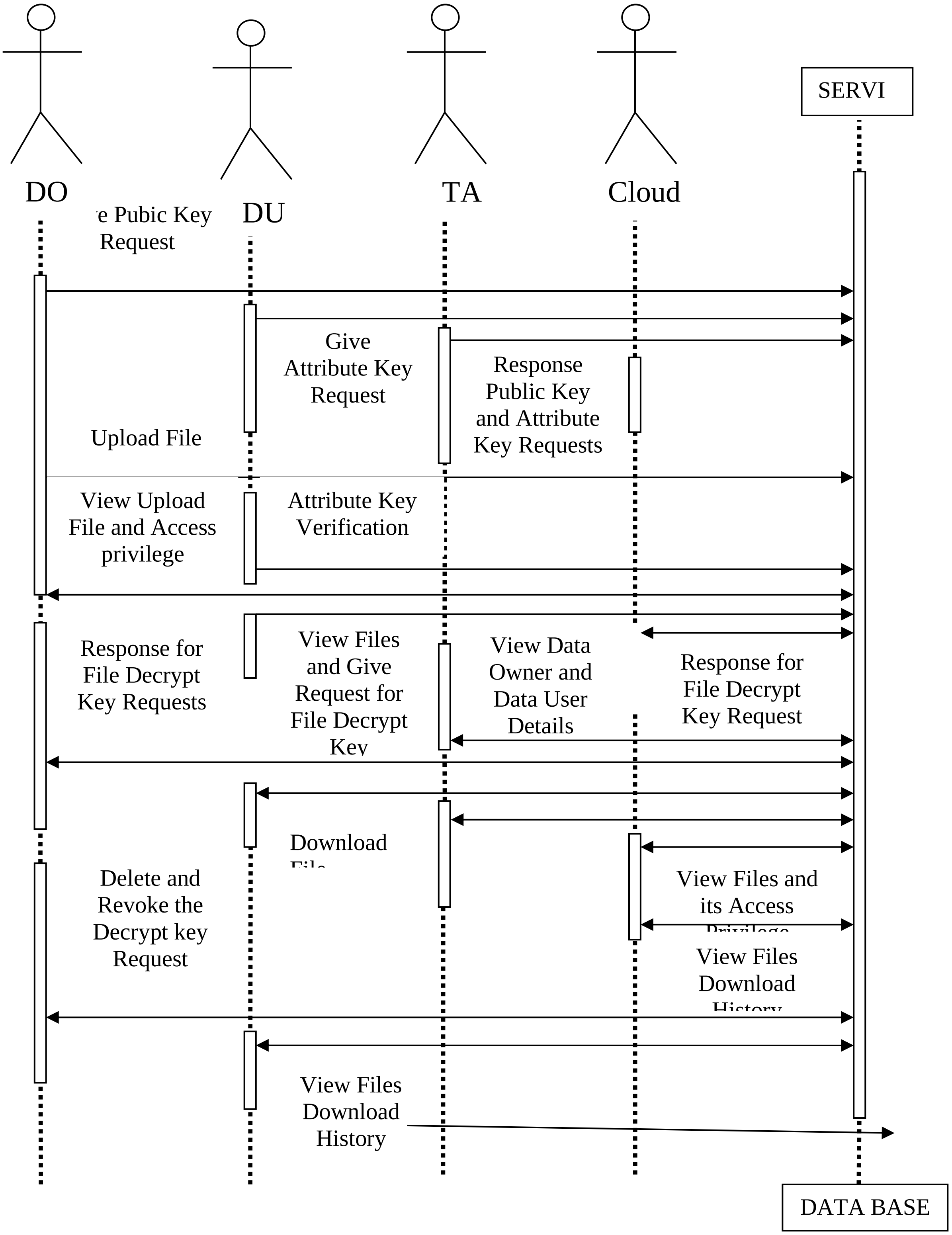


Data Owner
Login
Give Request for Public Key ()
Upload Files ()
Response File Decrypt Key Requests ()
Delete and Revoke the Decrypt key Request ()
View Uploaded File and its Access Privileges ()
Data User
Login
Give Request for Attribute Key ()
Attribute Key Verification ()
View File and its Access Privilege ()
Give Request for File Decrypt Key()
Download File ()
View File Download History ()
Trusted Authority
Login
View Data User and Data Owner Details ()
Response Public Key Requests ()
Response Attribute Key Request ()
View File and its Access Privilege ()
Cloud
Login
View File and its Access Privilege ()
Response File Decrypt Key Requests ()
View File Downloaded History ()

Fig: 4. Class Diagram

5.6 SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order.



DO
DU
TA
Cloud
SERVI
e Pubic Key Request
Give Attribute Key Request
Response Public Key and Attribute Key Requests
Upload File
View Upload File and Access privilege
Attribute Key Verification
Response for File Decrypt Key Requests
View Files and Give Request for File Decrypt Key
View Data Owner and Data User Details
Response for File Decrypt Key Request
Download File
Delete and Revoke the Decrypt key Request
View Files and its Access Privilege
View Files Download History
View Files Download History
DATA BASE

Fig: 5. Sequence Diagram

5.7 ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency.

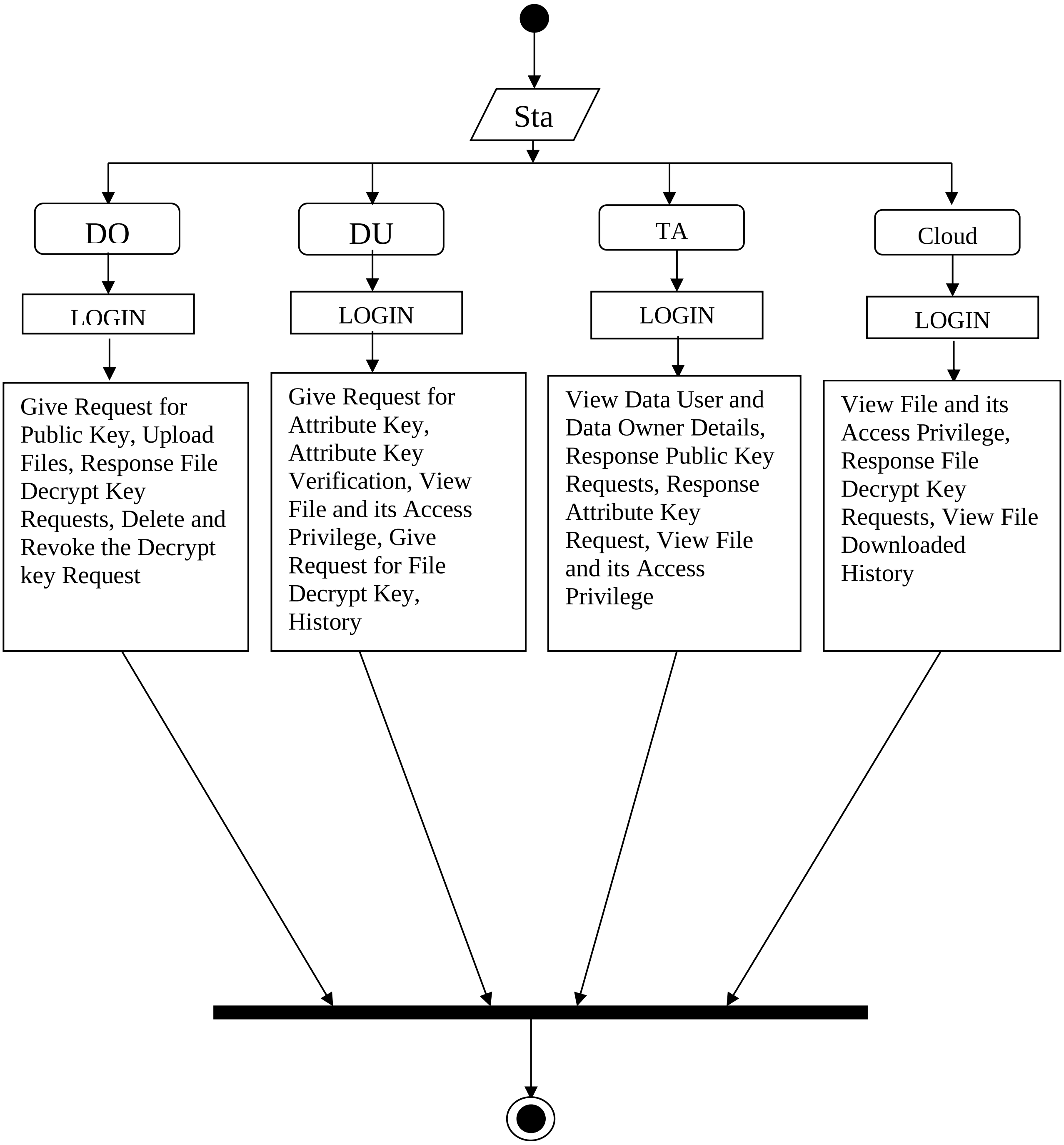

Sta
DO
DU
TA
Cloud
LOGIN
LOGIN
LOGIN
LOGIN
Give Request for Public Key, Upload Files, Response File Decrypt Key Requests, Delete and Revoke the Decrypt key Request
Give Request for Attribute Key, Attribute Key Verification, View File and its Access Privilege, Give Request for File Decrypt Key, History
View Data User and Data Owner Details, Response Public Key Requests, Response Attribute Key Request, View File and its Access Privilege
View File and its Access Privilege, Response File Decrypt Key Requests, View File Downloaded History

Fig: 6. Activity Diagram

CHAPTER – 6

IMPLEMENTATION

IMPLEMENTATION

8.1 MODULES:

- System Framework
- Data Owner
- Data User
- Trusted Authority
- Cloud Service Provider

8.2 MODULES DESCRIPTION:

8.2.1 System Framework:

The development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. In these applications, people (data owners) can upload their documents and other files to the cloud and share these data with other people (data users) they like to share. Clearly, data privacy of the personal sensitive data is a big concern for many data owners.

8.2.2 Data Owner (DO):

When the data owner (DO) registers on TA, TA runs the algorithm Setup () to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TA itself. DO defines its own attribute set and assigns attributes to its contacts. All these information will be sent to TA and the cloud. TA and the cloud receive the information and store it. DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies. DO sends data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU should obtain if he wants to access a certain data file.

8.2.3 Data User (DU):

DU logins onto the system and sends, an authorization request to TA. The authorization request includes attribute keys (SK) which DU already has. TA accepts the authorization request and checks the request and a generate attribute keys (SK) for DU. DU sends a request for data to the cloud-Cloud receives the request and checks if the DU meets the access requirement. DU receives the ciphertext, which includes ciphertext of data files and ciphertext of the symmetric key.

8.3.4 Trusted Authority:

To make LDSS feasible in practice, a trusted authority (TA) is introduced. It is responsible of generating public and private keys, and distributing attribute keys to users. With this mechanism, users can share and access data without being aware of the encryption and decryption operations. We assume TA is entirely credible, and a trusted channel exists between the TA and every user. The fact that a trusted channel exists doesn't mean that the data can be shared through the trusted channel, for the data can be in a large amount.

8.2.5 Cloud Service Provider:

CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud. DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement.

CHAPTER - 7

TECHNOLOGY DESCRIPTION

TECHNOLOGY DESCRIPTION

7.1 JAVA

Java technology is both a programming language and a platform. The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple
- Architecture neutral
- Object oriented
- Portable
- Distributed
- High performance
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted.

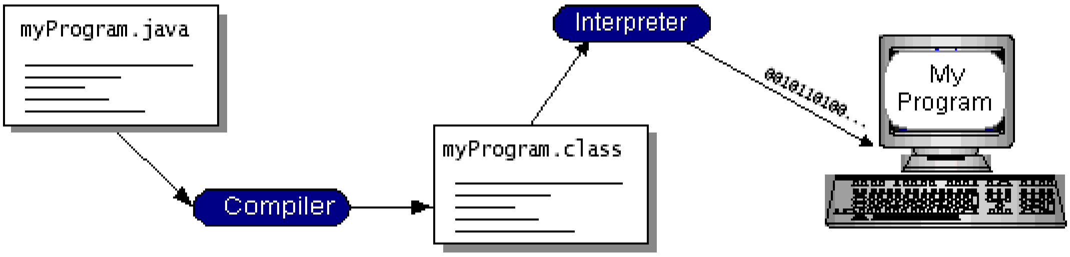
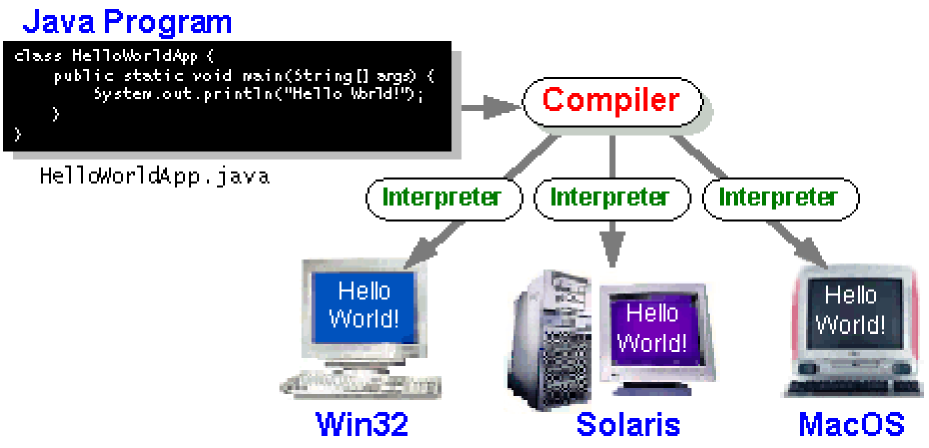


Fig: 1. Code Run

You can think of Java byte codes as the machine code instructions for the *Java Virtual Machine* (Java VM). Every Java interpreter, whether it’s a development tool or a Web browser that can run applets, is an implementation of the Java VM.



```
class HelloWorldApp {
    public static void main(String[] args) {
        System.out.println("Hello World!");
    }
}
```

Fig: 2. Compiler

7.1.1 The Java Platform:

A platform is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Windows 2000, Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms.

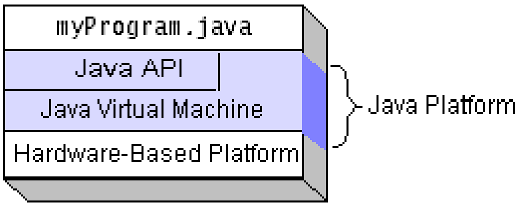


Fig: 3. java. Platform

Native code is code that after you compile it, the compiled code runs on a specific hardware platform. As a platform-independent environment, the Java platform can be a bit slower than native

7.1.2 ODBC:

Microsoft Open Database Connectivity (ODBC) is a standard programming interface for application developers and database systems providers. Before ODBC became a *de facto* standard for Windows programs to interface with database systems, programmers had to use proprietary languages for each database they wanted to connect to. Now, ODBC has made the choice of the database system almost irrelevant from a coding perspective, which is as it should be.

7.1.3 JDBC

In an effort to set an independent database standard API for Java; Sun Microsystems developed Java Database Connectivity, or JDBC. JDBC offers a generic SQL database access mechanism that provides a consistent interface to a variety of RDBMSs. This consistent interface is achieved through the use of "plug-in" database connectivity modules, or drivers. If a database vendor wishes to have JDBC support, he or she must provide the driver for each platform that the database and Java run on.

JDBC Goals

Few software packages are designed without goals in mind. JDBC is one that, because of its many goals, drove the development of the API. These goals, in conjunction with early reviewer feedback, have finalized the JDBC class library into a solid framework for building database applications in Java. The goals that were set for JDBC are important. They will give you some insight as to why certain classes and functionalities behave the way they do. The eight design goals for JDBC are as follows:

1. **SQL Level API**

   The designers felt that their main goal was to define a SQL interface for Java. Although not the lowest database interface level possible, it is at a low enough level for higher-level tools and APIs to be created. Conversely, it is at a high enough level for application programmers to use it confidently. Attaining this goal allows for future tool vendors to "generate" JDBC code and to hide many of JDBC's complexities from the end user.

2. **SQL Conformance**

   SQL syntax varies as you move from database vendor to database vendor. In an effort to support a wide variety of vendors, JDBC will allow any query statement to be passed through it to the underlying database driver. This allows the connectivity module to handle non-standard functionality in a manner that is suitable for its users.

3. **JDBC must be implemental on top of common database interfaces**

   The JDBC SQL API must "sit" on top of other common SQL level APIs. This goal allows JDBC to use existing ODBC level drivers by the use of a software interface. This interface would translate JDBC calls to ODBC and vice versa.

4. **Provide a Java interface that is consistent with the rest of the Java system**

   Because of Java's acceptance in the user community thus far, the designers feel that they should not stray from the current design of the core Java system.

5. **Keep it simple**

   This goal probably appears in all software design goal listings. JDBC is no exception. Sun felt that the design of JDBC should be very simple, allowing for only one method of completing a task per mechanism. Allowing duplicate functionality only serves to confuse the users of the API.

6. **Use strong, static typing wherever possible**

   Strong typing allows for more error checking to be done at compile time; also, less error appear at runtime.

7. **Keep the common cases simple**

Because more often than not, the usual SQL calls used by the programmer are simple SELECT's, INSERT's, DELETE's and UPDATE's, these queries should be simple to perform with JDBC. However, more complex SQL statements should also be possible.

Finally, we decided to proceed the implementation using Java Networking.

And for dynamically updating the cache table we go for MS Access database.

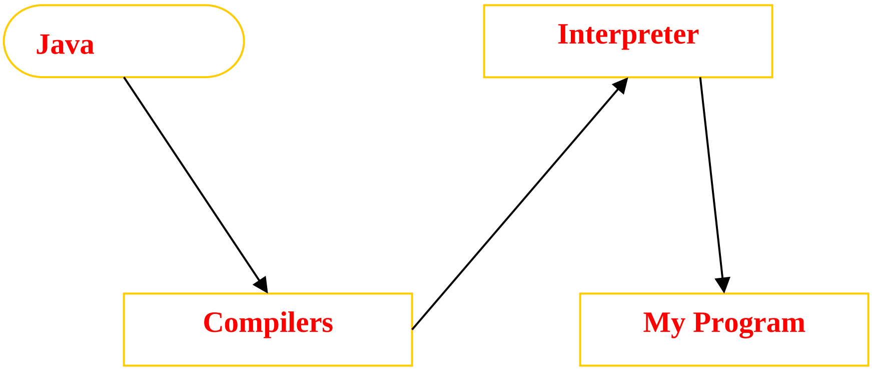


Fig: 5. Java VM

You can think of Java byte codes as the machine code instructions for the Java Virtual Machine (Java VM). Every Java interpreter, whether it's a Java development tool or a Web browser that can run Java applets, is an implementation of the Java VM. The Java VM can also be implemented in hardware. Java byte codes help make "write once, run anywhere" possible. You can compile your Java program into byte codes on my platform that has a Java compiler.

8. Networking

The TCP/IP stack is shorter than the OSI one:

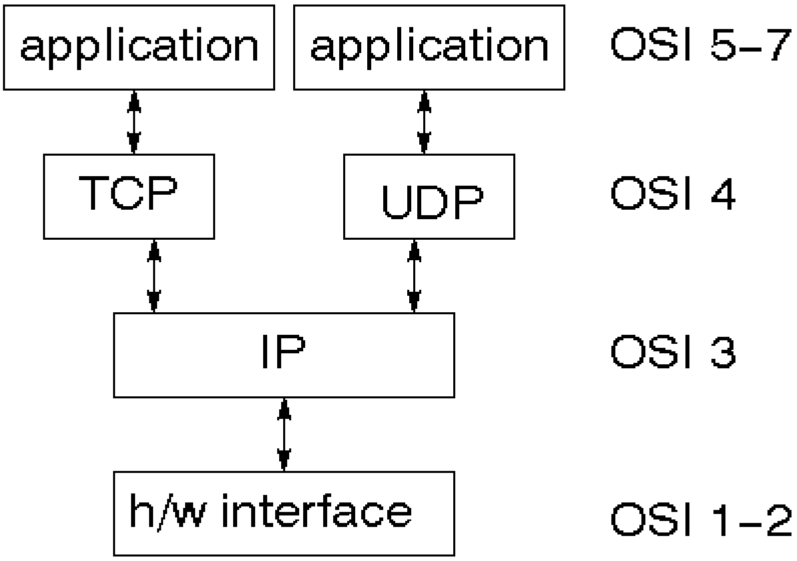


Fig: 6. Use Datagram Protocol

9. IP datagram's

The IP layer provides a connectionless and unreliable delivery system. It considers each datagram independently of the others. Any association between datagram must be supplied by the higher layers. The IP layer supplies a checksum that includes its own header. The header includes the source and destination addresses.

10. UDP

UDP is also connectionless and unreliable. What it adds to IP is a checksum for the contents of the datagram and port numbers. These are used to give a client/server model - see later.

11.TCP

TCP supplies logic to give a reliable connection-oriented protocol above IP. It provides a virtual circuit that two processes can use to communicate.

12.Internet Addresses

In order to use a service, you must be able to find it. The Internet uses an address scheme for machines so that they can be located. The address is a 32-bit integer which gives the IP address. This encodes a network ID and more addressing. The network ID falls into various classes according to the size of the network address.

13.Network Address

Class A uses 8 bits for the network address with 24 bits left over for other addressing. Class B uses 16- bit network addressing. Class C uses 24 -bit network addressing and class D uses all 32.

14. Subnet Address

Internally, the UNIX network is divided into sub networks. Building 11 is currently on one sub network and uses 10-bit addressing, allowing 1024 different hosts.

15. Host Address

8 bits are finally used for host addresses within our subnet. This places a limit of 256 machines that can be on the subnet.

16.Total Address

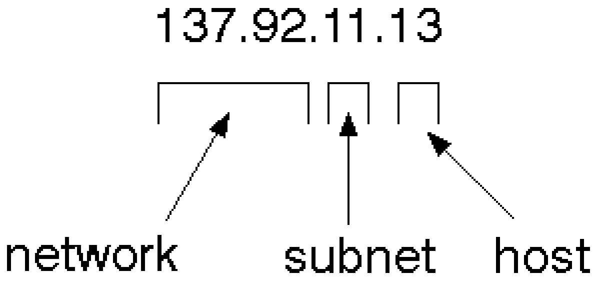


Fig: 7. Address Diagram

17.Port Addresses

A service exists on a host, and is identified by its port. This is a 16- bit number. To send a message to a server, you send it to the port for that service of the host that it is running on. This is not location transparency! Certain of these ports are "well known".

18. Sockets

A socket is a data structure maintained by the system to handle network connections. A socket is created using the call socket. It returns an integer that is like a file descriptor. In fact, under Windows, this handle can be used with Read File and Write File functions.

7.2 J2ME (Java 2 Micro edition):

Sun Microsystems defines J2ME as "a highly optimized Java run-time environment targeting a wide range of consumer products, including pagers, cellular phones, screen-phones, digital set-top boxes and car navigation systems." Announced in June 1999 at the JavaOne Developer Conference, J2ME brings the cross-platform functionality of the Java language to smaller devices, allowing mobile wireless devices to share applications.

7.2.1. General J2ME architecture

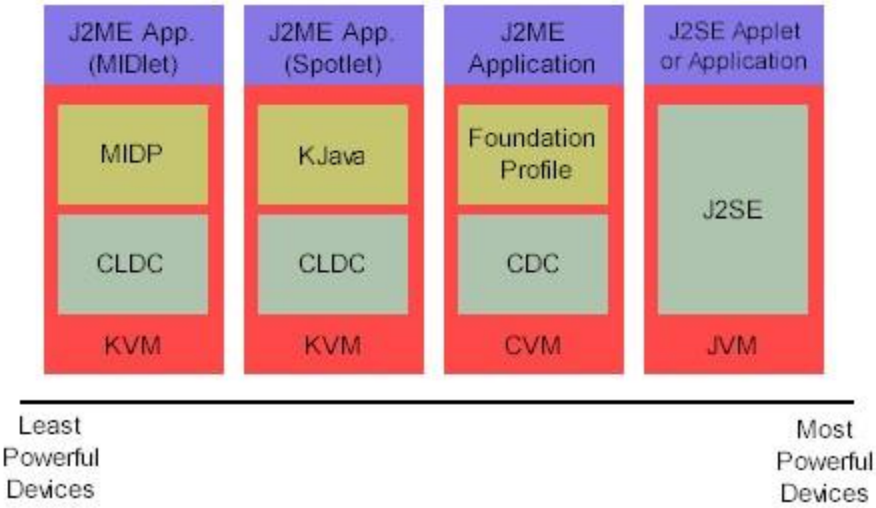


Fig: J2ME Diagram

J2ME uses configurations and profiles to customize the Java Runtime Environment (JRE). As a complete JRE, J2ME is comprised of a configuration, which determines the JVM used, and a profile, which defines the application by adding domain-specific classes.

7.2.2. Developing J2ME applications

Introduction In this section, we will go over some considerations you need to keep in mind when developing applications for smaller devices. We'll take a look at the way the compiler is invoked when using J2SE to compile J2ME applications. Finally, we'll explore packaging and deployment and the role precertification plays in this process.

7.2.3. Design considerations for small devices

Developing applications for small devices requires you to keep certain strategies in mind during the design phase. It is best to strategically design an application for a small device before you begin coding. Correcting the code because you failed to consider all of the "gotchas" before developing the application can be a painful process. Here are some design strategies to consider:

7.2.4. Configurations overview

The configuration defines the basic run-time environment as a set of core classes and a specific JVM that run on specific types of devices. Currently, two configurations exist for J2ME, though others may be defined in the future:

7.2.5. J2ME profiles

KJava is Sun's proprietary profile and contains the KJava API. The KJava profile is built on top of the CLDC configuration. The KJava virtual machine, KVM, accepts the same byte codes and class file format as the classic J2SE virtual machine. KJava contains a Sun-specific API that runs on the Palm OS MIDP is geared toward mobile devices such as cellular phones and pagers. The MIDP, like KJava, is built upon CLDC and provides a standard run-time environment that allows new applications and services to be deployed dynamically on end user devices. MIDP is a common, industry-standard profile for mobile devices that is not dependent on a specific vendor. It is a complete and supported foundation for mobile application.

CHAPTER – 8

SYSTEM TESTING

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

8.1 TYPES OF TESTS

8.1.1 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.

8.1.2 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.

8.1.3 Functional testing

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.

8.1.4 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.

8.1.7 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.

CHAPTER – 09

CODING

CODING

Index.html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Home Page</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="css/style.css" rel="stylesheet" type="text/css" />
<link rel="stylesheet" type="text/css" href="css/coin-slider.css" />
<script type="text/javascript" src="js/cufon-yui.js"></script>
<script type="text/javascript" src="js/cufon-times.js"></script>
<script type="text/javascript" src="js/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="js/script.js"></script>
<script type="text/javascript" src="js/coin-slider.min.js"></script>
<style type="text/css">
<!—
. style1 {
        color: #FF0000;
        font-weight: bold;
        }
. style2 {font-size: 18px}
. style3 {font-size: 24px}
-->
</style>
</head>
<body>
<div class="main">
        <div class="header">
        <div class="header resize">
        <div class="logo">
        <h1><a href="index.html" class="style3">A Lightweight Secure Auditing Scheme for Shared Data in
Cloud Storage</a></h1>
        </div>
        <div class="menu_nav">
        <ul>
<li class="active"><a href="index.html"><span>Home    Page</span></a></li>
```

```
        <li><a href="cs_login.jsp"><span>Cloud</span></a></li>
        <li><a href="au_login.jsp"><span>TPM</span></a></li>
        <li><a href="do_login.jsp52"><span>Data Owner</span></a></li>
        <li><a href="dr_login.jsp"><span>Group Member</span></a></li>
        </ul>
        </div>
        <div class="clr"></div>
        <div class="slider">
        <div id="coin-slider"> <a href="#"><img src="images/slide1.jpg" width="960" height="360" alt=""
/></a> <a href="#"><img src="images/slide2.jpg" width="960" height="360" alt="" /></a> <a href="#"><img
src="images/slide3.jpg" width="960" height="360" alt="" /></a>
        </div>
        <div class="clr"></div>
        </div>
        <div class="clr"></div>
        </div>
</div>
<div class="content">
<div class="content_resize">
<div class="mainbar">
<div class="article">
<h2 class="style3">A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage</h2>
        <ul class="ex_menu">
        <li><strong>Shared data, virtual TPM pool, lightweight calculation, agent security. </strong></li>
        </ul>
    <div class="clr"></div>
<div class="img"><img src="images/img1.jpg" width="206" height="287" alt="" class="fl" /></div>
<div class="post_content">
        <p align="justify" class="style1">A cloud platform provides users with shared data storage services.
To ensure shared data integrity, it is necessary to validate the data effectively. An audit scheme that enables
group members to modify data conducts the integrity verication of the shared data, but this approach results in
complex calculations for the group members. The audit scheme of the designated agent implements a lightweight
calculation for the group members, but it ignores the security risks between the group members and the agents.
By introducing Hashgraph technology and designing a Third-Party Medium (TPM) management strategy, a
lightweight secure auditing scheme for shared data in cloud storage (LSSA) is proposed, which achieves security
management of the groups and a lightweight calculation for the group members. Meanwhile, a virtual TPM pool
is constructed by combining the TCP sliding window technology and interconnected functions to improve agent
security. We evaluate our scheme in numerical analysis and in experiments, the results of which demonstrate
that our scheme achieves lightweight computing for the group members and ensures the data verication process
for security.</p>
```

```
div>
<div class="clr"></div>
</div>
<div class="article">
<div class="clr"></div>
</div>
</div>
<div class="sidebar">
<div class="search form">
 <form id="form search" name="form search" method="post" action="#">
<span>
<input name="editbox_search" class="editbox_search" id="editbox_search" maxlength="80"
value="Search our ste:" type="text" />
</span>
<input name="button search" src="images/search.gif" class="button search" type="image" />
</form>
</div>
<div class="clr"></div>
<div class="gadget">
<h2 class="star"><span>Sidebar</span> Menu</h2>
<div class="clr"></div>
<ul class="sb_menu">
<li><a href="index.html">Home Page</a></li>
<li><a href="cs_login.jsp">Cloud</a></li>
<li><a href="au_login.jsp">TPM</a></li>
<li><a href="do_login.jsp">Data Owner</a></
<li><a href="dr_login.jsp">Group Member</a></li>
</ul>
</div>
<div class="gadget">
<h2 class="star"><span>Concepts</span></h2>
<div class="clr"></div>
<ul class="ex_menu"><li><strong>Shared data, <br />
virtual TPM pool, <br />
lightweight calculation, <br />
agent security.</strong></li>
</ul>
</div>
</div>
```

```
		<div class="clr"></div>
		</div>
	</div>
	<div class="fbg`"></div>
	<div class="footer">
	<div class="footer_resize">
		<div style="clear: both;"></div>
		</div>
		</div>
	</div>
	<div align=center></div>
	</body>
	</html
```

cs login’s

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Cloud Login</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />\
<link href="css/style.css" rel="stylesheet" type="text/css" />
<link rel="stylesheet" type="text/css" href="css/coin-slider.css" />
<script type="text/javascript" src="js/cufon-yui.js"></script>
<script type="text/javascript" src="js/cufon-times.js"></script>
<script type="text/javascript" src="js/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="js/script.js"></script>
<script type="text/javascript" src="js/coin-slider.min.js"></script>
<script language="javascript" type="text/javascript">
function valid ()
{
var na3=document.s. userid.value;
if(na3=="")
{
alert ("Please Enter Name");
document.s. userid. Focus ();
return false;
}
Else
{
}
var na4=documents. pass. Value;
if(na4=="")
{
Alert ("Please Enter Password");
document.s. pass. Focus ();return false;
}
}
</script>
<style type="text/css">
```

```
<!—
. style1 {font-family: "Times New Roman", Times, serif}
. style2 {font-size: 15px}
. style3 {color: #1e5381}
. style4 {font-size: 20px}
. style5 {font-weight: bold}
. style7 {
 font-weight: bold;
 color: #ffae00;
}
. style9 {color: #ffae00}
. style10 {font-size: 24px}
-->
</style>
</head>
<body>
<div class="main">
 <div class="header">
  <div class="header resize">
   <div class="logo">
    <h1><a href="index.html" class="style10">A Lightweight Secure Auditing
Scheme for Shared Data in Cloud Storage</a></h1>
   </div>
   <div class="menu_nav">
    <ul>
     <li><a href="index.html"><span>Home Page</span></a></li>
     <li class="active"><a href="cs_login.jsp"><span>Cloud</span></a></li>
     <li><a href="au_login.jsp"><span>TPM</span></a></li>
     <li><a href="do_login.jsp"><span>Data Owner</span></a></li>
     <li><a href="dr_login.jsp"><span>Group Member</span></a></li>
    </ul>
   </div>
   <div class="clr"></div>
   <div class="slider">
<div id="coin-slider"> <a href="#"><img src="images/slide1.jpg" width="960" height="360" alt="" /></a>
<a href="#"><img src="images/slide2.jpg" width="960" height="360" alt="" /></a>
<a href="#"><img src="images/slide3.jpg" width="960" height="360" alt="" /></a>
 </div>
<div class="clr"></div>
```

```
   </div>
   <div class="clr"></div>
  </div>
 </div>
 <div class="content">
  <div class="content_resize">
   <div class="mainbar">
    <div class="article">
     <h2 align="center"> Cloud Login </h2>
     <p>&nbsp;</p>
<form name="s" action="cs_authentication.jsp" method="post" onSubmit="return valid ()" ons target="_top">
  <table align="center" border="1" width="57%" height="179">
       <tr>
   <td width="48%" height="46" bgcolor="#333333" class="style4 style2"><span class="style4 style3 style1
style7 style9"><strong> Name </strong></span></td>
         <td width="55%" height="46" bgcolor="#333333"><input type="text" name="userid" size="18"/>
       </td>
          </tr>
          <tr>
            <td width="48%" height="40" bgcolor="#333333" class="style5 style2"> <span class="style4
style1
       style9"><strong>Password</strong></span></td>
<td width="55%" height="40" bgcolor="#333333"><input type="password" name="pass" size="18"/></td>
          </tr>
       <tr>
       <td height="78" colspan="2" bgcolor="#999999"><p aligns="center">
             <input type="submit" value="Login" name="B1" />
             <input type="reset" value="Reset" name="B2" />
           </td>
          </tr>
         </table>
       </form>
           </div>
          </div>
          <div class="sidebar">
         <p>&nbsp;</p>
           <div class="gadget">
            <h2 class="star"><span>Sidebar</span> Menu</h2>
            <div class="clr"></div>
            <ul class="sb_menu">
             <li><a href="index.html">Home Page</a></li>
```

```
<li><a href="cs_login.jsp">Cloud</a></li>
                         <li><a href="au_login.jsp">TPM</a></li>
                         <li><a href="do_login.jsp">Data Owner</a></li>
                         <li><a href="dr_login.jsp">Group Member</a></li>
      <li><a href="attack.jsp">Attacker</a></li>
         </ul>
        </div>
      </div>
      <div class="clr"></div>
    </div>
  </div>
  <div class="fbg"></div>
  <div class="footer">    <div class="footer_resize">
      <div style="clear: both;"></div>
    </div>
  </div>
</div>
<div align=center></div>
</body>
</html>
```

Au login.jsp

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head><title>Attribute TPM Login</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="css/style.css" rel="stylesheet" type="text/css" />
<link rel="stylesheet" type="text/css" href="css/coin-slider.css" />
<script type="text/javascript" src="js/cufon-yui.js"></script>
<script type="text/javascript" src="js/cufon-times.js"></script>
<script type="text/javascript" src="js/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="js/script.js"></script>
<script type="text/javascript" src="js/coin-slider.min.js"></script>
<script language="javascript" type="text/javascript">
function valid ()
{
var na3=document.s. userid. Value;
if(na3=="")
{
Alert ("Please Enter Name");
document.s. userid.focus ();
return false;
}
Else
{
}
var na4=document.s. pass. Value;
if(na4=="")
{
Alert ("Please Enter Password");
document.s. pass. focus ();
return false;
}
}
</script>
<style type="text/css">
<!—
. style1 {font-family: "Times New Roman", Times, serif}
. style2 {font-size: 15px}
. style3 {color: #1e5381}
. style4 {font-size: 20px}
. style5 {font-weight: bold}
. style7 {
  font-weight: bold;
  color: #ffae00;
}
. style9 {color: #ffae00}
. style10 {font-size: 24px}
-->
</style>
</head>
<body>
<div class="main">
  <div class="header">
    <div class="header resize">
      <div class="logo">        <h1><a href="index.html" class="style10">A Lightweight Secure Auditing Scheme
for Shared Data in Cloud Storage</a></h1>
      </div>
      <div class="menu_nav">
        <ul>
          <li><a href="index.html"><span>Home Page</span></a></li>
          <li><a href="cs_login.jsp"><span>Cloud</span></a></li>
          <li class="active"><a href="au_login.jsp"><span>TPM</span></a></li>
          <li><a href="do_login.jsp"><span>Data Owner</span></a></li>
          <li><a href="dr_login.jsp"><span>Group Member</span></a></li>
        </ul>
      </div>
      <div class="clr"></div>
      <div class="slider">
        <div id="coin-slider"> <a href="#"><img src="images/slide1.jpg" width="960" height="360" alt="" /></a>
<a href="#"><img src="images/slide2.jpg" width="960" height="360" alt="" /></a> <a href="#"><img
src="images/slide3.jpg" width="960" height="360" alt="" /></a> </div>
        <div class="clr"></div>
      </div>
      <div class="clr"></div>
    </div>
  </div>
```

```
 <div class="content">
    <div class="content_resize">
      <div class="mainbar">
        <div class="article">
          <h2 align="center"> TPM Login </h2>
<p>&nbsp;</p>
<form name="s" action="au_authentication.jsp" method="post" onSubmit="return valid ()" ons target="_top">
    <table align="center" border="1" width="57%" height="179">
     <tr>
        <td width="48%" height="46" bgcolor="#333333" class="style4 style2"><span class="style4 style3 style1
style7 style9"><strong> Name </strong></span></td>
        <td width="55%" height="46" bgcolor="#333333"><input type="text" name="userid" size="18" /></td>
      </tr>
      <tr>
           <td width="48%" height="40" bgcolor="#333333" class="style5 style2"> <span class="style4 style1
style9"><strong>Password</strong></span></td>
           <td width="55%" height="40" bgcolor="#333333"><input type="password" name="pass" size="18"
/></td>
      </t>
      <tr>
        <td height="78" colspan="2" bgcolor="#999999"><p aligns="center">
            <input type="submit” value="Login" name="B1" />
            <input type="reset" value="Reset" name="B2" />
        </td>
      </tr>
    </table>
</form>
       </div>
      </div>
      <div class="sidebar">
    <p>&nbsp;</p>
        <div class="gadget">
          <h2 class="star"><span>Sidebar</span> Menu</h2>
          <div class="clr"></div>
          <ul class="sb_menu">
            <li><a href="index.html">Home Page</a></li>
            <li><a href="cs_login.jsp">Cloud</a></li>
            <li><a href="au_login.jsp">TPM</a></li>
            <li><a href="do_login.jsp">Data Owner</a></li>
            <li><a href="dr_login.jsp">Group Member</a></li>
```

```
   <li><a href="attack.jsp">Attacker</a></li>
     </ul>
    </div>
   </div>
   <div class="clr"></div>
  </div>
 </div>
 <div class="fbg"></div>
 <div class="footer">
  <div class="footer_resize">
   <div style="clear:both;"></div>
  </div>
 </div>
</div>
<div align=center></div>
</body>
</html>
```

Data Owner login.jsp

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Data Owner Login</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="css/style.css" rel="stylesheet" type="text/css" />
<link rel="stylesheet" type="text/css" href="css/coin-slider.css" />
<script type="text/javascript" src="js/cufon-yui.js"></script>
<script type="text/javascript" src="js/cufon-times.js"></script>
<script type="text/javascript" src="js/jquery-1.4.2.min.js"></script>
<script type="text/javascript" src="js/script.js"></script>
<script type="text/javascript" src="js/coin-slider.min.js"></script>
<script language="javascript" type="text/javascript">
function valid ()
{
var na3=document.s. userid. Value;
if(na3=="")
{
Alert ("Please Enter Name");
document.s. userid. focus ();
return false;
}
Else
{
}
var na4=document.s. pass. Value;
if(na4=="")
{
Alert ("Please Enter Password");
document.s. pass. focus ();
return false;
}
}
</script>
<style type="text/css">
```

```
<!—
.style1 {font-family: "Times New Roman", Times, serif}
.style2 {font-size: 15px}
.style3 {color: #1e5381}
.style4 {font-size: 20px}
.style5 {font-weight: bold}
.style7 {
  font-weight: bold;
  color: #ffae00;
}
.style9 {color: #ffae00}
.style10 {font-size: 24px}
-->
</style>
</head>
<body>
<div class="main">
  <div class="header">
    <div class="header resize">
      <div class="logo">
<h1><a href="index.html" class="style10">A Lightweight Secure Auditin
g Scheme for Shared Data in Cloud Storage</a></h1>
      </div>
      <div class="menu_nav">
        <ul>
          <li><a href="index.html"><span>Home Page</span></a></li>
          <li><a href="cs_login.jsp"><span>Cloud</span></a></li>
          <li><a href="au_login.jsp"><span>TPM</span></a></li>
          <li class="active"><a href="do_login.jsp"><span>Data Owner</span></a></li>
          <li><a href="dr_login.jsp"><span>Group Member</span></a></li>
        </ul>
      </div>
      <div class="clr"></div>
      <div class="slider">
        <div id="coin-slider"> <a href="#"><img src="images/slide1.jpg" width="960" height="360" alt="" /></a>
<a href="#"><img src="images/slide2.jpg" width="960" height="360" alt="" /></a> <a href="#"><img
src="images/slide3.jpg" width="960" height="360" alt="" /></a> </div>
        <div class="clr"></div>
      </div>
      <div class="clr"></div>
    </div>
  </div>
  <div class="content">
    <div class="content_resize">
      <div class="mainbar">
        <div class="article">
          <h2 align="center"> Data Owner Login </h2>
          <p>&nbsp;</p>
<form name="s" action="
do_authentication.jsp" method="post" onSubmit="return valid ()" ons
target="_top">

    <table align="center" border="1" width="57%" height="179">
        <tr>
        <td width="48%" height="46" bgcolor="#333333" class="style4 style2"><span class="style4 style3 style1
style7 style9"><strong> Name </strong></span></td>
        <td width="55%" height="46" bgcolor="#333333"><input type="text" name="userid" size="18" /></td>
      </tr>
      <tr>
          <td width="48%" height="40" bgcolor="#333333" class="style5 style2"> <span class="style4 style1
style9"><strong>Password</strong></span></td>
            <td width="55%" height="40" bgcolor="#333333"><input type="password" name="pass" size="18"
/></td>
      </tr>
      <tr>
        <td height="78" colspan="2" bgcolor="#999999"><p align="center">
            <input type="submit" value="Login" name="B1" />
            <input type="reset" value="Reset" name="B2" />
        </td>
      </tr>
    </table>
  <p align="center" class="style2">New User? <a href="do_register.jsp">Register Here</a></p>
</form>
        </div>
      </div>
      <div class="sidebar">
    <p>&nbsp;</p>
        <div class="gadget">
          <h2 class="star"><span>Sidebar</span> Menu</h2>
          <div class="clr"></div>
          <ul class="sb_menu">  <li><a href="index.html">Home Page</a></li>
            <li><a href="cs_login.jsp">Cloud</a></li>
            <li><a href="au_login.jsp">TPM</a></li>
            <li><a href="do_login.jsp">Data Owner</a></li>
            <li><a href="dr_login.jsp">Group Member</a></li>
      <li><a href="attack.jsp">Attacker</a></li>
          </ul>
        </div>
      </div>
      <div class="clr"></div>
    </div>
  </div>
  <div class="fbg"></div>
  <div class="footer">
    <div class="footer_resize">
      <div style="clear:both;"></div>
    </div>
  </div>
</div>
<div align=center></div>
</body>
</html>
```

```
}
```

Group member login.jsp

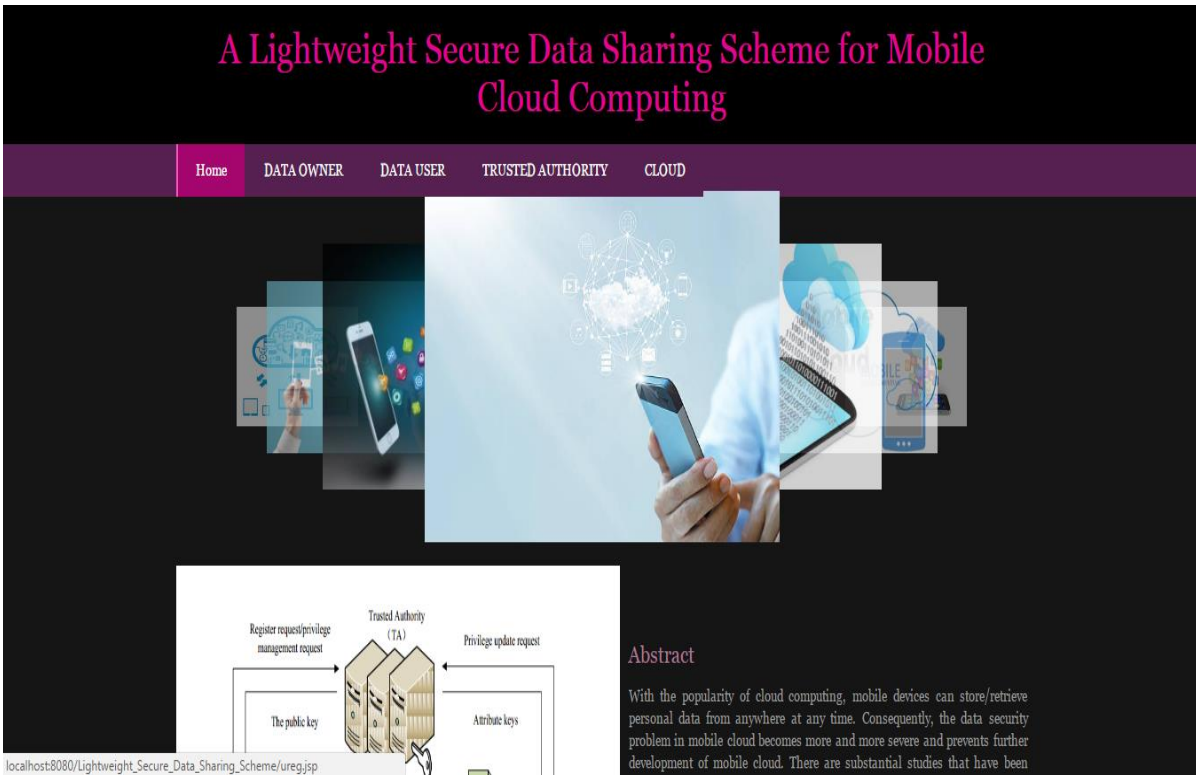
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Group Member Login</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="css/style.css" rel="stylesheet" type="text/css" />
<link rel="stylesheet" type="text/css" href="css/coin-slider.css" />
<script type="text/javascript" src="js/cufon-yui.js"></script>
<scripttype="text/javascript"src="js/cufon-times.js"></script><script type="text/javascript" src="js/jquery-
1.4.2.min.js"></script>
<script type="text/javascript" src="js/script.js"></script>
<script type="text/javascript" src="js/coin-slider.min.js"></script>
<script language="javascript" type="text/javascript">
function valid()
{
var na3=document.s. userid.value;
if(na3=="")
{
Alert ("Please Enter Name");
document.s.userid.focus ();
return false;
}
else
{
}
var na4=document.s.pass.value;
if(na4=="")
{
Alert ("Please Enter Password");
document.s.pass.focus ();
return false;
}
}
</script>
```

```
<style type="text/css">

<!—
.style1 {font-family: "Times New Roman", Times, serif}
.style2 {font-size: 15px}
.style3 {color: #1e5381}
.style4 {font-size: 20px}
.style5 {font-weight: bold}
.style7 {
  font-weight: bold;
  color: #ffae00;
}
.style9 {color: #ffae00}
.style10 {font-size: 24px}
-->
</style>
</head>
<body>
<div class="main">
  <div class="header">
    <div class="header_resize">
      <div class="logo">
         <h1><a href="index.html" class="style10">A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage</a></h1>
      </div>
      <div class="menu_nav">
        <ul>
          <li><a href="index.html"><span>Home Page</span></a></li>
          <li><a href="cs_login.jsp"><span>Cloud</span></a></li>
          <li><a href="au_login.jsp"><span>TPM</span></a></li>
          <li><a href="do_login.jsp"><span>Data Owner</span></a></li>
          <li class="active"><a href="dr_login.jsp"><span>Group Member</span></a></li>
        </ul>
      </div>
      <div class="clr"></div>
      <div class="slider">
       <div id="coin-slider"> <a href="#"><img src="images/slide1.jpg" width="960" height="360" alt="" /></a> <a href="#"><img src="images/slide2.jpg" width="960" height="360" alt="" /></a> <a href="#"><img src="images/slide3.jpg" width="960" height="360" alt="" /></a> </div>
        <div class="clr"></div>
      </div>
      <div class="clr"></div>
    </div></div>

  <div class="content">
    <div class="content_resize">
      <div class="mainbar">
        <div class="article">
          <h2 align="center"> Group Member Login </h2>
          <p>&nbsp;</p>
<form name="s" action="dr_authentication.jsp" method="post" onSubmit="return valid ()" ons target="_top">
    <table align="center" border="1" width="57%" height="179">
        <tr>
        <td width="48%" height="46" bgcolor="#333333" class="style4 style2"><span class="style4 style3 style1 style7 style9"><strong> Name </strong></span></td>
        <td width="55%" height="46" bgcolor="#333333"><input type="text" name="userid" size="18" /></td>
      </tr>
      <tr>
           <td width="48%" height="40" bgcolor="#333333" class="style5 style2"> <span class="style4 style1 style9"><strong>Password</strong></span></td>
            <td width="55%" height="40" bgcolor="#333333"><input type="password" name="pass" size="18" /></td>
      </tr>
      <tr>
        <td height="78" colspan="2" bgcolor="#999999"><p align="center">
            <input type="submit" value="Login" name="B1" />
            <input type="reset" value="Reset" name="B2" />
        </td></tr>
    </table>
  <p align="center" class="style2">New User? <a href="dr_register.jsp">Register Here</a></p>
</form>
        </div>
      </div>
      <div class="sidebar">
    <p>&nbsp;</p>
        <div class="gadget">
          <h2 class="star"><span>Sidebar</span> Menu</h2>
          <div class="clr"></div>
          <ul class="sb_menu">
            <li><a href="index.html">Home Page</a></li>
            <li><a href="cs_login.jsp">Cloud</a></li>
            <li><a href="au_login.jsp">TPM</a></li>
            <li><a href="do_login.jsp">Data Owner</a></li>
            <li><a href="dr_login.jsp">Group Member</a></li>



      <li><a href="attack.jsp">Attacker</a></li>
          </ul>
        </div>
      </div>
      <div class="clr"></div>
    </div>
  </div>
  <div class="fbg"></div>
  <div class="footer">
    <div class="footer_resize">
      <div style="clear: both;"></div>
    </div>
  </div>
</div>
<div align=center></div>
</body>
</html>
```

CHAPTER – 10

RESULT

RESULT



A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

Abstract

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

Fig: 1

The above picture contains of some pages they are

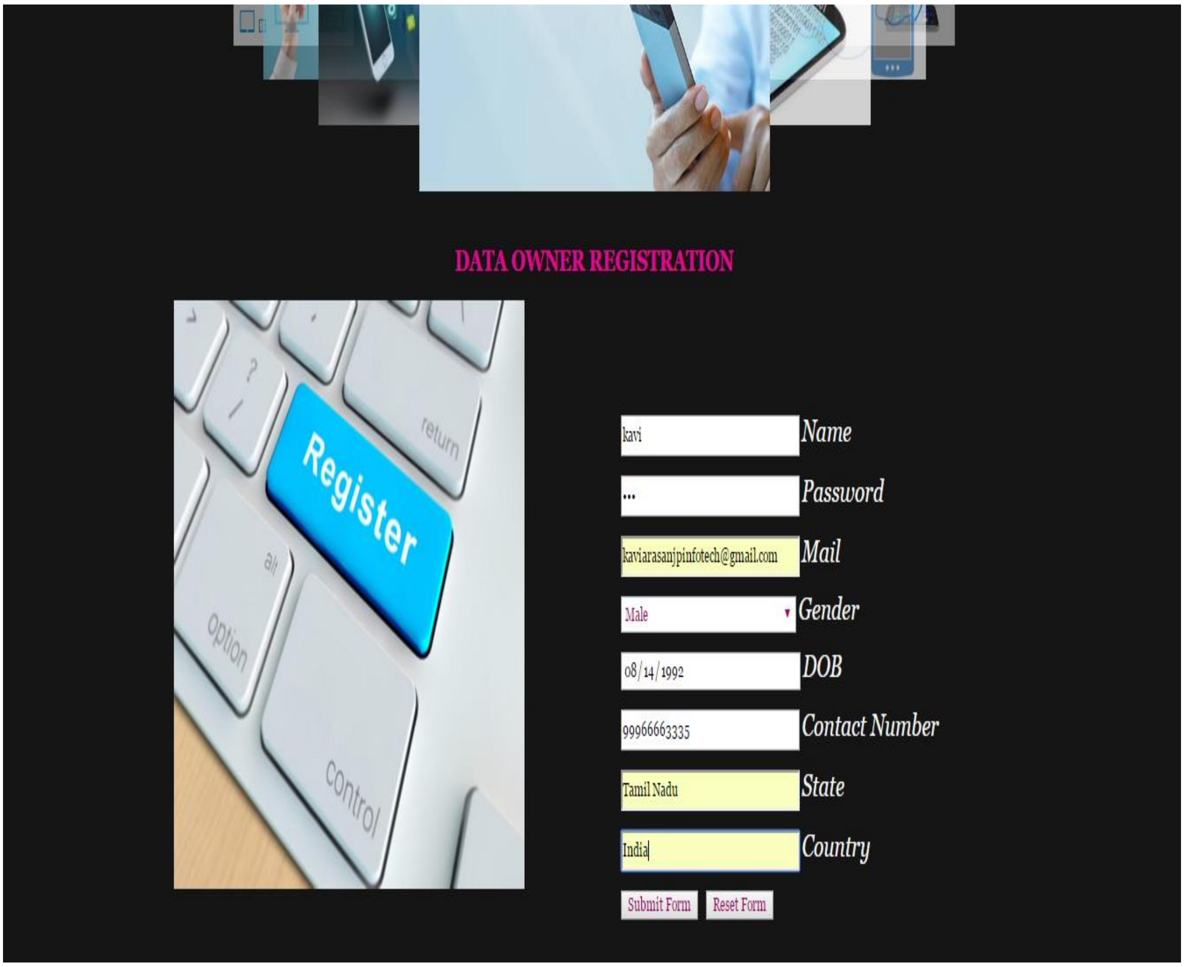
1)home page

2)Data owner

3)Data user

4)Trusted Authority

5)cloud



DATA OWNER REGISTRATION

kavi	Name
•••	Password
kaviarasanjpinfotech@gmail.com	Mail
Male ▾	Gender
08/14/1992	DOB
99966663335	Contact Number
Tamil Nadu	State
India	Country

Fig: 2

The above picture shows the process of Data owner Registration. This registration includes some components they are

1)Name

2)password

3)Mail

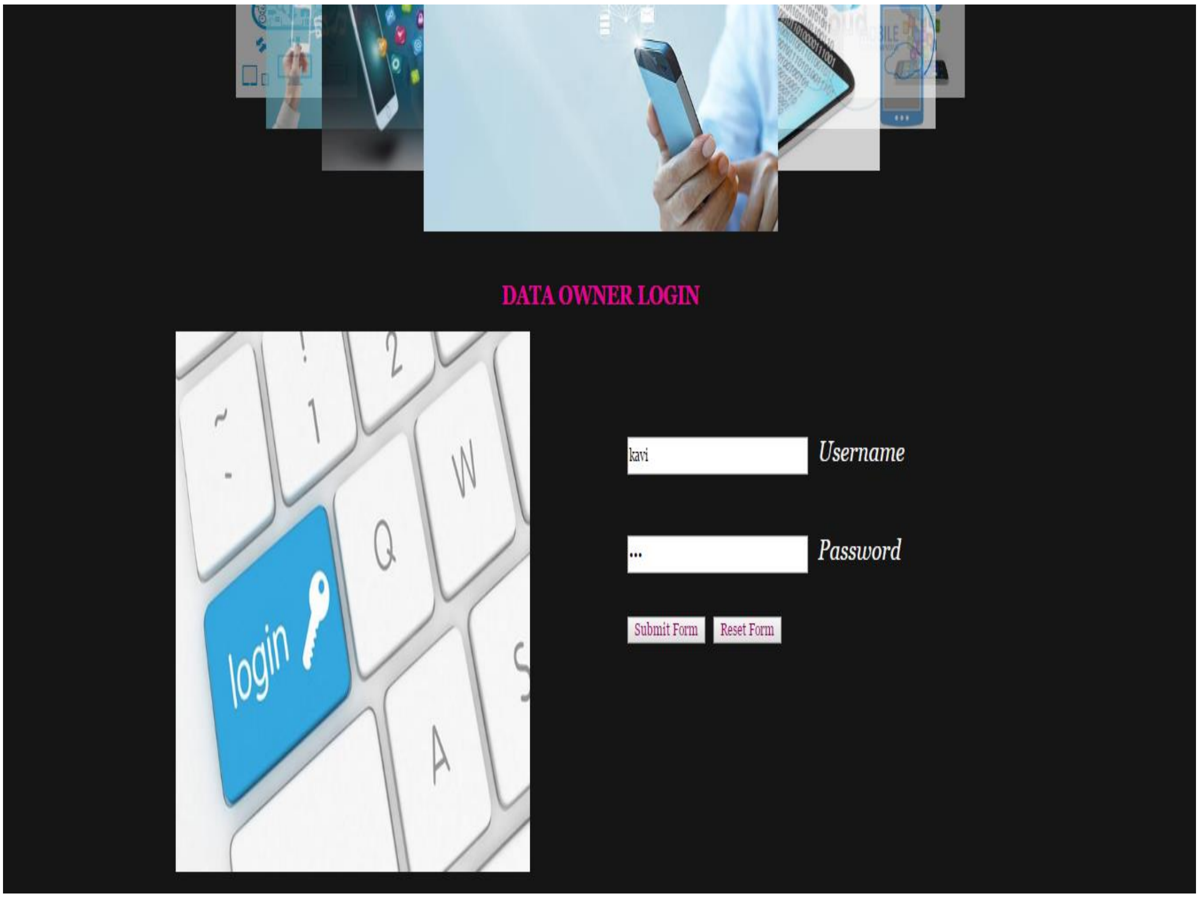
4)Gender

5)DOB

6)Contact Number

7)State

8)Country



DATA OWNER LOGIN

kavi Username

••• Password

Fig: 3

The above picture explains about the process of Data owner login. This contains of mostly two components

1)Username

2)password

After completion of giving required information, we need to click on the submit form. Then it will get submitted. The Another option included in this login process is the reset option.

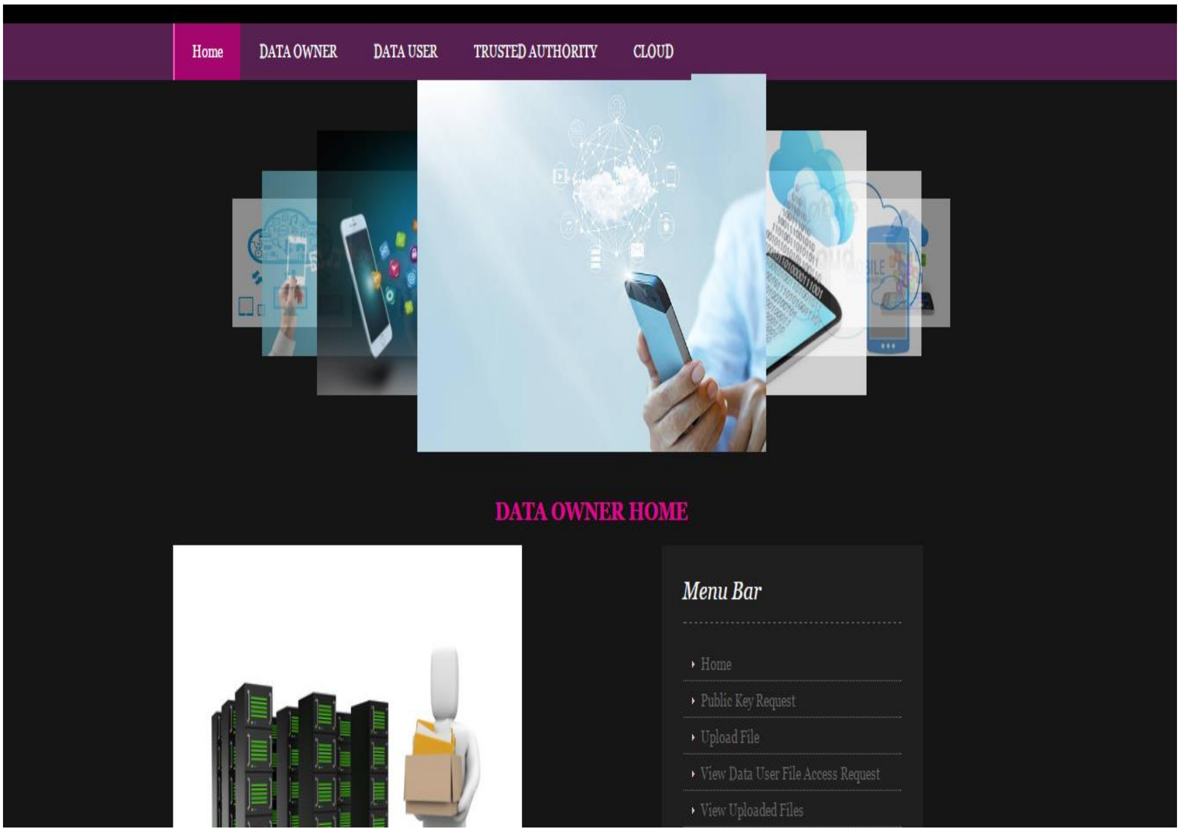


Fig: 4

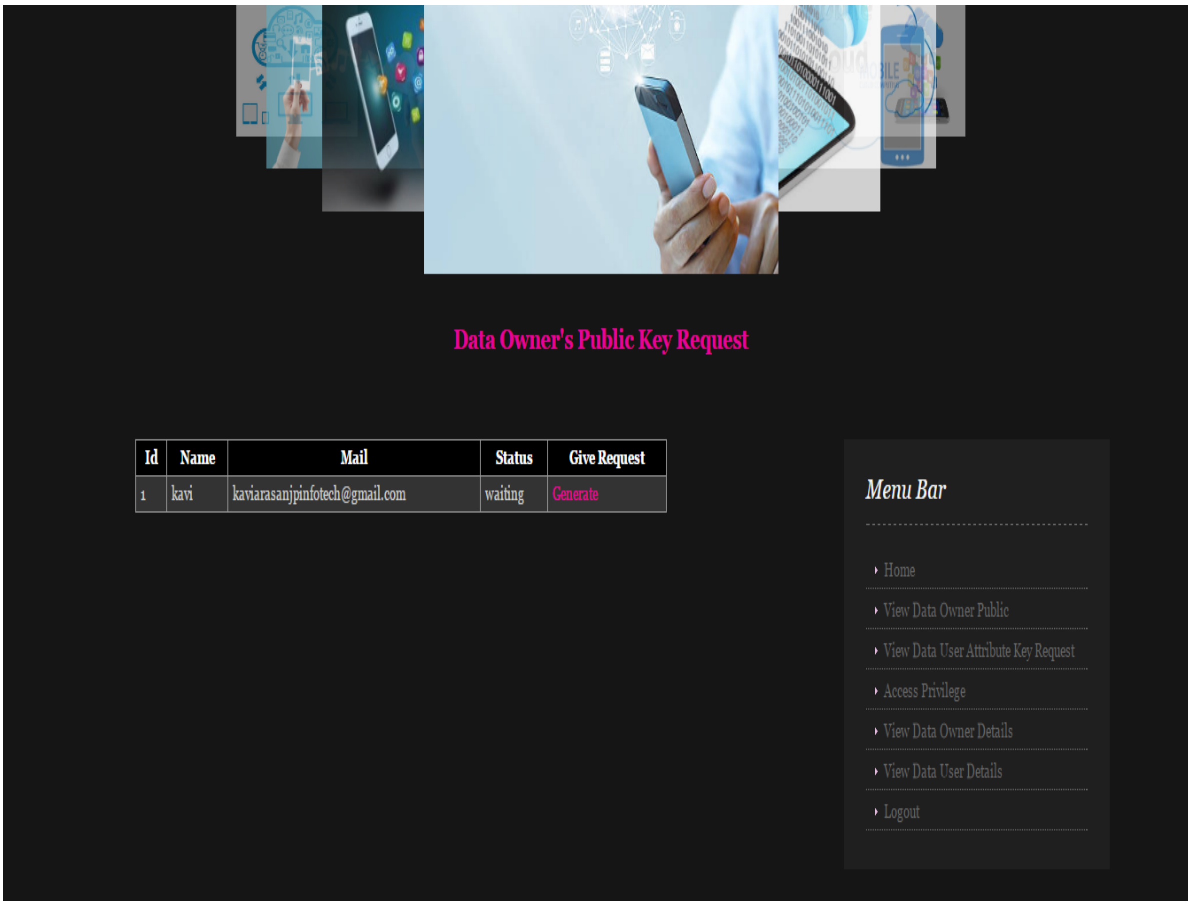
The above picture explains the data owner home. In this menu bar we can see some components such as

1)Home

2)public key request

3)Upload file

4)view data user file Access request



Data Owner's Public Key Request

Id	Name	Mail	Status	Give Request
1	kavi	kaviarasanjpinfotech@gmail.com	waiting	Generate

Fig: 5

The above picture shows the trusted authority login. This trusted authority login contains of mainly two components

1)Username

2)Password

After giving the username and password we must click on the submit form. The reset form is used to reset the whole data

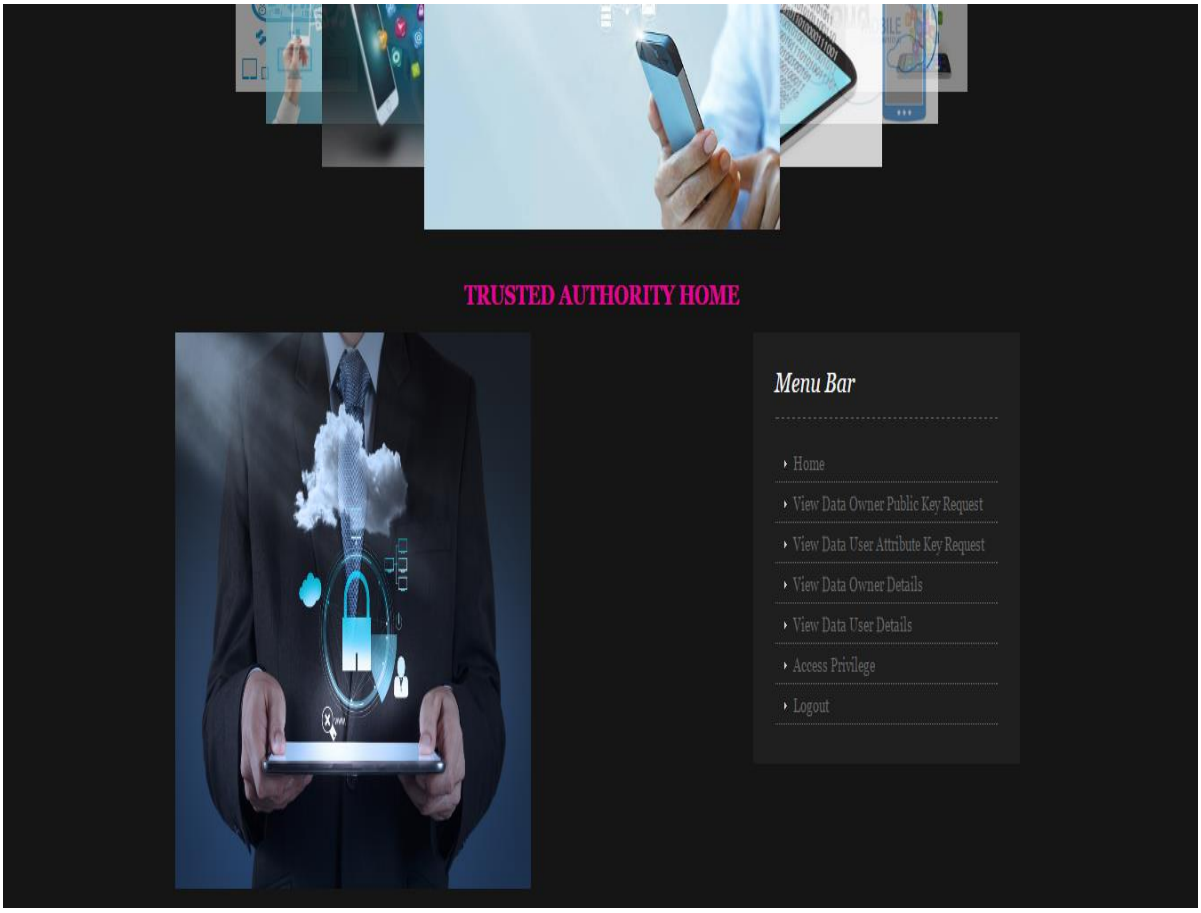


Fig: 6

This trusted authority home page contains of some fields they are as follows:

1)Home

2)view data owner public key request

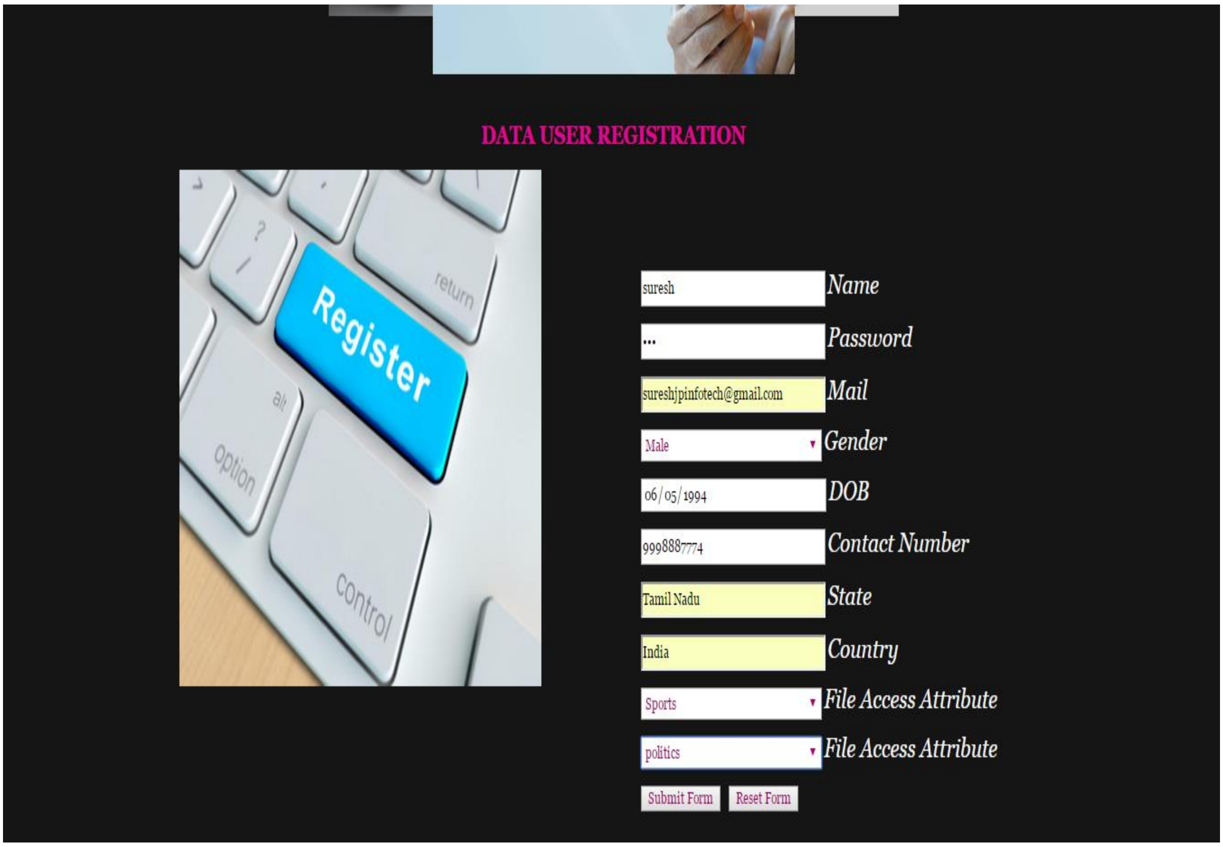
3)view data use attribute key request

4)view data owner details

5)view data user details

6)access privilege

7)logout



DATA USER REGISTRATION

suresh	Name
•••	Password
sureshjpinfotech@gmail.com	Mail
Male	Gender
06/05/1994	DOB
9998887774	Contact Number
Tamil Nadu	State
India	Country
Sports	File Access Attribute
politics	File Access Attribute

Fig: 7

This above picture shows the data user registration. This data user registration process contains of some fields they are:

1)Name

2)Password

3)Mail

4)Gender

5)DOB

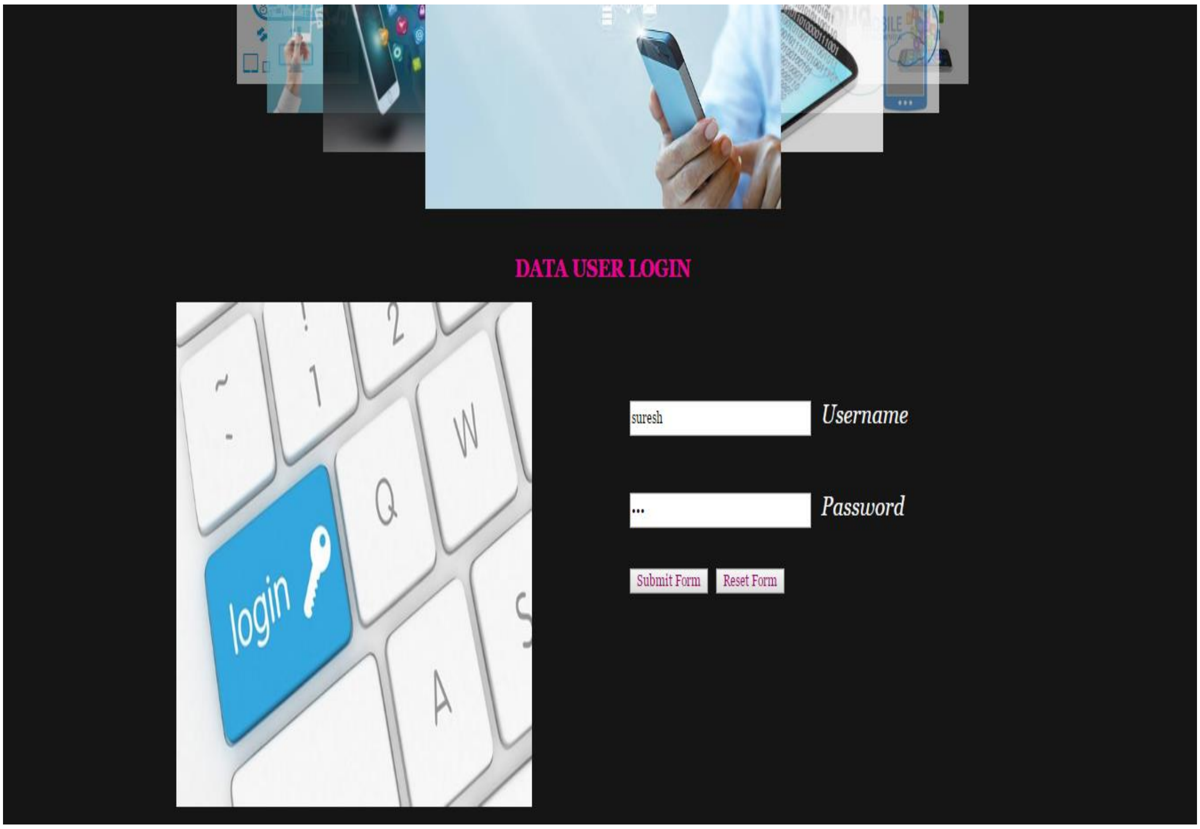
6)Contact number

7)State

8)Country

9) File access attribute

10)File access attribute



DATA USER LOGIN

Username: suresh

Password: ...

Fig: 8

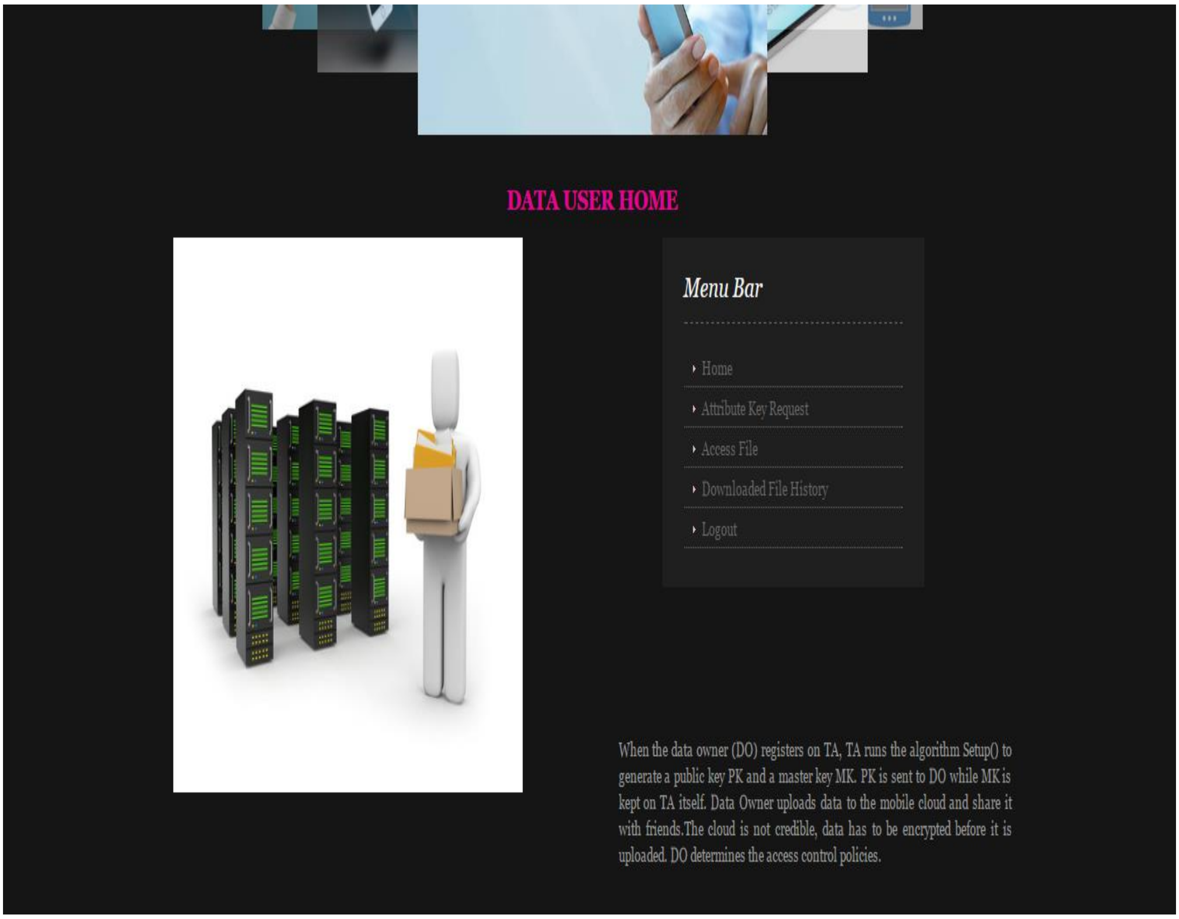
The above picture shows the login of data user. This data user login

Contains of mostly two components. They are:

1)Username

2)Password

After giving the giving name and password we must click on the submit form.



When the data owner (DO) registers on TA, TA runs the algorithm Setup() to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TA itself. Data Owner uploads data to the mobile cloud and share it with friends.The cloud is not credible, data has to be encrypted before it is uploaded. DO determines the access control policies.

Fig: 9

The above picture shows the components that are included in the data user home. They are:

1)Home

2)Attribute key request

3)Access file

4)Downloaded file history

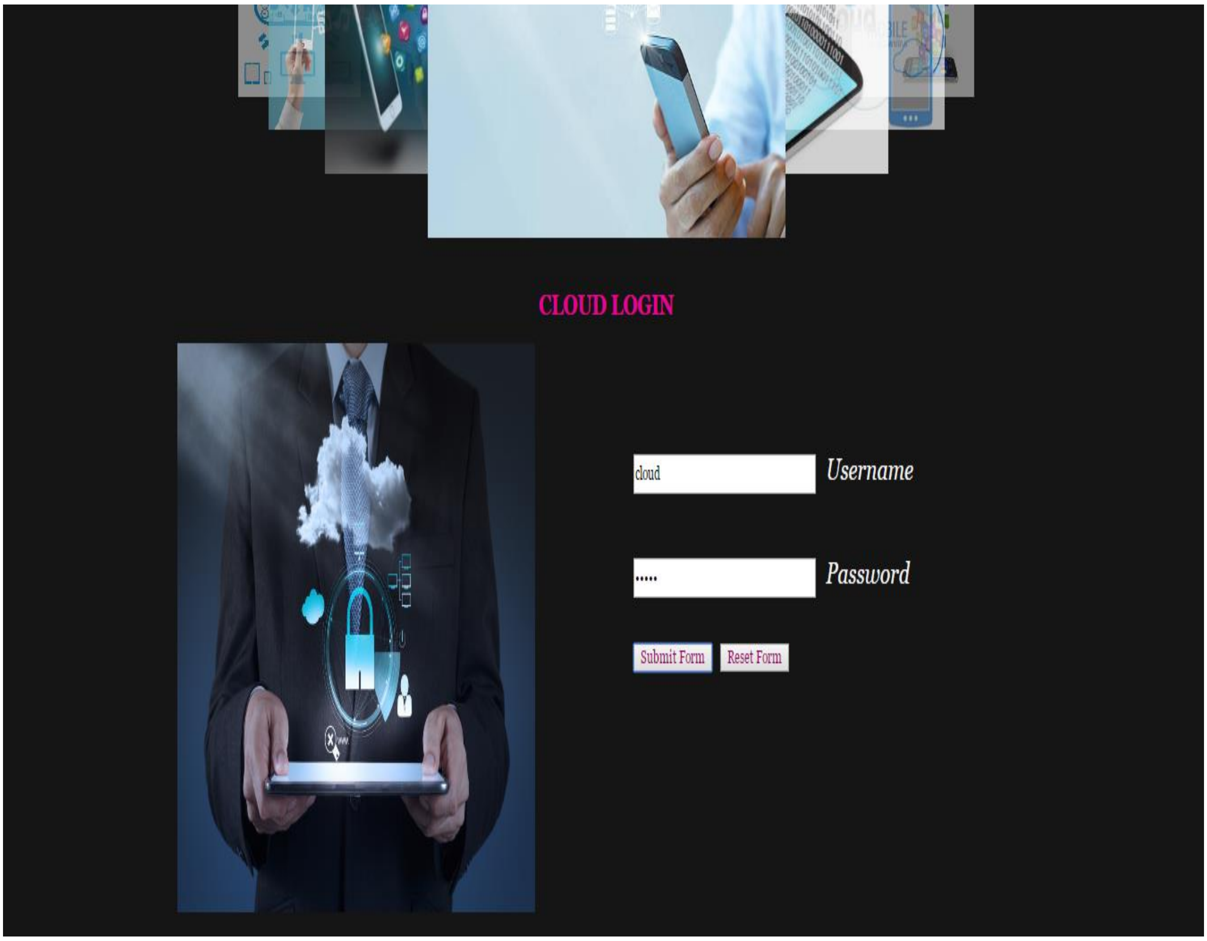


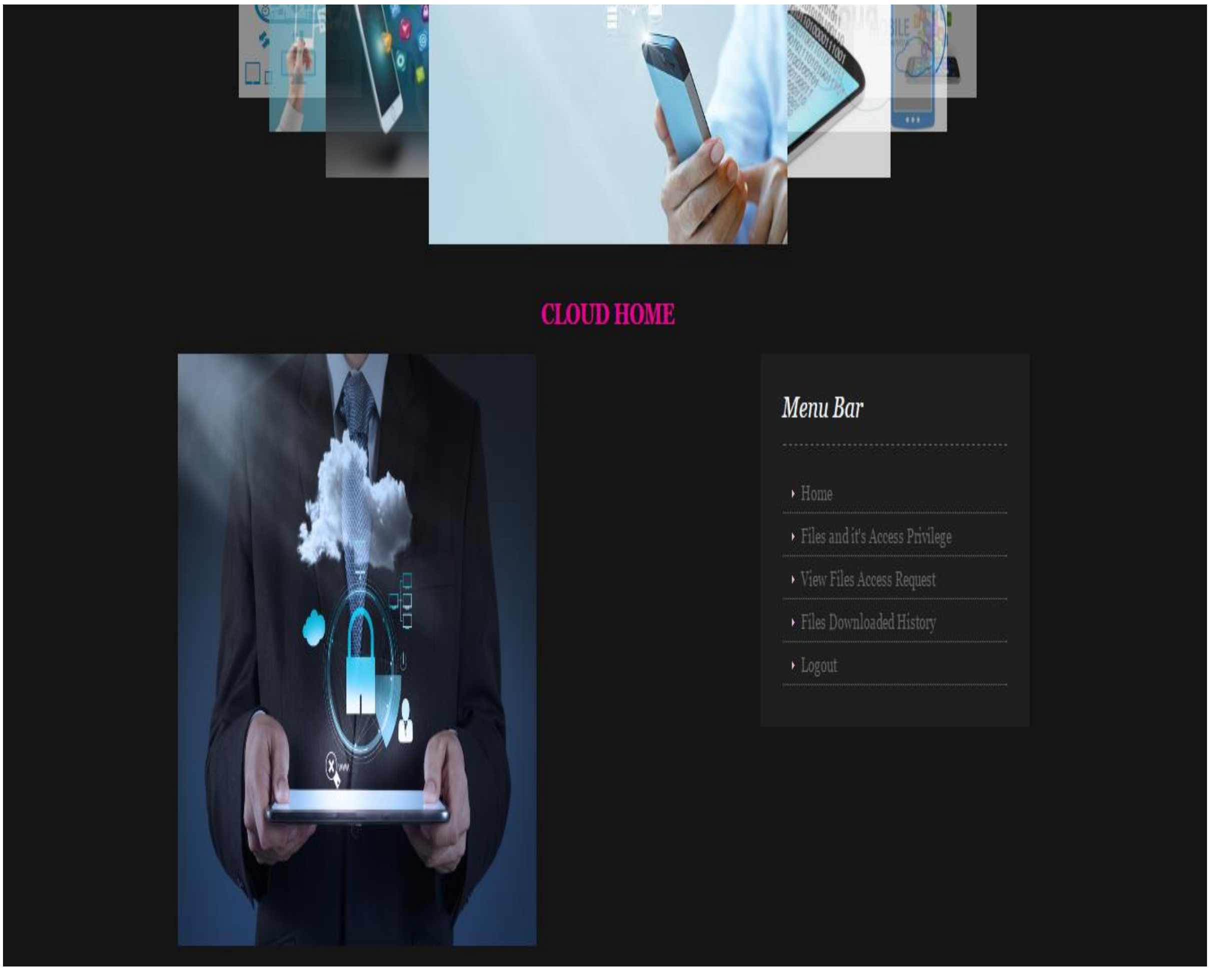
Fig: 10

The above picture shows the cloud login process. This contains of mainly two components they are:

1)Username

2)Password

After giving the username and password we need to click on the submit form.



CLOUD HOME

Menu Bar

Fig: 11

The above picture shows the cloud home. That component that are included in cloud home menu bar are:

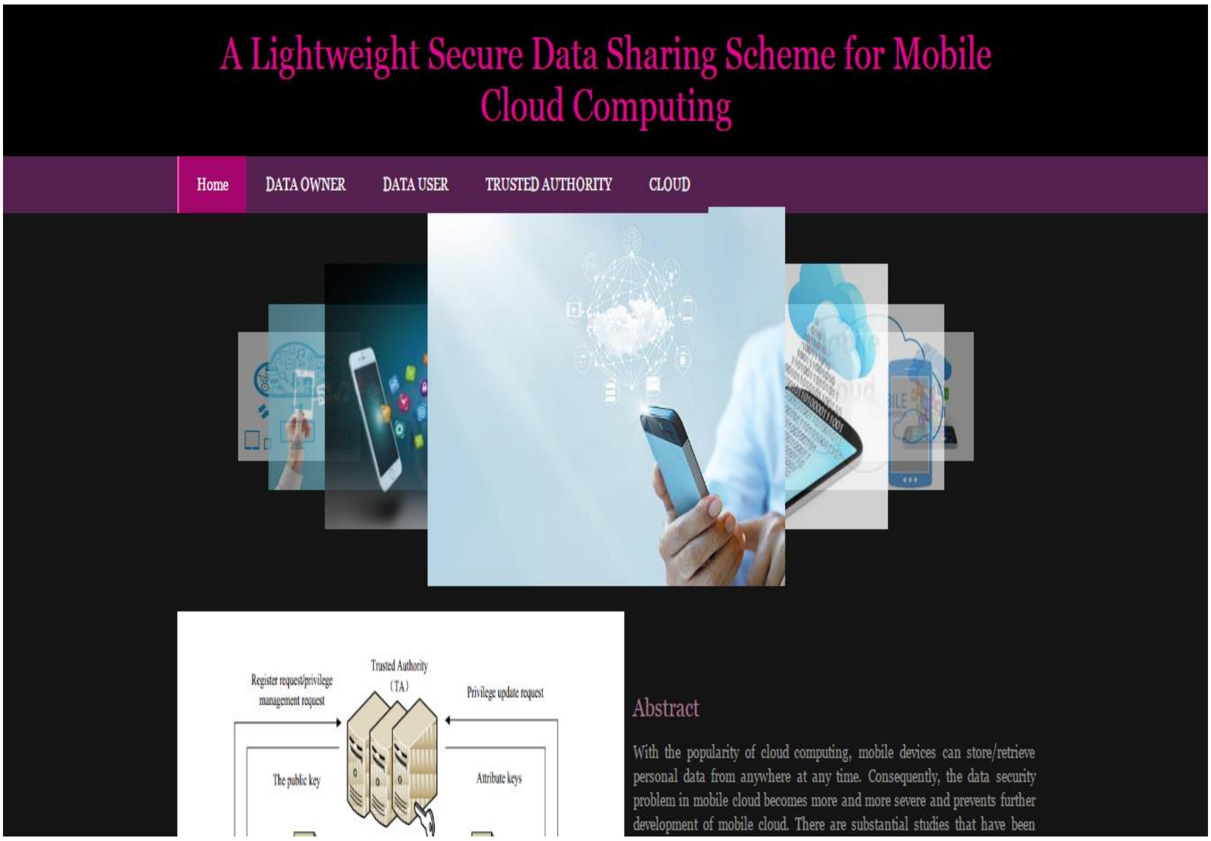
1)Home

2)Files and its access privilege

3)View files access request

4)Files download history

5)logout



A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

Abstract

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

Fig: 12

CHAPTER-11

CONCLUSION

CONCLUSION

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud.

The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do ciphertext retrieval over existing data sharing schemes.

CHAPTER-12

REFERENCES

REEFERENCES

[1] Gentry C, Halevi S. Implementing gentry’s fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[2] Brake ski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.

[3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.

[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.

[5] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.

[6] Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage. in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation-Volume 4. USENIX Association, pp. 10-12, 2000.

[7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.

[9] Shi E, Bethencourt J, Chan T H H, et al. multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350- 364

[10] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and

Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[11] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

[12] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

[14] Junzuo Lai, Robert H. Deng, Yingjiu Li, et al. Fully secure key policy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

[16] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities. in: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. New
York, NY, USA: ACM press, pp. 276-286, 2009.

[17] Pirretti M, Traynor P, McDaniel P, et al. Secure attribute-based systems. in: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM press, pp. 99-112, 2006.

[18] Yu S., Wang C., Ren K., et al. Attribute based data sharing with attribute revocation. in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security (ASIACCS), New York, USA: ACM press pp. 261-270, 2010.

[19] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models. Computer, 29(2): 38-47, 1996.

[20] Tian X X, Wang X L, Zhou A Y. DSP RE-Encryption: A flexible mechanism for access control enforcement management in DaaS. in: Proceedings of IEEE International Conference on Cloud Computing. IEEE press, pp.25-32, 2009

[21] Di Vimercati S D C, Foresti S, Jajodia S, et al. Over-encryption: management of access control evolution on outsourced data. in: Proceedings of the 33rd international conference on Very large data bases. Vienna, Austria: ACM, pp. 123-134, 2007.

[22] Kan Yang, Xiaohua Jia, Kui Ren, Ruitao Xie, Liusheng Huang: Enabling efficient access control with dynamic policy updating for big data in the cloud. INFOCOM 2014, pp.2013-2021, 2014.

[23] Jia W, Zhu H, Cao Z, et al. SDSM: a secure data service mechanism in mobile cloud computing. in: Proceedings of 30th IEEE International Conference on Computer Communications. Shanghai, China: IEEE, pp. 1060-1065, 2011.

[24] D. Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication. in: Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering. Nanjing, China: IEEE, pp. 90-98, 2010.

[25] Benjamin Livshits, Jaeyeon Jung. Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications. USENIX Security, pp.113-130, Aug. 2013.

[26] Zhou Z, Huang D. Efficient and secure data storage operations for mobile cloud computing. in: Proceedings of 8th International Conference on Network and Service Management (CNSM 2012), Las Vegas, USA: IEEE, pp. 37-45, 2012.

[27] P. K. Tysowski and M. A. Hasan. Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds. IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172-186, Nov. 2013.

[28] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. in: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, pp. 213−229, 2001.