

CLOUD SUPPORTED SECURED DATA AQUISITION

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree
in
Computer Science and Engineering

By

ERLA VENKATA SAI KEERTHANA
(Reg. No. 37110212)



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with Grade "A" by NAAC
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600 119

MARCH - 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work **ERLA VENKATA SAI KEERTHANA (Reg. No.37110212)** who carried out the project entitled "**CLOUD SUPPORTED SECURED DATA AQUISITION**" under our supervision from **August 2020 to March 2021**.

Internal Guide

Mrs. B. KEERTHI SAMHITHA M.Tech.,(Ph.D).,

Head of the Department

Dr. S.VIGNESHWARI M.E.,Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **ERLA VENKATA SAI KEERTHANA** hereby declare that the Project Report entitled “**CLOUD SUPPORTED SECURED DATA AQUISITION**” is done by me under the guidance of **Mrs. B. KEERTHI SAMHITHA M.Tech.,(Ph.D).**,Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean**, School of Computing, **Dr. S. Vigneswari, M.E., Ph.D.,** and **Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department** of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Mrs. B. KEERTHI SAMHITHA M.Tech.,(Ph.D), Assistant Professor**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

Cloud-supported Internet of Things (Cloud-IoT) has been broadly deployed in smart grid systems. The IoT front-ends are responsible for data acquisition and status supervision, while the substantial amount of data is stored and managed in the cloud server. Achieving data security and system efficiency in the data acquisition and transmission process are of great significance and challenging, because the power grid-related data is sensitive and in huge amount. In this paper, we present an efficient and secure data acquisition scheme based on CP-ABE (Cipher text Policy Attribute Based Encryption). Data acquired from the terminals will be partitioned into blocks and encrypted with its corresponding access sub-tree in sequence, thereby the data encryption and data transmission can be processed in parallel. Furthermore, we protect the information about the access tree with threshold secret sharing method, which can preserve the data privacy and integrity from users with the unauthorized sets of attributes. The formal analysis demonstrates that the proposed scheme can fulfill the security requirements of the Cloud-supported IoT in smart grid. The numerical analysis and experimental results indicate that our scheme can effectively reduce the time cost compared with other popular approaches.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	v
	LIST OF FIGURES	viii
	LIST OF ABBREVIATIONS	x
1.	INTRODUCTION	1
	1.1 INTRODUCTION	1
	1.2 CLOUD STORAGE SECURITY	2
	1.3 BENEFITS OF CLOUD STORAGE SECURITY	2
2.	LITERATURE SURVEY	5
3.	AIM AND SCOPE	9
	3.1 AIM OF THE PROJECT	9
	3.2 OBJECTIVES	9
	3.3 SCOPE	10
	3.4 ADVANTAGES	10
4.	SYSTEM DESIGN AND METHODOLOGY	11
	4.1 EXISTING SYSTEM	11
	4.1.1 DISADVANTAGES	11
	4.2 PROPOSED SYSTEM	11
	4.2.1 ADVANTAGES	12
	4.3 SYSTEM FUNCTIONALITIES	12
	4.3.1 OUTPUT DESIGN	13
	4.4 REQUIREMENT SPECIFICATION	13
	4.4.1 SOFTWARE REQUIREMENTS	14
	4.4.2 HARDWARE REQUIREMENTS	14
	4.5 MODULES	14
	4.6 SYSTEM STUDY	15

5.	SOFTWARE DEVELOPMENT	17
	METHODOLOGY	
	5.1 ARCHITECTURAL DESIGN	17
	5.2 USE CASE DIAGRAM	18
	5.3 CLASS DIAGRAM	20
	5.4 SEQUENCE DIAGRAM	20
	5.5 COLLEBORATION DIAGRAM	22
	5.6 ACTIVITY DIAGRAM	22
	5.7 COMPONENT DIAGRAM	23
	5.8 DEPLOYMENT DIAGRAM	24
	5.9 SYSTEM TESTING	24
	5.9.1 UNIT TESTING	25
	5.9.2 INTEGRATION TESTING	25
	5.9.3 ACCEPTANCE TESTING	25
6.	RESULTS AND DISCUSSION	26
	6.1 SCREENSHOTS	26
7.	CONCLUSION AND FUTURE WORK	38
	7.1 CONCLUSION	38
	7.2 FUTURE WORK	38
	REFERENCES	39

LIST OF FIGURES

FIGURE NO	FIGURE NAME	PAGE NO
5.1	Work Flow Implementation	17
5.2	Use case diagram for cloud consumer	18
5.2.1	Use case diagram for data owner	19
5.2.2	Use case diagram for cloud server	19
5.3	Class diagram	20
5.4	Sequence diagram	21
5.5	Collaboration diagram	22
5.6	Activity diagram	23
5.7	Component diagram	24
5.8	Deployment diagram	24
6.1	Home page	26
6.2	Data owner registration page	26
6.3	File Uploading in data owner page	27
6.4	File uploaded successfully in data owner login page	27
6.5	Same file is uploading again by owner	28
6.6	It displays same file is already exists	28
6.7	Consumer login page	29
6.8	Keywords	29
6.9	Keyword entered for generating unique key	30
6.10	Generating key for keyword	30
6.11	Request accepted by data owner for generating key for keyword	31
6.12	Key successfully generated for keyword testing	31
6.13	Encrypted keyword generating	32

6.14	Successfully created encrypted keyword	32
6.15	Sending request to cloud	33
6.16	Cloud server login page	33
6.17	Cloud server accept the customer request and send files to customer	34
6.18	Data owner got file request	34
6.19	Data owner generating key for file Project	35
6.20	Key generated successfully for file	35
6.21	Consumer want to download file	36
6.22	Key entered for downloading file	36
6.23	Secured File is downloaded successfully	37
6.24	User is viewing downloaded data file	37

LIST OF ABBREVIATIONS

ACRONYM	EXPANSION
IoT	Internet Of Things
CP-ABE	Ciphertext Policy Attribute Based Encryption
SSO	Single Sign-On
MFA	Multi-Factor Authentication
UML	Unified Modeling Language

CHAPTER1

INTRODUCTION

1.1 INTRODUCTION

With the support of modern information technologies like the Internet of Things (IoT) and cloud computing, smart grid has emerged as the next-generation power supply network, in which the electricity is generated according to the real-time demands of electric equipment or household appliances. To make the smart grid more intelligent, a great number of IoT terminals are deployed to gather the status of the power grid timely for the control center. Some sample applications are the power transmission line monitoring, power generation monitoring, substation state monitoring, smart metering, electric energy data acquisition, smart home. For instance, in power transmission line monitoring scenario, using preplaced sensors, the status parameters of the transmission line and power towers can be gathered in real time, so that any fault can be diagnosed and located in a timely manner.

In smart grid, the different kinds of applications mentioned above all generate an enormous amount of data, which needs to be stored and managed efficiently. Cloud-IoT is proposed to address this issue. With the support of cloud computing, mass data from different IoT terminals can be collected and processed by local front-end servers, then transferred and stored in the cloud servers. The data in cloud can be accessed by various types of data users. The power grid staff can continually monitor the status of power grid. Researchers and government agencies can analyze the data for research or policymaking.

As organizations and individuals adopt cloud technologies, many have become aware of the serious concerns regarding security and privacy of accessing personal and confidential information over the Internet. In particular, the recent and continuing data breaches highlight the need for more secure cloud storage systems. While it is generally agreed that encryption is necessary, cloud providers often perform the encryption and maintain the private keys instead of the data owners. That is, the cloud can read any data it desired, providing no privacy to its users. The storage of private keys and encrypted data by the cloud provider is also problematic in case of data breach. Hence, researchers have actively been exploring solutions for secure storage on private and public clouds where private keys remain in the hands of data

owners. In this, we present a phrase search scheme which achieves a much faster response time than existing solutions. The scheme is also scalable, where documents can easily be removed and added to the corpus. We also describe modifications to the scheme to lower storage cost at a small cost in response time and to defend against cloud providers with statistical knowledge on stored data.

1.2 CLOUD STORAGE SECURITY

Cloud-based internet security is an outsourced solution for storing data. Instead of saving data onto local hard drives, users store data on Internet-connected servers. Data Centers manage these servers to keep the data safe and secure to access. Enterprises turn to cloud storage solutions to solve a variety of problems. Small businesses use the cloud to cut costs. IT specialists turn to the cloud as the best way to store sensitive data. Any time you access files stored remotely, you are accessing a cloud. Email is a prime example. Most email users don't bother saving emails to their devices because those devices are connected to the Internet.

1.3 BENEFITS OF CLOUD STORAGE SECURITY

1. Data Encryption

Data you store on a cloud can be encrypted either before or after you send it, providing added protection. There is a range of cloud storage security options, including Single Sign-On (SSO), Multi-Factor Authentication (MFA) and more. This means that your data can only be accessed by the people you want it to, even if your device is stolen. Your privacy is completely protected and you don't need to worry about your data being stolen or sold off.

2. Back-Up Storage

Storing all your data on one server is very risky. If it fails for any reason, you could lose everything in an instant. Even if you don't use cloud storage as your primary storage system, it can function as a place to store second copies of files in case you ever need a back-up. If you're already using cloud storage, you don't have to worry about backing anything up yourself. The system takes the hassle out of that by doing it for you. Clouds are backed up to multiple servers, so you never need to

worry about losing the information you keep on them. If one server crashes, your data will still be safely stored in multiple other locations. This significantly reduces the risk of data loss. Hardware failure and technical glitches are completely unpredictable, and there's no reason to leave yourself vulnerable to them when there's cloud storage available.

3. Protect Against Hackers and Malware

Storing your data on a cloud system provides added protection from hackers and data loss. If you run a small business, this is particularly vital, as 43% of cyber attacks target small businesses. Of those businesses affected, 60% will be out of business after just 6 months. Hacking could be completely devastating to your business, so why would you take the risk? It's not just small businesses that are vulnerable to hackers. When larger businesses get hacked, it always causes a stir in the media. Well-known companies which have fallen victim to famous hacking scandals include Sony, LinkedIn, Target and Ashley Madison. Each of these companies' reputations took a hit as a result. Don't let your business suffer the same fate. According to Duke University, 80% of all US companies have suffered from some kind of hacking, so failing to protect yourself from the possibility is extremely dangerous. However, hacking isn't your only concern. Your company could also suffer data loss as a result of a server failure or human error. With cloud storage, you're protected from all of those things.

4. Save Money

Cloud storage is not only safe and secure, it's also cost-effective. Without cloud storage, you're constantly spending money on servers, whether it's through purchase or just maintenance. Not to mention the manpower that's required to run them. Switching to cloud storage could save you a considerable amount of money. Overheads reduce as it reduces the need for power and staff to support in-house servers. Overall, your storage costs could drop by up to 87%.

This will make your business more eco-friendly, too. The precise amount that cloud storage costs can vary, but you only pay for what you need. There are different payment plans for different storage sizes, and if you need more, you can always

upgrade. There's no need to spend money on an entire server that you won't be using to its full capacity.

5. Easier to Share and Access Files

Cloud storage allows you to work much more efficiently. Sending bulky email attachments is becoming a thing of the past. Uploading files is inconvenient and takes time and bandwidth. With cloud storage, you can avoid that and simply send a link. This also eliminates the need for syncing devices, as all of your data is centralized and accessible from anywhere. You don't need to be connected to a server and have the freedom to use any device you choose. This is extra important for people who spend a lot of time away from the office, perhaps traveling for work, and need to access files on the go. Along with cloud storage security advantages, this is one of the top reasons why everyone is using clouds. Some cloud systems also allow real-time collaboration, so more than one person can make changes to a file at any one time. This is perfect for project management and teamwork scenarios.

6. Organized

We can control what information is stored and how. While it is possible to simply upload everything you have, you don't need to. If you want, you can just keep your most important data on the cloud system and leave the rest. Within the cloud, you can create folders to organize your information in a way that suits you. That way, it's easy for you to navigate and access.

7. Intrusion Detection

Online secure storage can serve many users at the same time. Successful cloud security systems rely on identifying when someone tries to break into the system. Multiple levels of detection ensure cloud vendors can even stop intruders who break past the network's initial defenses.

CHAPTER2

LITERATURE SURVEY

2.1 LITERATURE SURVEY

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

An efficient conjunctive keyword and phrase search scheme for encrypted cloud storage systems H. Poon and A. Miri

There have been increasing interests in the area of privacy-protected searching as industries continue to adopt cloud technologies. Much of the recent efforts have been towards incorporating more advanced searching techniques. Although many have proposed solutions for conjunctive keyword search, it is only recently that researchers began exploring phrase search over encrypted data. In this paper, we present a scheme that incorporates both functionalities. Our solution makes use of symmetric encryption, which provides computational and storage efficiency over schemes based on public key encryption. By considering the statistical properties of natural languages, we were able to design indexes that significantly reduce storage cost when compared to existing solutions. Our solution allows for simple ranking of results and requires a low storage cost while providing document and keyword security. By using both the index and the encrypted documents to performs searches, our scheme is also currently the only phrase search scheme capable of searching for non-indexed keywords.

A low storage phrase search scheme based on bloom filters for encrypted cloud services

Despite the many benefits of cloud technologies, there have also been significant

concerns regarding its security and privacy. To address the issues, much efforts have been made towards development of an encrypted cloud system. One of the key features being investigated is the ability to search over encrypted data. Although many have proposed solutions for conjunctive keyword search, few have considered phrase searching techniques over encrypted data. Due to the increased amount of information required to identify phrases, existing phrase search algorithms require significantly more storage than conjunctive keyword search schemes. In this paper, we propose a phrase search scheme, which takes advantage of the space efficiency of Bloom filters, for applications requiring a low storage cost. It makes use of symmetric encryption, which provides computational and storage efficiency over schemes based on public key encryption. The scheme provides simple ranking capability, can be adapted to non-keyword search and is suitable against inclusion-relation attack.

Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query Z. Fu, X. Sun, N. Linge, and L. Zhou

In recent years, consumer-centric cloud computing paradigm has emerged as the development of smart electronic devices combined with the emerging cloud computing technologies. A variety of cloud services are delivered to the consumers with the premise that an effective and efficient cloud search service is achieved. For consumers, they want to find the most relevant products or data, which is highly desirable in the "pay-as-you use" cloud computing paradigm. As sensitive data (such as photo albums, emails, personal health records, financial records, etc.) are encrypted before outsourcing to cloud, traditional keyword search techniques are useless. Meanwhile, existing search approaches over encrypted cloud data support only exact or fuzzy keyword search, but not semantics-based multi-keyword ranked search. Therefore, how to enable an effective searchable system with support of ranked search remains a very challenging problem. This paper proposes an effective approach to solve the problem of multi-keyword ranked search over encrypted cloud data supporting synonym queries. The main contribution of this paper is summarized in two aspects: multi-keyword ranked search to achieve more accurate search results and synonym-based search to support synonym queries. Extensive experiments on real-world dataset were performed to validate the approach, showing

that the proposed solution is very effective and efficient for multikeyword ranked searching in a cloud environment.

An effective fuzzy keyword search scheme in cloud computing H.Tuo

With the development of cloud computing, individuals and enterprises stored their data in the cloud for great flexibility and economic savings. Many keyword search schemes over encrypted data with privacy preserving were proposed, however, few schemes cloud efficiently support the similarity search. In this paper, we investigate the issue on fuzzy search over cloud data, then by using technique of filter, we improve a efficient keyword search scheme to achieve fuzzy searching with low cost, which is suit for practical cloud computing.

Encrypted phrase searching in the cloud S. Zittrower and C. C. Zou

As cloud computing is increasing in popularity, it is difficult to both maintain privacy in datasets while still providing adequate retrieval and searching procedures. This paper introduces a novel approach in the field of encrypted searching that allows both encrypted phrase searches and proximity ranked multi-keyword searches to encrypted datasets on untrusted cloud. By storing encrypted keyword-location data along with specially truncated encrypted keyword indexes in a relational database, we are able to allow for a full range of search features in our encrypted searches, something that has never been accomplished before. Furthermore, our approach permits the encrypted corpus and index to both be stored on cloud data servers. We modify currently available open-source search engine software to complete a prototype and provide results from experiments on a large scale real-world dataset that has more than half a million documents.

Phrase search over encrypted data with symmetric encryption scheme Y. Tang,

D. Gu, N. Ding, and H. Lu

We study the case of searching over encrypted data from a remote server. In order to retrieve the encrypted documents that satisfy a client's criteria, a special index must be built and sent by the client together with encrypted documents. A trapdoor will also be produced to offer the privilege to search on the index. In the area of searchable encryption, many works mainly focused on search criteria consisting of a

single keyword or conjunctive keywords. Up until now, searching of the exact documents that contain a phrase, or consecutive keywords still remains an unsolved problem. We first define the model of phrase search over encrypted data with symmetric encryption and its security definition based on the latest security definition raised by R. Curtmola. Then we propose a construction for phrase search with symmetric encryption (PSSE), which meets the functionality of searching a phrase over encrypted documents securely and efficiently. The computing complexity of our scheme when performing a query is linear in the size of the phrase, and at a moderate communication cost between server and client as well. In addition, we prove that our scheme achieves non-adaptive security.

"VABKS: Verifiable Attribute-essentially based Keyword Search over Outsourced Encrypted Data", Q. Zheng, S. Xu, and G. Ateniese,

As a rule lately for records owner to outsource their information to the cloud. Since the cloud can't be totally depended on, the outsourced data must be mixed. This at any rate brings an extent of issues, for instance, How need to a data proprietor permit look abilities to the actualities customers? In what potential can the certify data customers investigate an insights proprietor's outsourced mixed data? By what way can the realities clients be guaranteed that the cloud reliably done the interest commitments for his or her gain? Prodded by means of these request, we prescribe a novel cryptographic course of action, known as certain characteristic based watchword are hunting down (VABKS). The affiliation permits a data buyer, whose capabilities fulfill a records proprietor's front control approach, to (i) appearance over the records proprietor's outsourced encoded actualities, (ii) outsource the horrid request games to the cloud, and (iii) attest regardless of whether the cloud has enduringly played out the hunt duties. We formally symbolize the security states of VA B K S and painting an improvement that satisfies them. Execution assessment exhibits that the proposed plans are close by and deployable.

CHAPTER 3

AIM AND SCOPE

3.1 AIM OF PROJECT

The primary aim of this proposed system i.e. “Cloud Supported Secured Data Acquisition” is to achieve the data security and system efficiency. In the data acquisition and transmission process are of great significance and challenging, because the power grid-related data is sensitive and in huge amount. In this ,we present an efficient and secure data acquisition scheme based on CP-ABE (Cipher text Policy Attribute Based Encryption). Data acquired from the terminals will be partitioned into blocks and encrypted with its corresponding access sub-tree in sequence, thereby the data encryption and data transmission can be processed in parallel. The analysis shows that the proposed scheme can meet the security requirements of data acquisition in smart grid, and it also reduces response time overhead significantly compared to other popular schemes.

3.2 OBJECTIVES

- 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.
- 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. 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.

3.3 SCOPE

CP-ABE Model will present a methodology acquire data from the terminals partitioned into blocks and encrypted with its corresponding access sub-tree in sequence, thereby the data encryption and data transmission can be processed in parallel. Furthermore, we protect the information about the access tree with threshold secret sharing method, which can preserve the data privacy and integrity from users with the unauthorized sets of attributes.

3.4 ADVANTAGES

- It diminishes the time cost separated and exact strategies of insight.
- It diminishes reaction time overhead.
- Security is extreme

CHAPTER 4

SYSTEM DESIGN AND METHODOLOGY

4.1 EXISTING SYSTEM

The existing method based on CP-ABE (Ciphertext Policy Attribute Based Encryption). Data acquired from the terminals will be partitioned into blocks and encrypted with its corresponding access sub-tree in sequence, thereby the data encryption and data transmission can be processed in parallel. Furthermore, we protect the information about the access tree with threshold secret sharing method, which can preserve the data privacy and integrity from users with the unauthorized sets of attributes. The formal analysis demonstrates that the proposed scheme can fulfill the security requirements of the Cloud-supported IoT in smart grid. The numerical analysis and experimental results indicate that our scheme can effectively reduce the time cost compared with other popular approaches.

4.1.1 DISADVANTAGES

- Security is bad.
- Response time is extra crucial.
- It improves the time price.
- keyword searches are not possible
- Data access and retrieve ability is not efficient.

4.2 PROPOSED SYSTEM

According to our experiment, it also achieves a lower storage cost than all existing solutions the solution addresses the high computational cost noted in by reformulating phrase search as n-gram verification rather than a location search or a sequential chain verification. Our approach is also the first to effectively allow phrase search to run independently without first performing a conjunctive keyword search to identify candidate documents. The proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storage cost depending on the application.

4.2.1 ADVANTAGES

- keyword search can also performed
- Performance has been increased with the reasonable cost.
- It reduces the time cost compared with other approaches.
- It reduces response time overhead.
- Security is high.

4.3 SYSTEM FUNCTIONALITIES

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.

The input form of an information system should accomplish one or more of the following 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

4.3.1 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.

1. 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.

2. Select methods for presenting information.

3. 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.

4.4 REQUIREMENT SPECIFICATION

This proposed software runs effectively on a computing system that has the minimum requirements. Undertaking all the equipment necessities are not satisfied but rather exist in their systems administration between the customer's machines already. So the main need is to introduce appropriate equipment for the product.

The requirements are split into two categories, namely:

1. Software requirements
2. Hardware requirements

4.4.1 SOFTWARE REQUIREMENTS

The basic software requirements to run the program are:

- Operating System : Windows95/98/2000/XP
- Application Server : Tomcat5.0/6.X

- Front End : HTML, Jsp
- Scripts : JavaScript.
- Server side Script : Java Server Pages.
- Database : MySQL 5.0
- Database Connectivity : JDBC

4.4.2 HARDWARE REQUIREMENTS

The basic hardware required to run the program are:

- Processor : Pentium –III
- RAM : 256 MB (min)
- Hard Disk : 20 GB
- Key Board : Standard Windows Keyboard
- Mouse : Two or Three Button Mouse
- Monitor : SVGA

4.5 MODULES

1. Data Owner
2. Cloud Consumer
3. Cloud Server

1. Data Owner:

In this module first register with valid details after completing registration login with email and password then home page will appear. Now click on upload and fill the details and upload a file. Check the users request for data then generate key for that data. By using that key user can upload data into server. If we want to download data from the file then user send request to owner when owner accept the request then only user can download the file

2. Cloud Consumer:

In this module first register with valid details after completing registration, login with email and password then consumer homepage will appear. If we want to get data from the cloud then search the file with some keyword. Then automatically request will be sent to owner. When owner will accept the request then encrypt the data and send files to server. Then server will store the data in encrypted form. If we want to get data from the server then send request to owner then owner will accept our request the we can download the decrypted file.

3. Cloud Server:

In this module first login with valid details. In this we can view how many users are registered and how many owners are registered, users requests for data and view files uploaded by owner.

4.6 SYSTEM 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 of the 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.

CHAPTER 5

SOFTWARE DEVELOPMENT METHODOLOGY

5.1 ARCHITECTURAL DESIGN

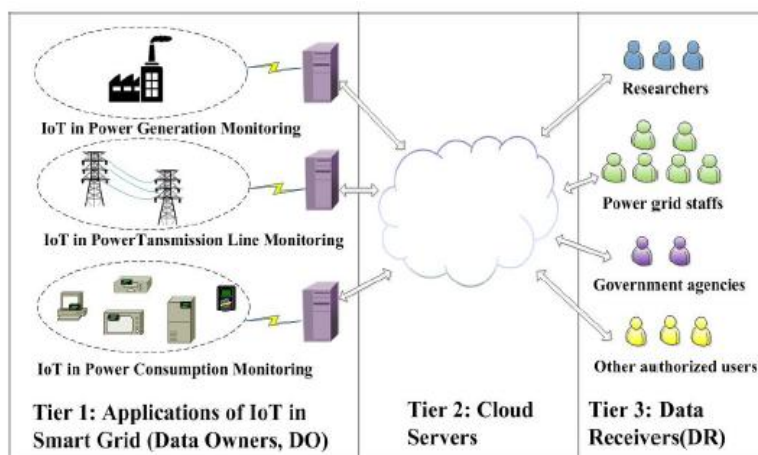


Fig 5.1 Work Flow Implementation

With the support of modern information technologies like the Internet of Things (IoT) and cloud computing, smart grid has emerged as the next-generation power supply network, in which the electricity is generated according to the real-time demands of electric equipment or household appliances. To make the smart grid more intelligent, a great number of IoT terminals are deployed to gather the status of the power grid timely for the control center. Some sample applications are the power transmission line monitoring, power generation monitoring, substation state monitoring, smart metering, electric energy data acquisition, smart home. For instance, in power transmission line monitoring scenario, using preplaced sensors, the status parameters of the transmission line and power towers can be gathered in real time, so that any fault can be diagnosed and located in a timely manner.

In smart grid, the different kinds of applications mentioned above all generate an enormous amount of data, which needs to be stored and managed efficiently. Cloud-IoT is proposed to address this issue. With the support of cloud computing, mass data from different IoT terminals can be collected and processed by local front-end servers, then transferred and stored in the cloud servers. The data in cloud can be accessed by various types of data users. The power grid staff can continually

monitor the status of power grid. Researchers and government agencies can analyze the data for research or policymaking

5.2 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.

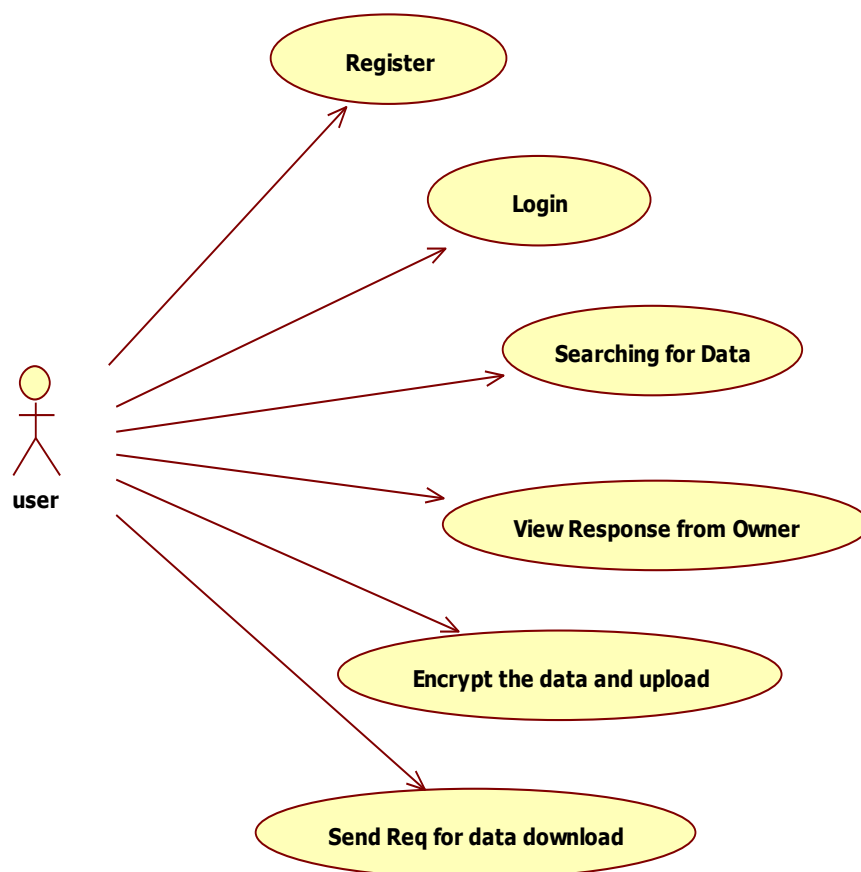


Fig 5.2 Use case diagram for cloud consumer

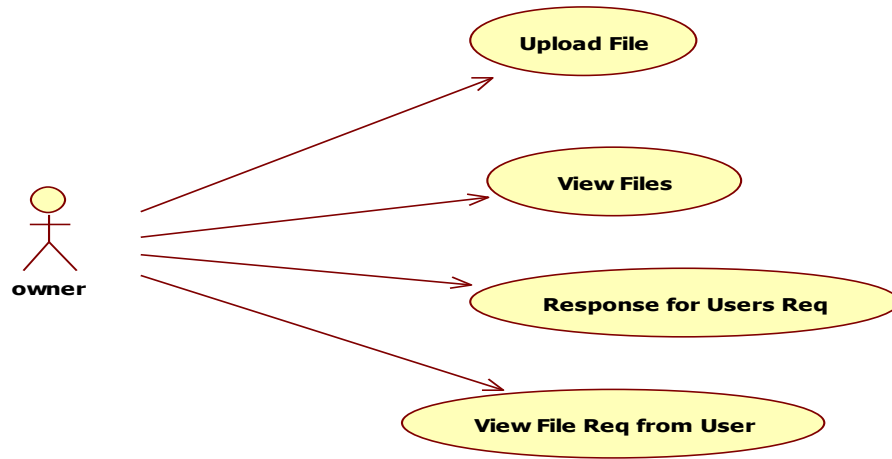


Fig 5.2.1 Use case diagram for data owner

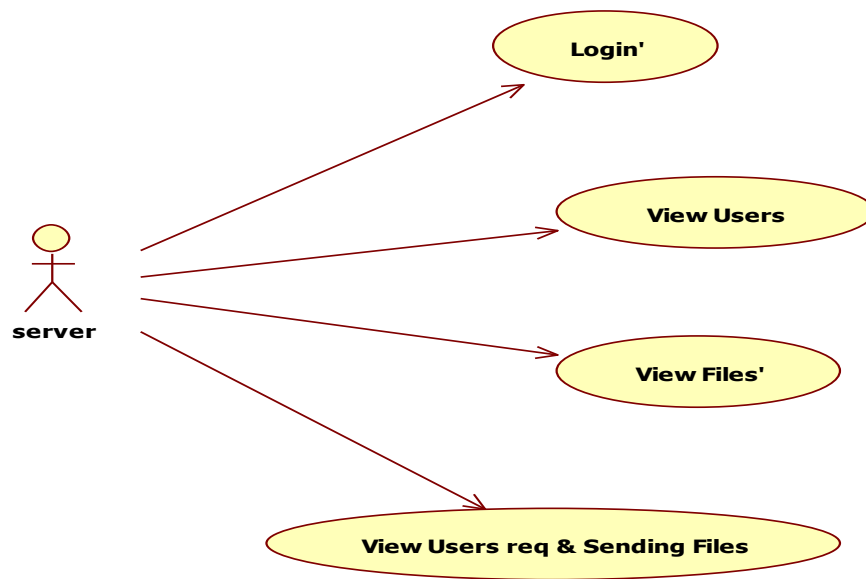


Fig 5.2.2 Use case diagram for cloud server

5.3 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.

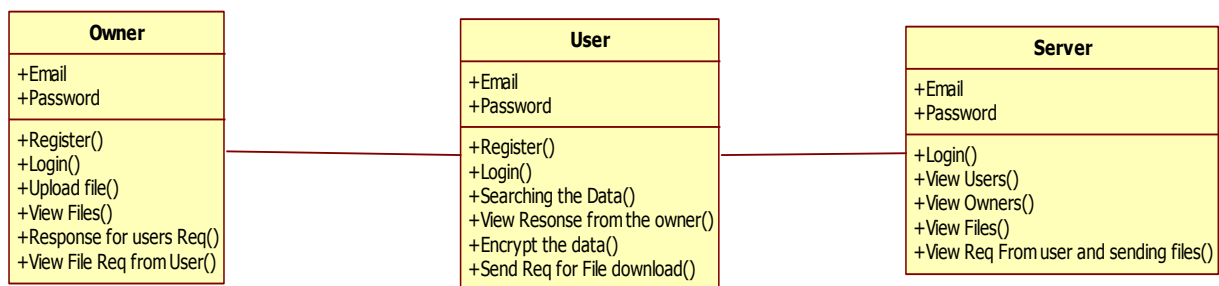


Fig 5.3 Class diagram

5.4 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. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams.

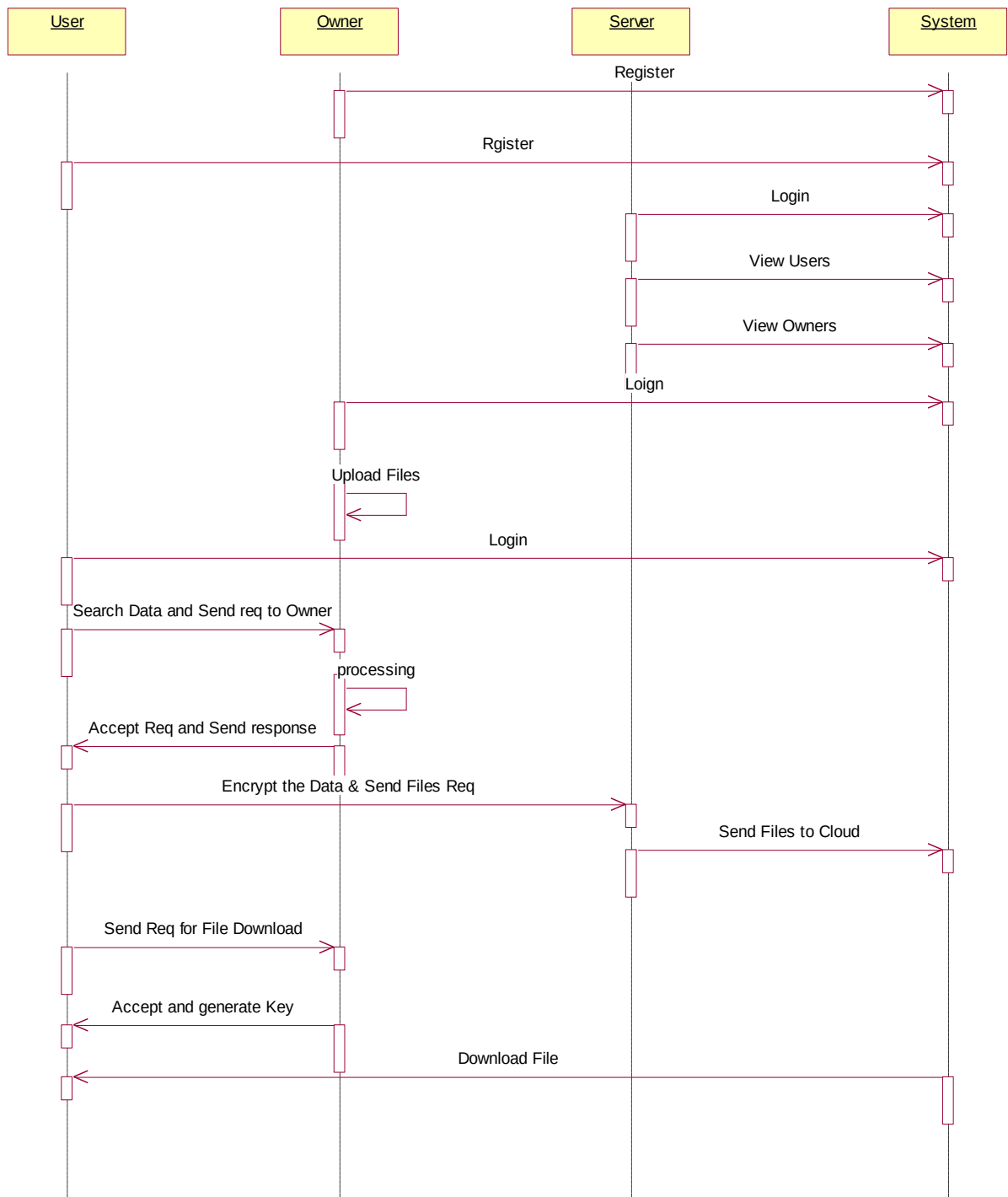


Fig 5.4 Sequence diagram

5.5 COLLABORATION DIAGRAM

In collaboration diagram the method call sequence is indicated by some numbering technique as shown below. The number indicates how the methods are called one after another. We have taken the same order management system to describe the collaboration diagram. The method calls are similar to that of a sequence diagram. But the difference is that the sequence diagram does not describe the object organization where as the collaboration diagram shows the object organization.

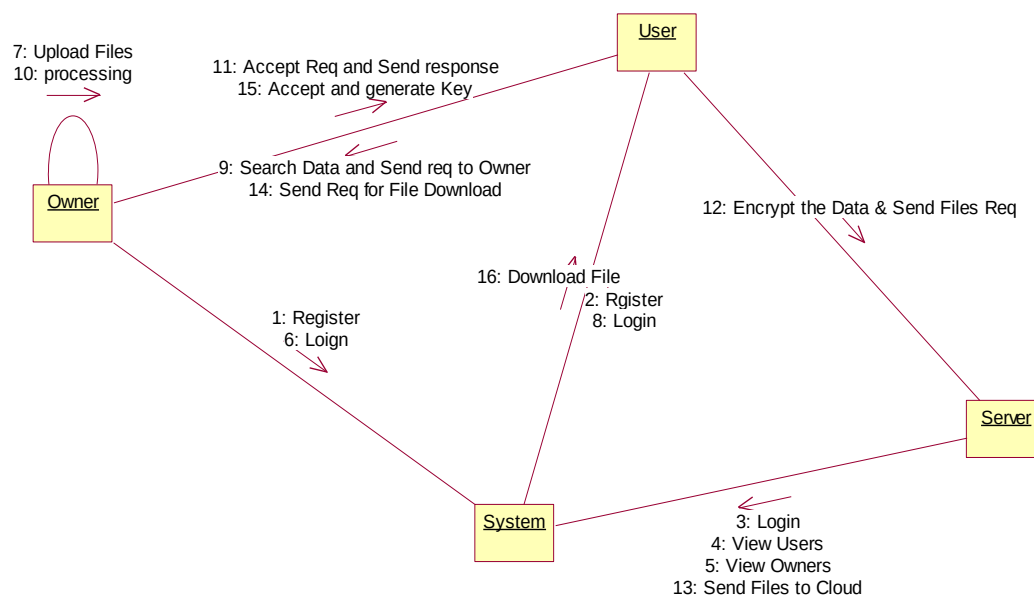


Fig 5.5 Collaboration diagram

5.6 ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

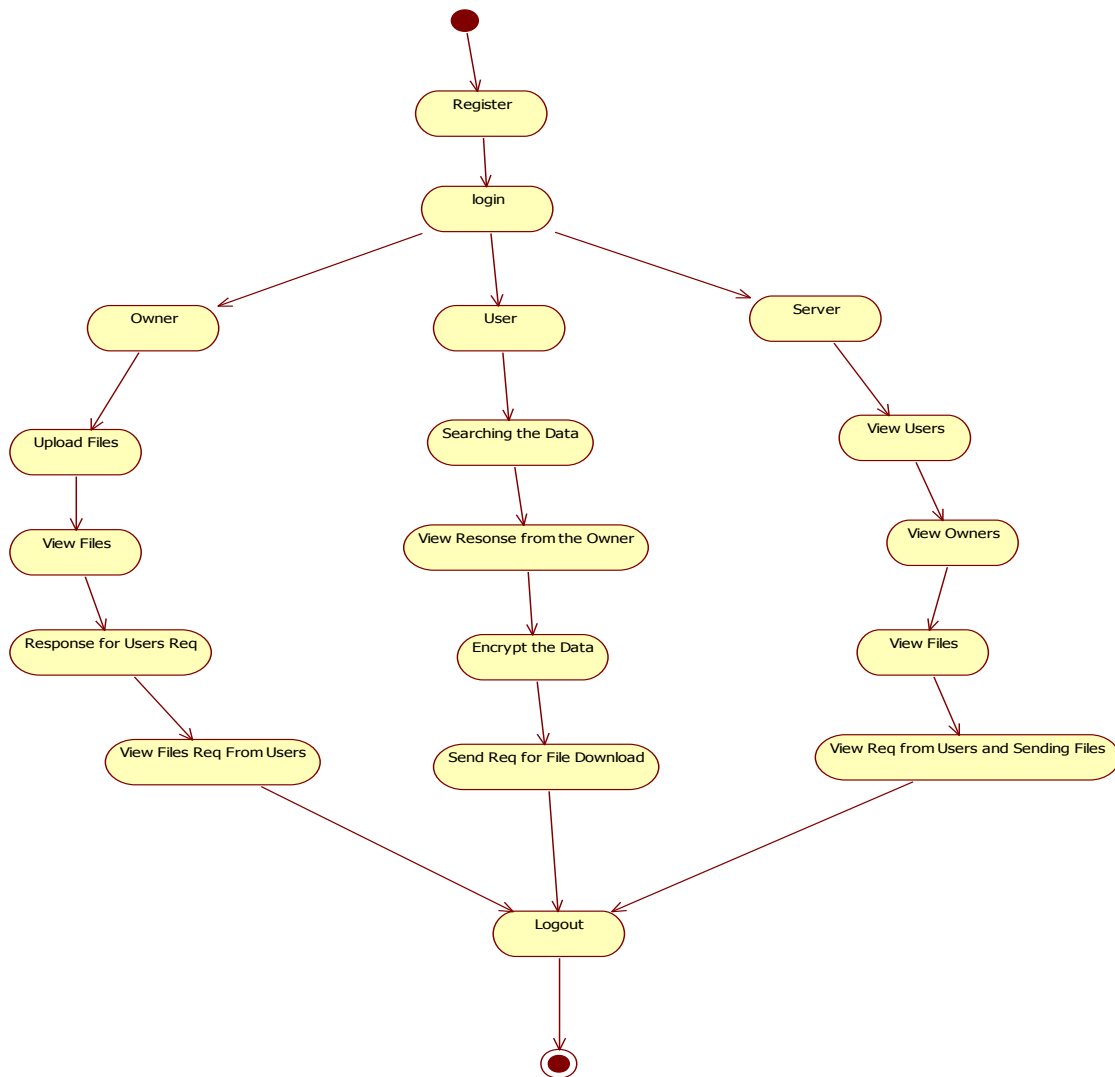


Fig 5.6 Activity diagram

5.7 COMPONENT DIAGRAM

Component diagrams are used to describe the physical artifacts of a system. This artifact includes files, executables, libraries etc. So the purpose of this diagram is different, Component diagrams are used during the implementation phase of an application. But it is prepared well in advance to visualize the implementation details. Initially the system is designed using different UML diagrams and then when the artifacts are ready component diagrams are used to get an idea of the implementation.

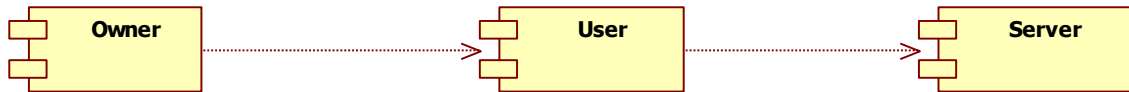


Fig 5.7 Component diagram

5.8 DEPLOYMENT DIAGRAM

Deployment diagram represents the deployment view of a system. It is related to the component diagram. Because the components are deployed using the deployment diagrams. A deployment diagram consists of nodes. Nodes are nothing but physical hardwares used to deploy the application.

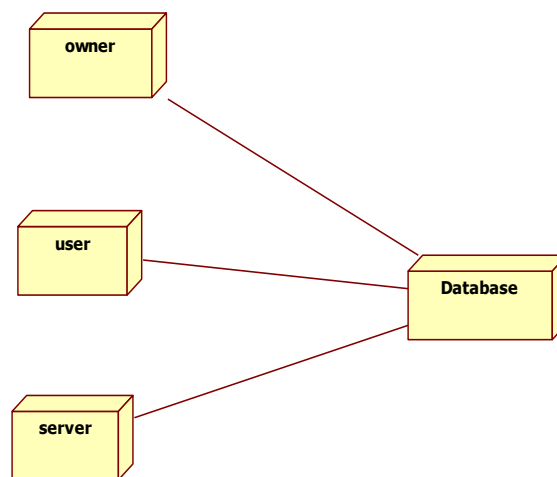


Fig 5.8 Deployment diagram

5.9. SYSTEM TESTING

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

a specific testing requirement

.

5.9.1 Unit Testing:

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

Test strategy and approach

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

Test objectives

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

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

5.9.2 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.

5.9.3 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 6

RESULTS AND DISCUSSION

6.1 SCREENSHOTS

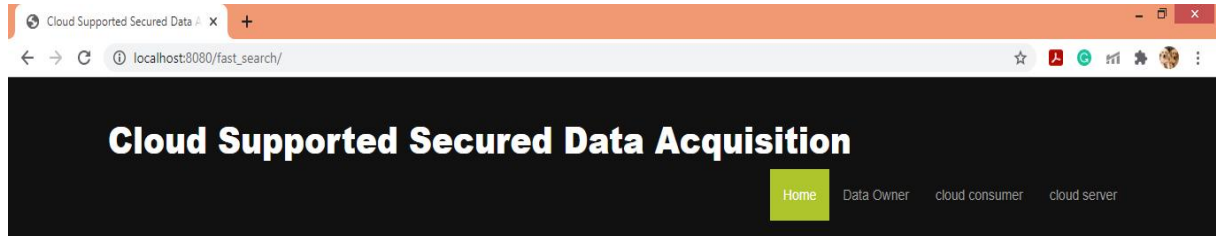


Fig 6.1 Home page

A screenshot of the "Registration Page" for a "Data Owner". The page has a dark header with the title "Cloud Supported Secured Data Acquisition" and a navigation bar with links: "Home" (highlighted in green), "Data Owner", "cloud consumer", and "cloud server". Below the header, a green message says "welcome to the owner Registration Page". The registration form contains the following fields and values:

- Name :
- Password :
- Phone :
- E-Mail :
- Address :

At the bottom of the form are two buttons: "User Register" and "Reset".

Fig 6.2 Data owner registration page

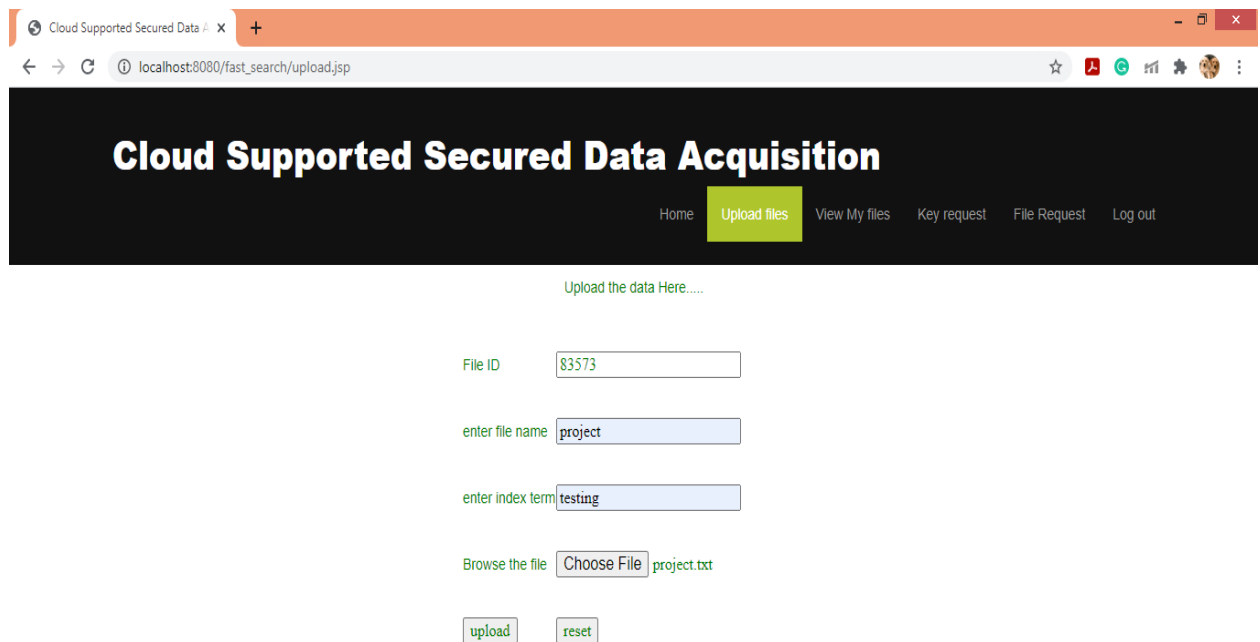


Fig 6.3 File Uploading in data owner page

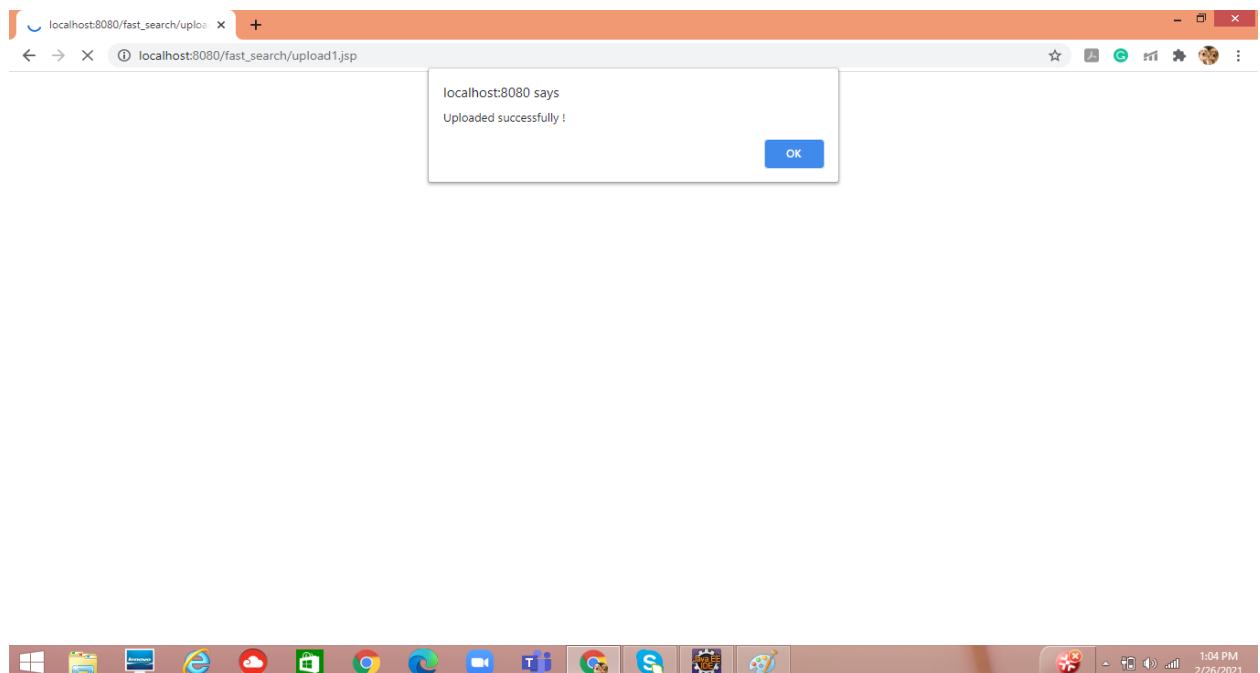


Fig 6.4 File uploaded successfully in data owner login page

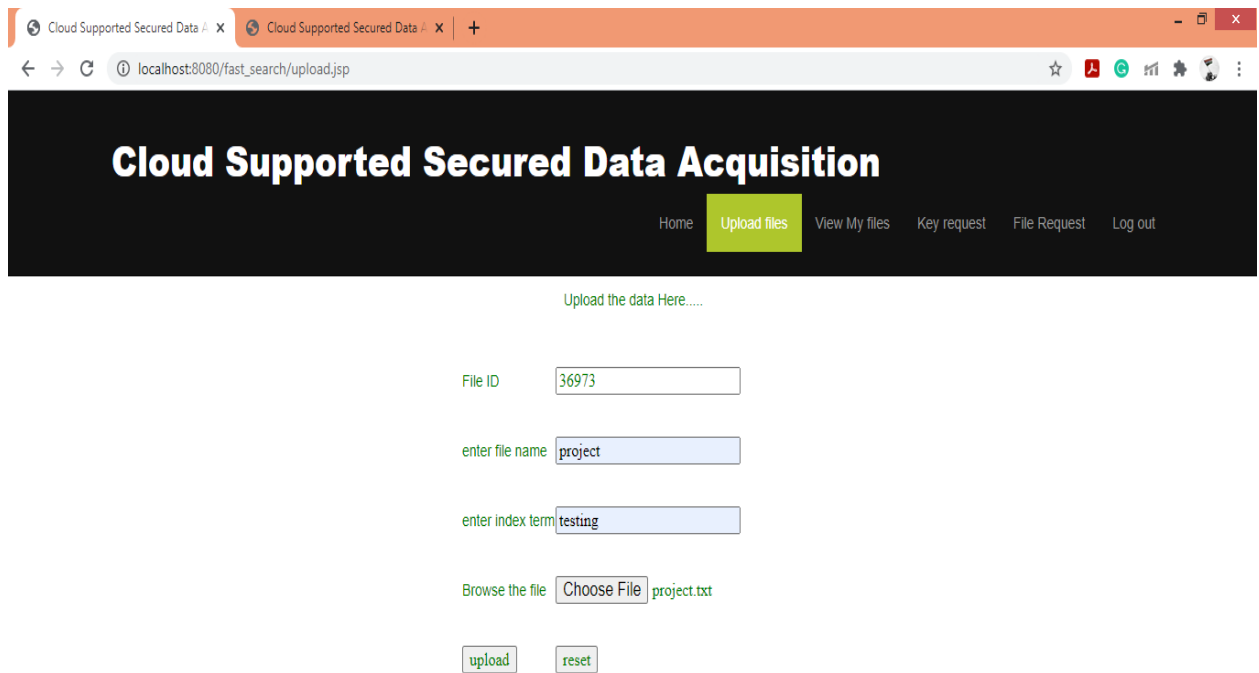


Fig 6.5 Same file is uploading again by owner

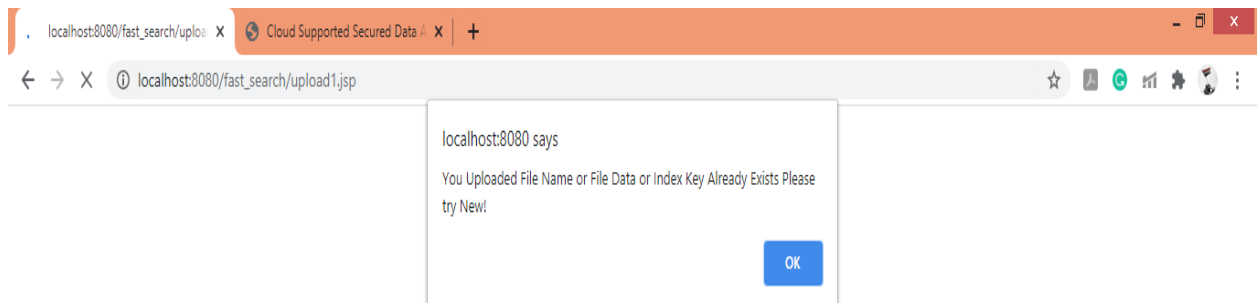


Fig 6.6 It displays same file is already exists

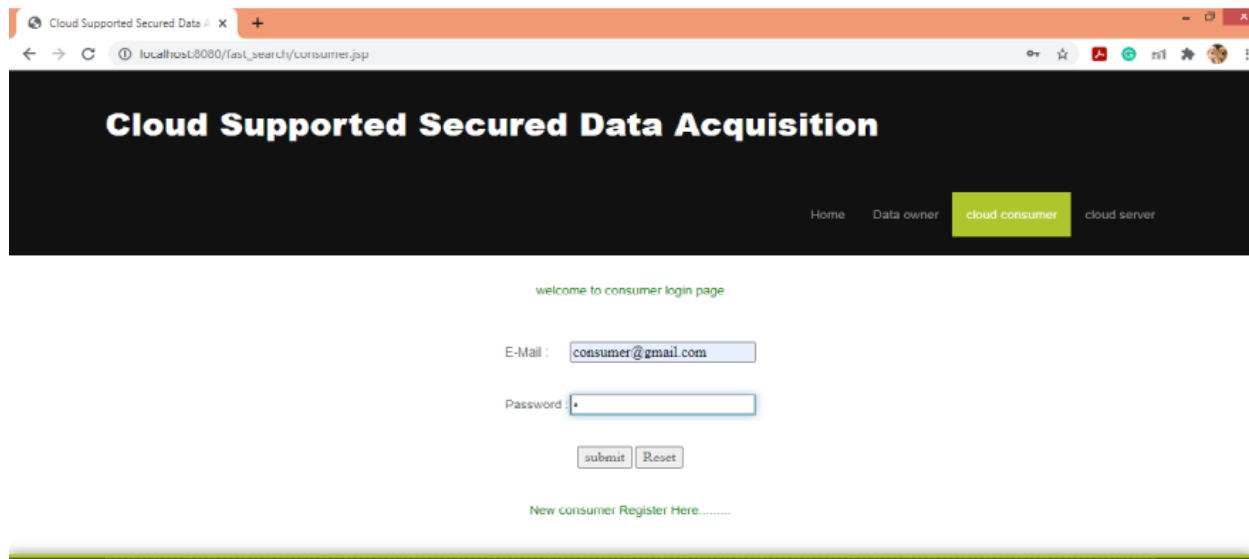


Fig 6.7 Consumer login page

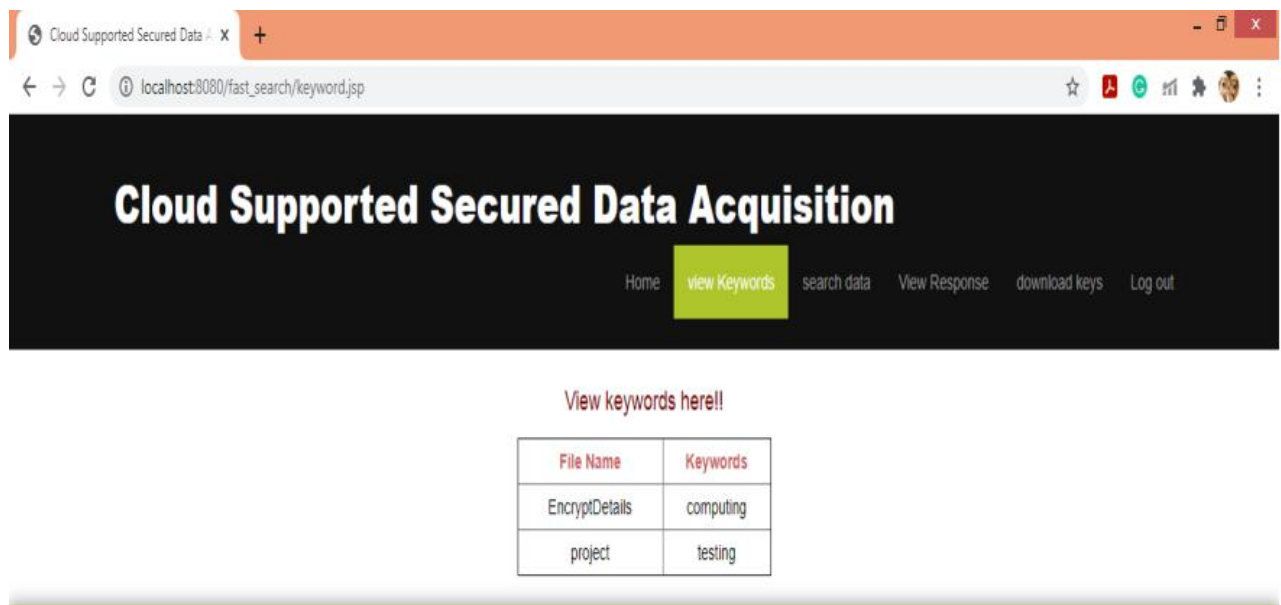


Fig 6.8 Keywords

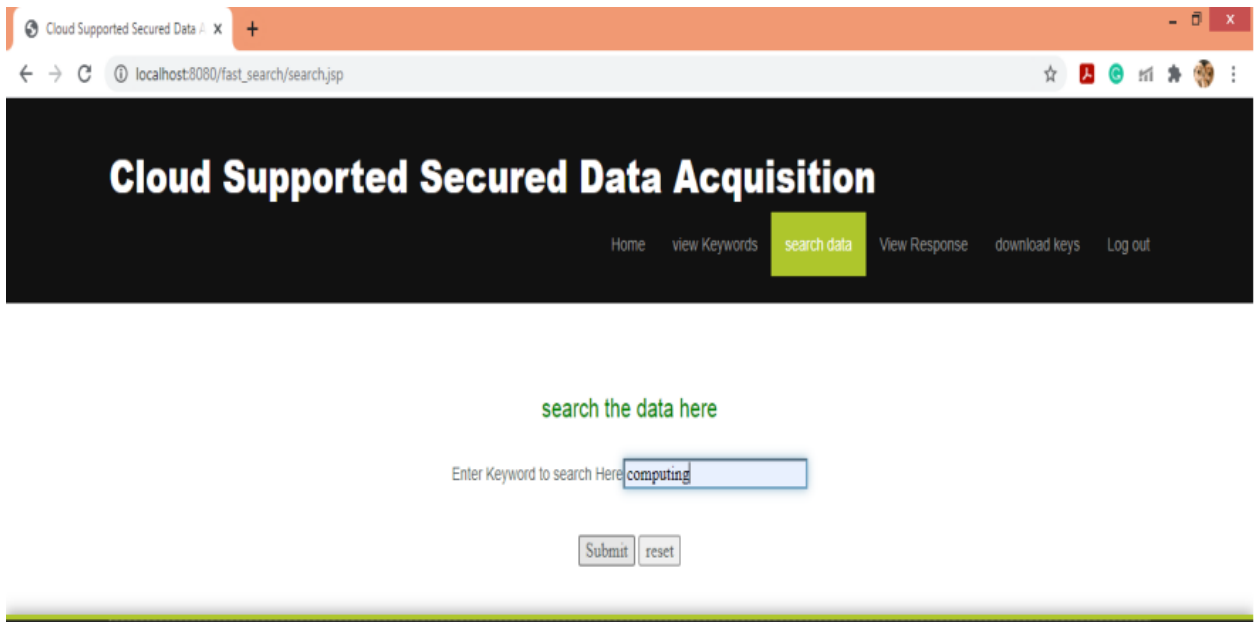
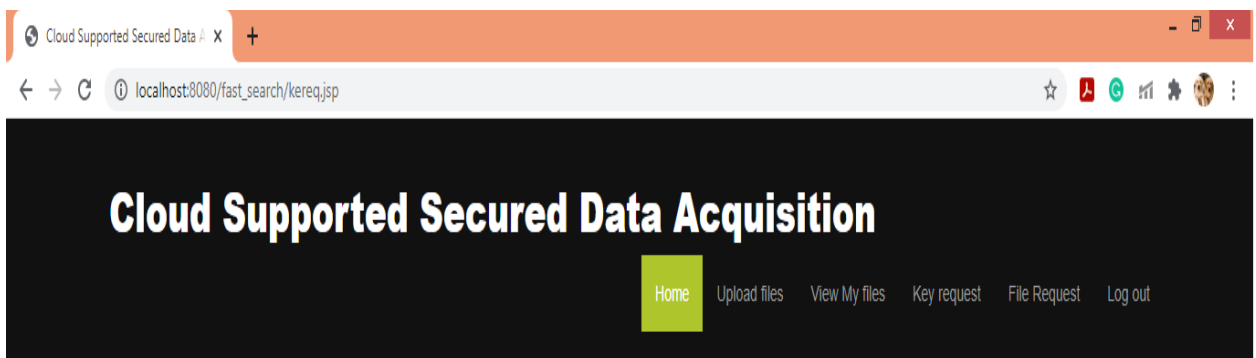
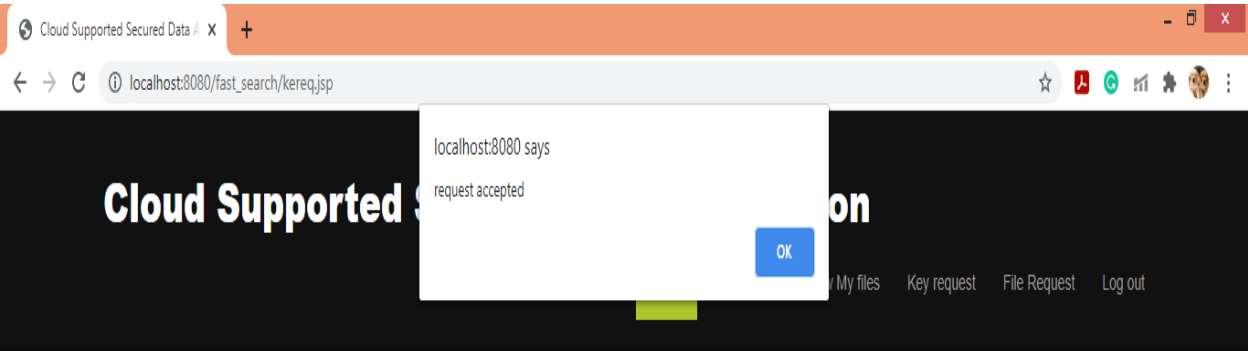


Fig 6.9 Keyword entered for generating unique key



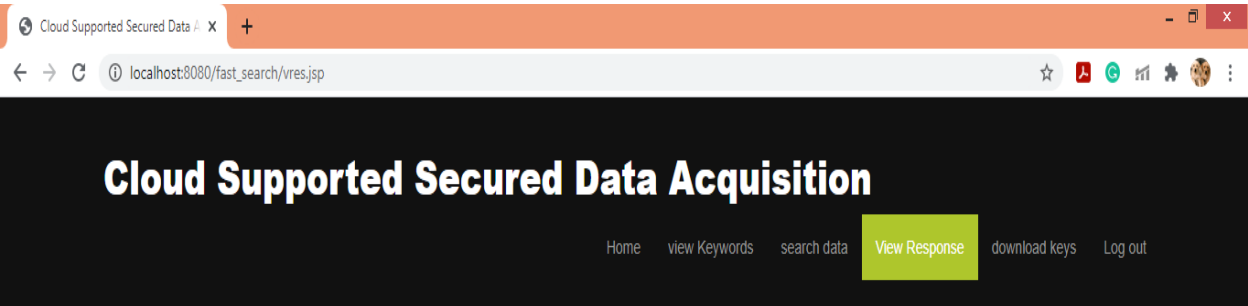
Request Id	Mail	Keyword	Generate Key	Reject
56	consumer@gmail.com	testing	<button>Generate Key</button>	Reject

Fig 6.10 Generating key for keyword



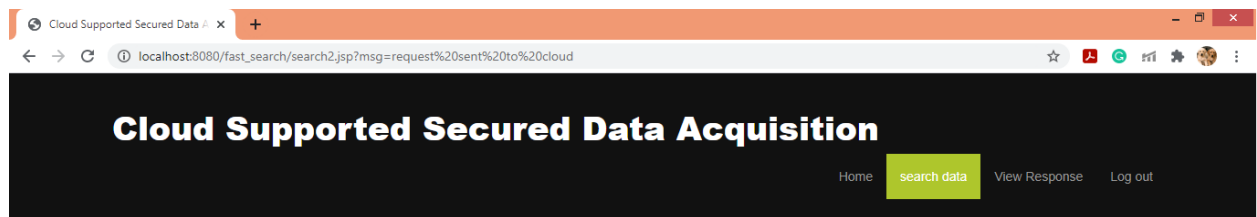
Request Id	Mail	Keyword	Generate Key	Reject
56	consumer@gmail.com	testing	Generate Key	Reject

Fig 6.11 Request accepted by data owner for generating key for keyword



request id	User mail	keyword	Key	status	File id
54	consumer@gmail.com	computing	nokey	req	92510
56	consumer@gmail.com	testing	3R28C	accept	83573

Fig 6.12 Key successfully generated for keyword testing



Enter Key To Encrypt The Keyword	
Keyword	testing
Enter Key	3R28C
Encrypt Keyword	

Fig 6.13 Encrypted keyword generating

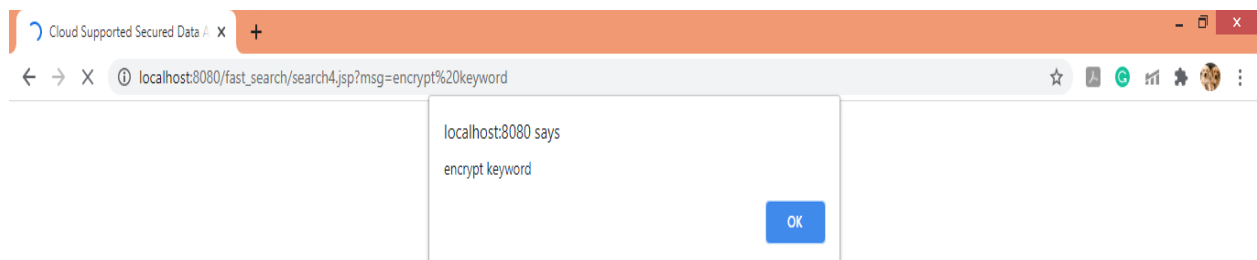


Fig 6.14 Successfully created encrypted keyword

The screenshot shows a web browser window with the title 'Cloud Supported Secured Data Acquisition'. The address bar shows 'localhost:8080/fast_search/search4.jsp?msg=encrypt%20keyword'. The page has a dark header with the title and navigation links: 'Home', 'search data' (highlighted in green), 'View Response', and 'Log out'. Below the header, there is a form titled 'Send Request To Cloud'. The form contains two input fields: 'Keyword' with the value 'testing' and 'Encrypted Keyword' with the value 'dGVzdGluZw=='. A 'Send to cloud' button is located at the bottom right of the form.

Send Request To Cloud	
Keyword	testing
Encrypted Keyword	dGVzdGluZw==
Send to cloud	

Fig 6.15 Sending request to cloud

The screenshot shows a web browser window with the title 'Cloud Supported Secured Data Acquisition'. The address bar shows 'localhost:8080/fast_search/server.jsp'. The page has a dark header with the title and navigation links: 'Home', 'Data owner', 'cloud consumer', and 'cloud server' (highlighted in green). Below the header, there is a green message 'welcome to the server Page'. The login form contains two input fields: 'E-Mail' with the value 'server@gmail.com' and 'Password' with the value '*****'. There are 'submit' and 'Reset' buttons at the bottom of the form.

welcome to the server Page

E-Mail:

Password:

Fig 6.16 Cloud server login page

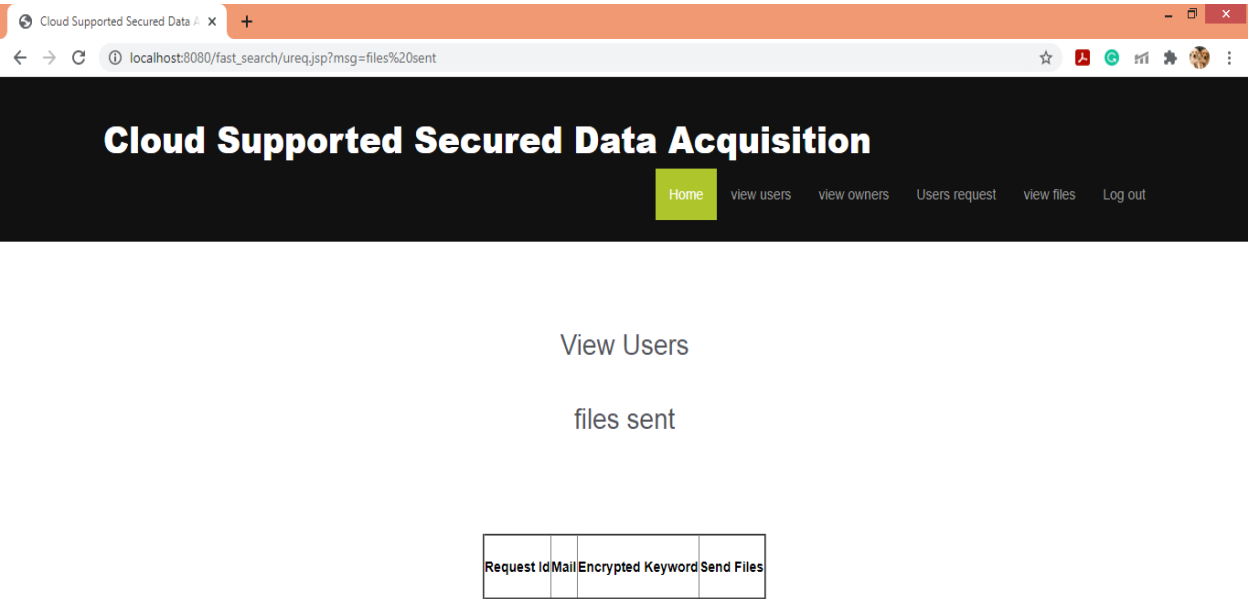


Fig 6.17 Cloud server accept the customer request and send files to customer

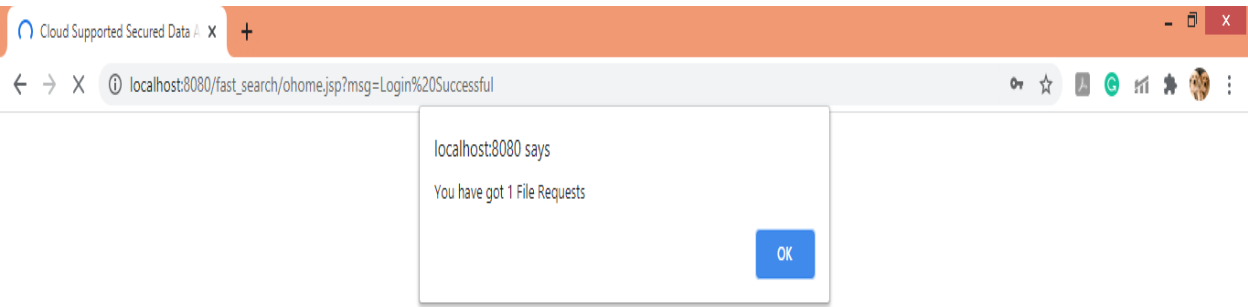


Fig 6.18 Data owner got file request

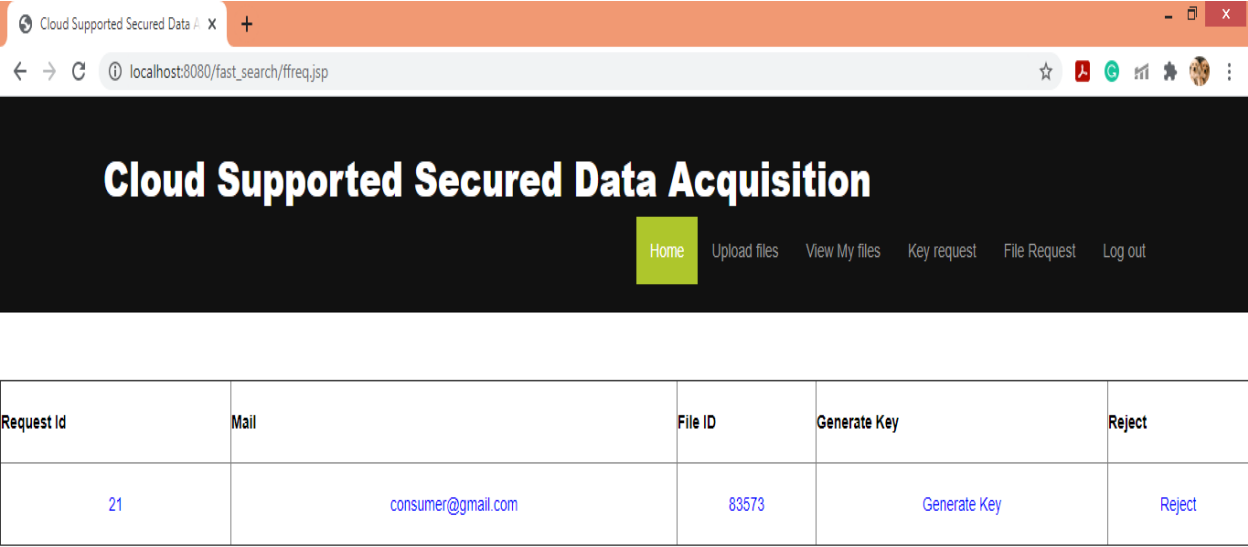


Fig 6.19 Data owner generating key for file Project

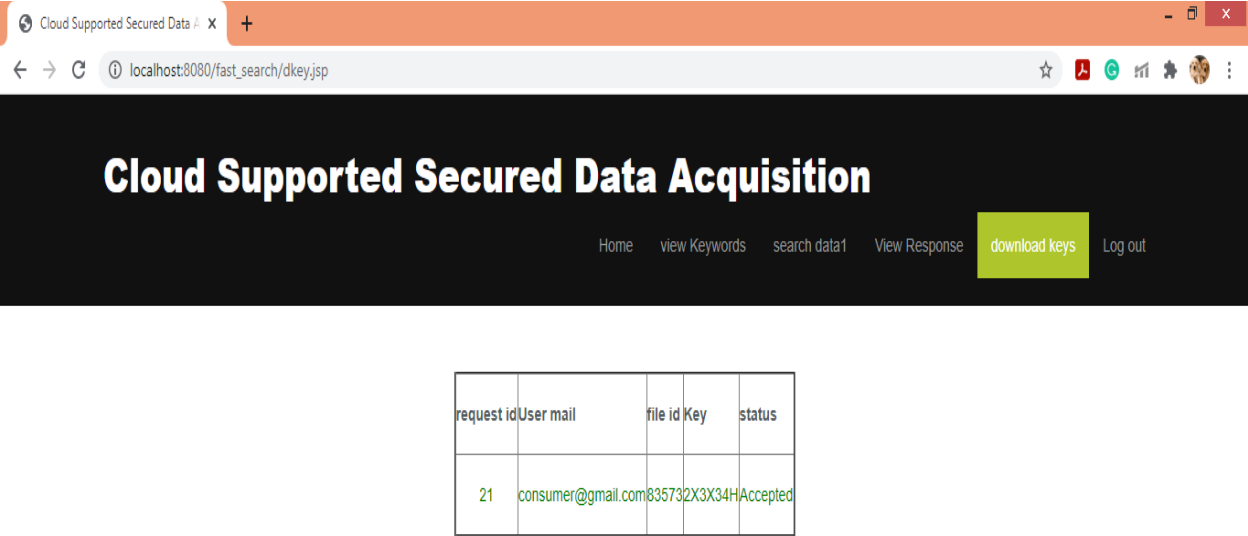


Fig 6.20 Key generated successfully for file

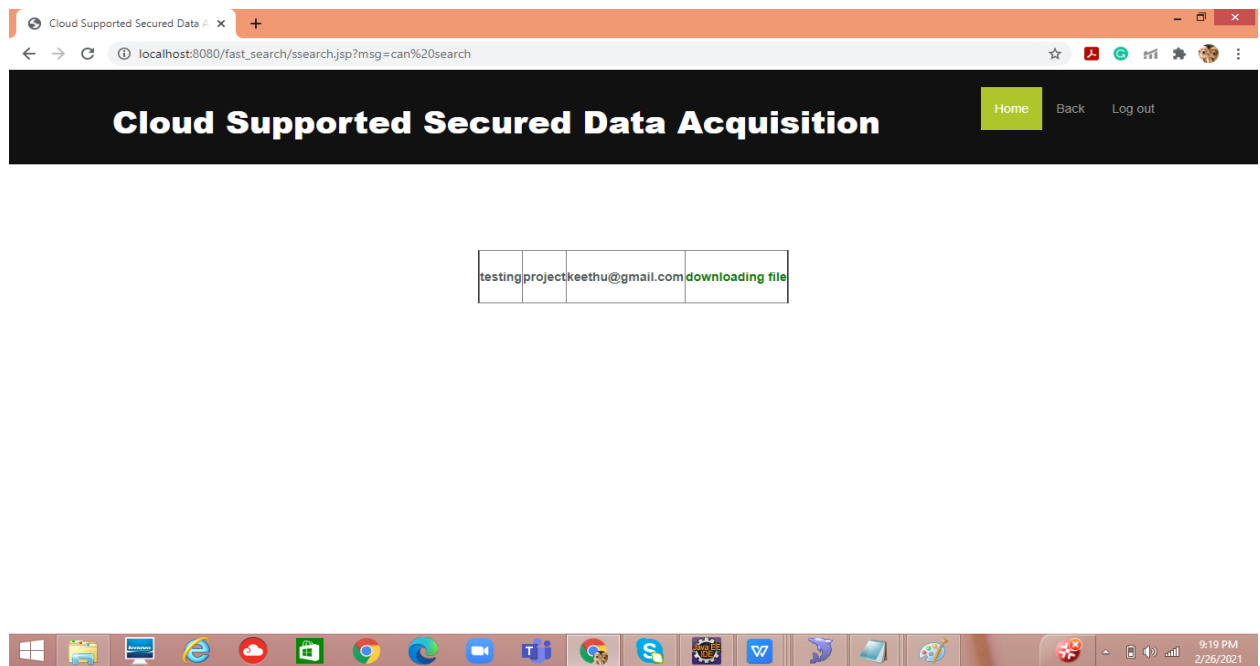


Fig 6.21 Consumer want to download file

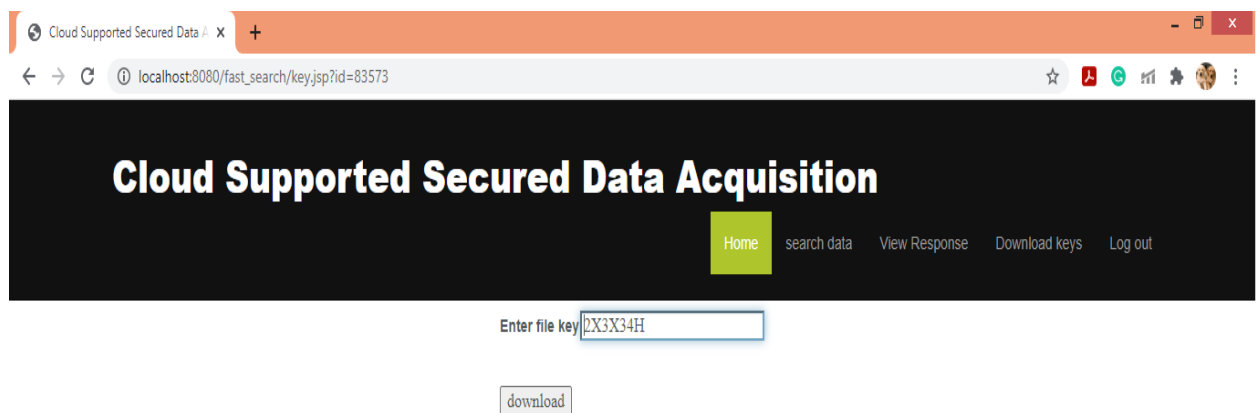


Fig 6.22 Key entered for downloading file

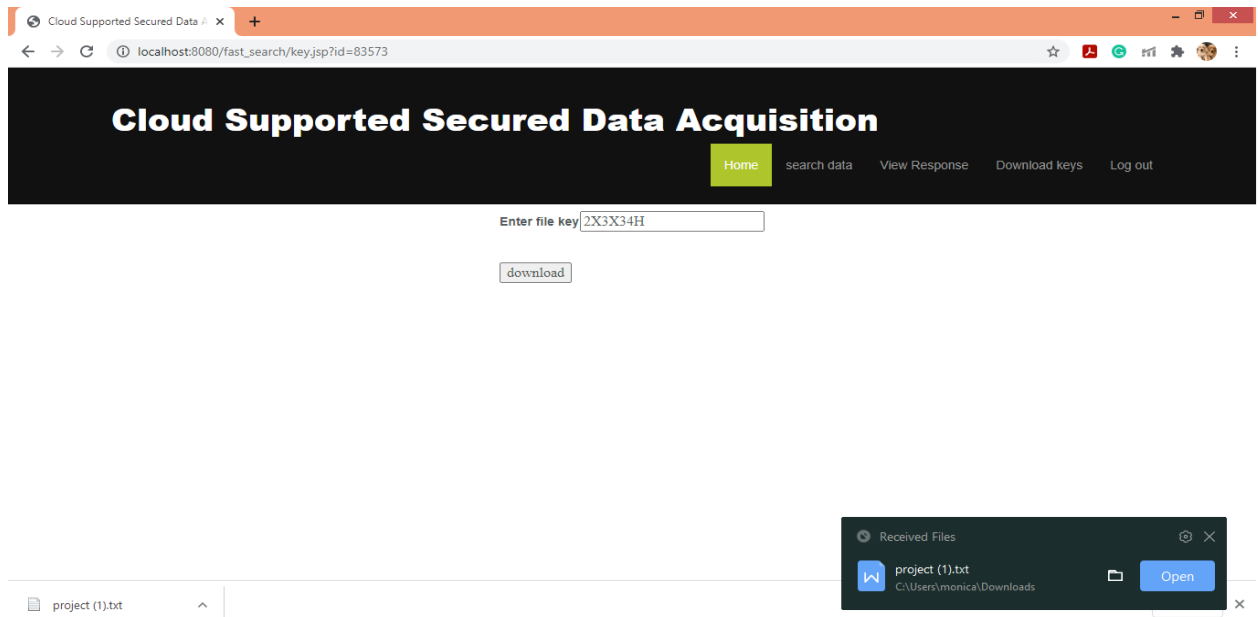


Fig 6.23 Secured File is downloaded successfully

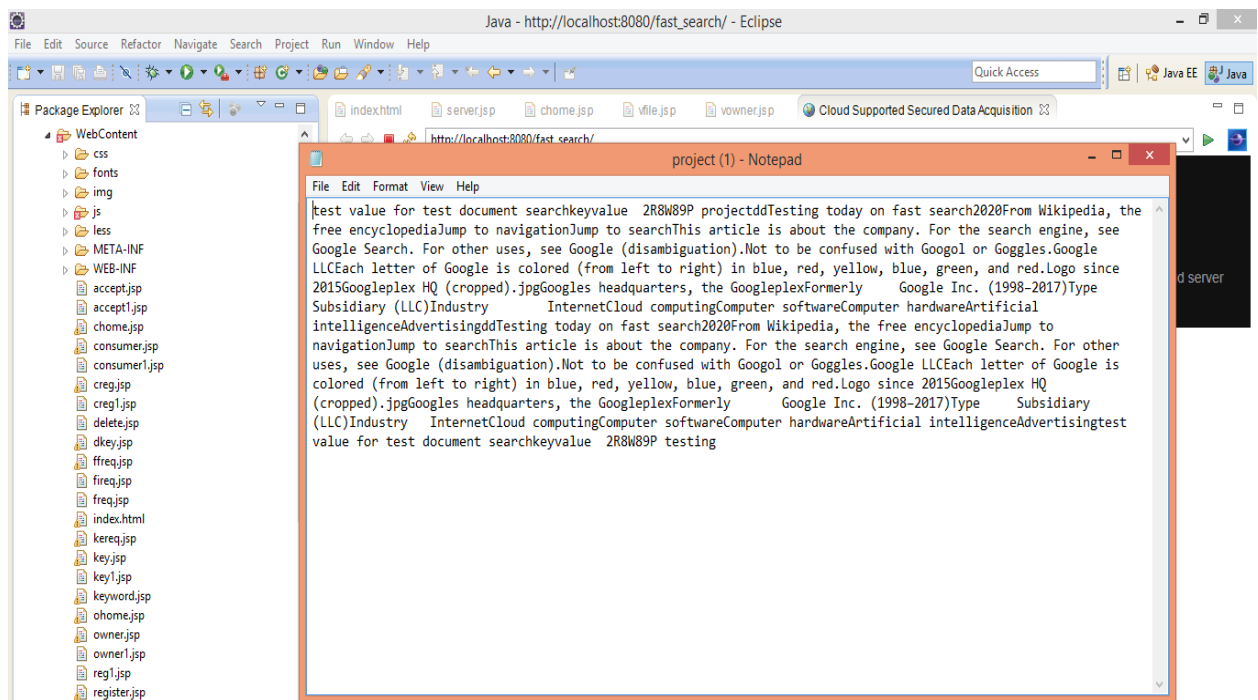


Fig 6.24 User is viewing downloaded data file

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

In this paper, we presented a phrase search scheme that is significantly faster than existing approaches, requiring only a single round of communication and verifications. The solution addresses the high computational cost noted by reformulating phrase search as n-gram verification rather than a location search or a sequential chain verification. Our schemes consider only the existence of a phrase, omitting any information of its location. Our schemes do not require sequential verification, is parallelizable and has a practical storage requirement. Our approach is also the first to effectively allow phrase search to run independently without first performing a conjunctive keyword search to identify candidate documents. The technique of constructing a phrase search scheme introduced enables fast verification in the same manner as indexing. According to our experiment, it also achieves a lower storage cost than all existing solutions, where a higher computational cost was exchanged in favor of lower storage. While exhibiting similar communication cost to leading existing solutions, the proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storage cost depending on the application. An approach is also described to adapt the scheme to defend against inclusion-relation attacks. Various issues on security and efficiency, such as the effect of long phrases and precision rate, were also discussed to support our design choices.

7.2 FUTURE WORK

In proposed system, it achieves a lower storage cost than all existing solutions the solution addresses the high computational cost noted in by reformulating phrase search as n-gram verification rather than a location search or a sequential chain verification. Our approach is also the first to effectively allow phrase search to run independently without first performing a conjunctive keyword search to identify candidate documents. The proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storage cost depending on the application.

REFERENCES

- [1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in In proceedings of Eurocrypt, 2004, pp. 506–522.
- [2] B. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in Network and Distributed System Security Symposium, 2004.
- [3] M. Ding, F. Gao, Z. Jin, and H. Zhang, "An efficient public key encryption with conjunctive keyword search scheme based on pairings," in IEEE International Conference on Network Infrastructure and Digital Content, 2012, pp. 526–530.
- [4] F. Kerschbaum, "Secure conjunctive keyword searches for unstructured text," in International Conference on Network and System Security, 2011, pp. 285–289.
- [5] C. Hu and P. Liu, "Public key encryption with ranked multikeyword search," in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 109–113.
- [6] Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," IEEE Transactions on Consumer Electronics, vol. 60, pp. 164–172, 2014.
- [7] C. L. A. Clarke, G. V. Cormack, and E. A. Tudhope, "Relevance ranking for one to three term queries," Information Processing and Management: an International Journal, vol. 36, no. 2, pp. 291–311, Jan. 2000.
- [8] H. Tuo and M. Wenping, "An effective fuzzy keyword search scheme in cloud computing," in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 786–789.

- [9] M. Zheng and H. Zhou, "An efficient attack on a fuzzy keyword search scheme over encrypted data," in International Conference on High Performance Computing and Communications and Embedded and Ubiquitous Computing, 2013, pp. 1647–1651.
- [10] S. Zittrower and C. C. Zou, "Encrypted phrase searching in the cloud," in IEEE Global Communications Conference, 2012, pp. 764–770.
- [11] Y. Tang, D. Gu, N. Ding, and H. Lu, "Phrase search over encrypted data with symmetric encryption scheme," in International Conference on Distributed Computing Systems Workshops, 2012, pp. 471–480.
- [12] H. Poon and A. Miri, "An efficient conjunctive keyword and phrase search scheme for encrypted cloud storage systems," in IEEE International Conference on Cloud Computing, 2015.
- [13] "A low storage phrase search scheme based on bloom filters for encrypted cloud services," to appear in IEEE International Conference on Cyber Security and Cloud Computing, 2015.
- [14] H. S. Rhee, I. R. Jeong, J. W. Byun, and D. H. Lee, "Difference set attacks on conjunctive keyword search schemes," in Proceedings of the Third VLDB International Conference on Secure Data Management, 2006, pp. 64–74.
- [15] K. Cai, C. Hong, M. Zhang, D. Feng, and Z. Lv, "A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack," in IEEE International Conference on Cloud Computing Technology and Science, 2013, pp. 339–346.