

**MULTI STAGE CLOUD SECURITY
FOR CLOUD DATA USING
AMALGAMATE DATA**

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

By

**PRUDHVI RAJ J (Reg.No - 40110480)
NAGARJUNA J (Reg.No – 40110479)**



**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 GANDHISALAI,
CHENNAI - 600119

APRIL- 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Category - I University by UGC

Accredited "A++" by NAAC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work **Prudhvi Raj J (40110480)** and **Nagarjuna Reddy J (40110479)** who have done the Project work as a team entitled "**A MULTI STAGE CLOUD SECURITY FOR CLOUD DATA USING AMALGAMATE DATA**" under our supervision from June 2023 to April 2024.


13/4/24
Internal Guide

Dr. M. SELVI B.E., M.TECH., Ph.D.


HEAD OF THE DEPARTMENT
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SATHYABAMA
Head of the Department
INSTITUTE OF SCIENCE AND TECHNOLOGY
Dr. L. LAKSHMANAN M.E., Ph.D.
Jeppiaar Nagar, Rajiv Gandhi Salai,
Chennai - 600 119.

Submitted for Viva voce Examination held on 13/4/24


13/4/24
Internal Examiner


13/4/24
External Examiner

DECLARATION

I **PRUDHVI RAJ J** (Reg no - 40110480) hereby declare that the Project Report entitled "" done by us under the guidance of **Dr. M. Selvi, B.E., M.TECH., Ph.D.** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**.

DATE: 13/04/24

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 Computer science, **Dr. L. Lakshmanan M.E., Ph.D.**, Head 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 **Dr. M. Selvi, M.Tech.,Ph.D** ,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

The development of cloud computing technology with the explosive growth of unstructured data, cloud storage technology gets more attention and better development. The cloud provider does not have suggestions regarding the information and the cloud data stored and maintained globally anywhere in the cloud. The privacy protection schemes are usually based on encryption technology. There are many privacy preserving methods in the side to prevent data in cloud. We propose a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Here we are using Hash-Solomon code algorithm is designed to divide data into different parts. If the one data part missing we lost the data information. In this framework we are using bucket concept based algorithms and secure the data information and then it can show the security and efficiency in our scheme. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively Software as a Service (SaaS): Client releases their application on a hosting environment which can be accessed through network from various clients by application users. The client does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings. Google Apps and Microsoft Office 365 are the examples for Saas..

Chapter No	Title	Page No
0	ABSTRACT	v
0	LIST OF FIGURES	vii
1	INTRODUCTION	1
2	LITERATURE SURVEY	3
2.1	2.1 EXISTING SYSTEM	8
2.2	2.2 PROPOSED SYSTEM	9
3	REQUIREMENT ANALYSIS	10
4	MODULES	15
5	REFERENCES	18

LIST OF FIGURES

FIGURE NO	FIGURE NAME	Page No.
3.1	System Architecture	11
3.2	Data Flow Diagram	11
3.3	Usecase Diagram	12
3.4	Sequence Diagram	13
3.5	Collaboration Diagram	14
4.1	Home Page	17
4.2	Registration Page	18
4.3	Login Page	18

CHAPTER 1

INTRODUCTION

In Computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or transported. Every month, they pay for what they consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally. Cloud computing is usually Internet-based computing. The cloud is a metaphor for the Internet based on how the internet is described in computer network diagrams; which means it is an abstraction hiding the complex infrastructure of the internet. It is a style of computing in which related capabilities are provided "as a service", allowing users to access technology-enabled services from the Internet ("in the cloud") without knowledge of, or control over the technologies behind these servers.

Fog computing can be perceived both in large cloud systems and big data structures, making reference to the growing difficulties in accessing information objectively. This results in a lack of quality of the obtained content. The effects of fog computing on cloud computing and big data systems may vary. However, a common aspect that can be extracted is a limitation in accurate content distribution, an issue that has been tackled with the creation of metrics that attempt to improve accuracy. Fog networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives, dense geographical distribution and local resource pooling, latency reduction and backbone bandwidth savings to achieve better quality of service (QoS) and edge analytics/stream mining, resulting in superior user-experience and redundancy in case of failure while it is also able to be used in AAL scenarios.

In order to protect user's privacy, we propose a TLS framework based on fog computing model. The TSL framework can give user a certain power of management

and effectively protect user's privacy. As mentioned, the interior attack is difficult to resist. Traditional approaches work well in solving outside attack, but when CSP itself has problems, traditional ways are all invalid. Different from the traditional approaches, in our scheme, user's data is divided into three different-size parts with encoding technology. Each of them will lack a part of key information for confidentiality. Combining with the fog computing model, the three parts of data will be stored in the cloud server, the fog server and user's local machine according to the order from large to small. By this method, the attacker cannot recover the user's original data even if he gets all the data from a certain server. As for the CSP, they also cannot get any useful information

without the data stored in the fog server and local machine because both of the fog server and local machine are controlled by users

CHAPTER 2.

LITERATURE SURVEY

Title 1:

A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-cities

Author:

J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun'

Content:

Attribute-based encryption (ABE) is a promising cryptography technique which can be used in the cloud to solve many security issues. In this paper, we propose a framework for urban data sharing by exploiting the attribute-based cryptography. In order to fit the real world ubiquitous-cities utilization, we extend our scheme to support dynamic operations. In particular, from the part of performance analysis, it can be concluded that our scheme is secure and can resist possible attacks. Moreover, experimental results and comparisons show that our scheme is more efficient in terms of computation. From the experiment analysis, we can see that our dynamic operations have less computation 340 time. We hold that this framework can be applied into the real urban data sharing applications in real-world ubiquitous-cities. The features of this framework is suitable for citizens' sensitive data protection and utilization, such as the life electricity consumption and healthcare information, which can only be utilized and modified by some specific people and users besides the data owners, With the accelerated process of urbanization, more and more people tend to live in cities, In order to deal with the big data that are generated by citizens and public city departments, new information and communication technologies are utilized to process the urban data, which makes it more easier to manage. Cloud computing is a novel computation technology. After cloud computing was commercialized, there have been lot of cloud-based applications. Since the cloud service is provided by the third party, the cloud is semi-trusted. Due to the features of cloud computing, there are many security issues in cloud computing.

Title 2:

Privacy-Preserving Smart Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data

Author:

Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang

Content:

we introduce conceptual graphs (CGs) as a knowledge representation tool. Then, we present our two schemes (PRSCG and PRSCG-TF) based on CGs according to different scenarios. In order to conduct numerical calculation, we transfer original CGs into their linear form with some modification and map them to numerical vectors. Second, we employ the technology of multi-keyword ranked search over encrypted cloud data as the basis against two threat models and raise PRSCG and PRSCG-TF to resolve the problem of privacy-preserving smart semantic search based on CGs. Finally, we choose a real-world data set: CNN data set to test our scheme. We also analyze the privacy and efficiency of proposed schemes in detail. The experiment results show that our proposed schemes are efficient. We implement our scheme on the real data set to prove its effectiveness and efficiency. For the further work, we will explore the possibility of semantic search over encrypted cloud data with natural language processing technology. Due to the scalability and high efficiency of cloud servers, the way for public data access is much more scalable, low-cost and stable, especially for the small enterprises: However, data owners are puzzled by the privacy of data and existing schemes prefer to using data encryption to solve the problem of information leakage. How to realize an efficient searchable encryption scheme is a challenging and essential problem.

Title 3:

A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing

Author:

2. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren

Content:

The feature vectors are protected by the secure KNN algorithm, and image pixels are encrypted by a standard stream cipher. In addition, considering the case that the authorized query users may illegally copy and distribute the retrieved images to someone unauthorized, we propose a watermark-based protocol to deter such illegal distributions. In our watermark-based protocol, a unique watermark is directly embedded into the encrypted images by the cloud server before images are sent to the query user. Hence, when an illegal image copy is found, the unlawful query user who distributed the image can be traced by the watermark extraction. The security analysis and experiments show the security and efficiency of the proposed scheme. we consider the dishonest users in an SE schemes and propose a watermark-based protocol to deter the illegal distribution of images. Overall, the image features are secure against Ciphertext- only Attack model, the image contents are secure against those plaintext Attack model, and the search efficiency is Retrieval (CBIR) has been widely studied. Compared with text documents, images consume much more storage space. Hence, its maintenance is considered to be a typical example for cloud storage outsourcing. For privacy preserving purposes, sensitive images, such as medical and personal images, need to be encrypted before outsourcing, which makes the CBIR technologies in plaintext domain to be unusable.

Title 4:

Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement

Author:

Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren

Content:

Concretely, we develop a novel method of keyword transformation and introduce the stemming algorithm. With these two techniques, the proposed scheme is able to efficiently handle more misspelling mistake. Moreover, our proposed scheme takes the keyword weight into consideration during ranking. Like Wang et al.'s scheme, our proposed scheme does not require a predefined keyword set and hence enables efficient file update too. We also give thorough security analyses and conduct experiments on real world data set, which indicates the proposed scheme's potential of practical usage. Experiments using real-world data show that our scheme is practically efficient and achieve high accuracy. The majority of the existing techniques are focusing on multi-keyword exact match or single keyword fuzzy search. However, those existing techniques find less practical significance in real-world applications compared with the multi keyword fuzzy search technique over encrypted data. The first attempt to construct such a multi-keyword fuzzy search scheme was reported by Wang et al., who used locality-sensitive hashing functions and Bloom filtering to meet the goal of multi-keyword fuzzy search. Nevertheless, Wang's scheme was only effective for a one letter mistake in keyword but was not effective for other common spelling mistakes. Moreover, Wang's scheme was vulnerable to server out-of-order problems during the ranking process and did not consider the keyword weigh

Title 5:

A Literature Survey on Secure Data Sharing in Cloud Storage with Key Aggregate Cryptosystem

Author:

Prof. B. M. Kore, Archana Jadhav, Prof. V. V. Pottigar

Content:

In this survey we studied different cryptographic techniques for data sharing

security. One trivial solution to achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the Cloud provider and other malicious users. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Thus it considers how to compress secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. Our approach is more flexible than hierarchical key assignment. One trivial solution to achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the Cloud provider and other malicious users. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Thus it considers how to compress secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. Our approach is more flexible than hierarchical key assignment. This paper reveals an overview and study of cryptographic techniques for securely and efficiently data sharing in cloud storage.

2.1 EXISTING SYSTEM

- Recent years witness the development of cloud computing technology. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development.
- The computer technology has developed rapidly. Cloud computing has gradually matured through so many people effort's.
- In current storage schema, the user's data is totally stored in cloud servers. If the user lose their right of control on data and face privacy risk.
- The privacy protection schemes are usually based on encryption technology. These kinds of methods cannot effectively resist attack from the inside of cloud server.

DISADVANTAGES:

- Changes in the understanding of risk as a result of extending the datacentre into the cloud.
- Low latency and lation awareness

2.2 PROPOSED SYSTEM

- The framework can take full of cloud storage and protect the privacy of data.
- Here the cloud computing has attracted great attention from different sector of society.
- The three layer cloud storage stores in to the three different parts of data parts If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms.

ADVANTAGES

- In our system we using a bucket concept so reduce the data wastages and reduce the process timings.
- We are using a BCH code algorithm. It's High flexible.
- BCH code are used in many communications application and low amount of redundan

CHAPTER

REQUIREMENT ANALYSIS

HARDWARE REQUIREMENTS:

System - Pentium-IV

Speed - 2.4GHZ

Hard disk-40GB

Monitor -15VGA color

RAM -512MB

SOFTWARE REQUIREMENTS:

Operating System - Windows XP

Coding language -Net

IDE - Visual Studio

Database -SQL Server

SYSTEM ARCHITECTURE

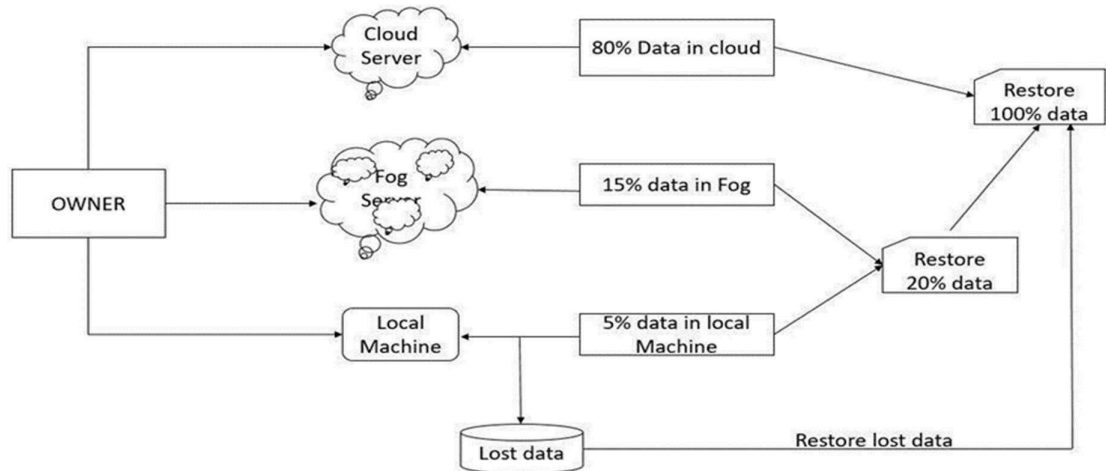


Fig.No: 3.1 System Architecture

DATA FLOW DIAGRAM

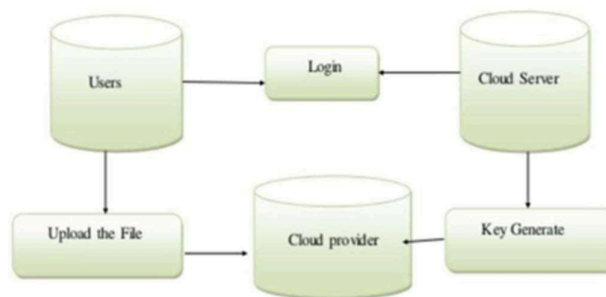


Fig.No: 3.2 Data Flow Diagram

Use Case Diagram

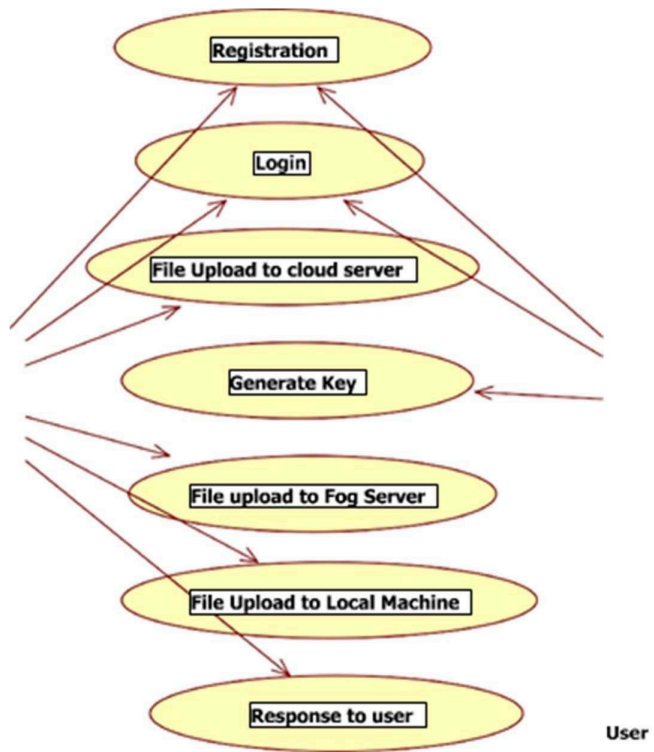


Fig.No: 3.3 Usecase Diagram

Sequence Diagram

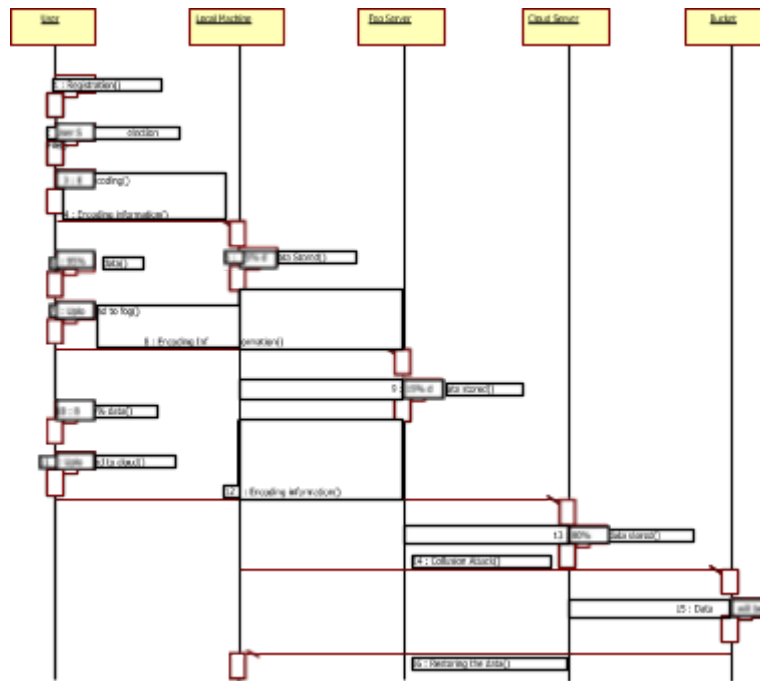
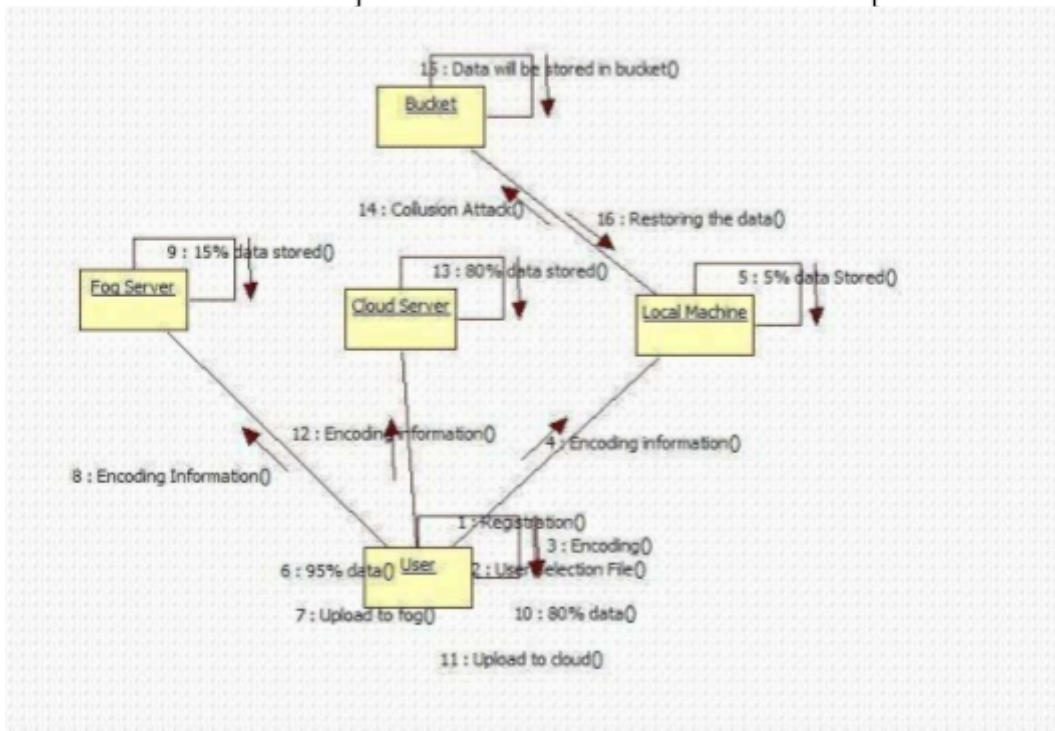
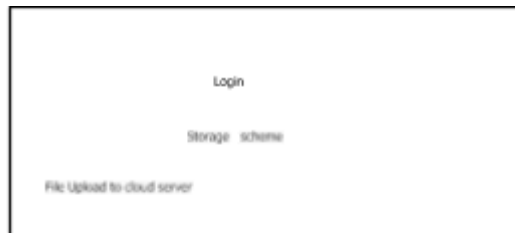


Fig.No: 3.4 Sequence Diagram

Activity Diagram



Collaboration Diagram

Fig.No: 3.5 Collaboration Diagram

CHAPTER 4

MODULES

- Login
- Registration
- Storage Scheme
- Recovery Scheme

Login Module

This is the first activity that opens when user open the website. User needs to provide a correct contact number and a password, which user enters while registering, in order to login into the website. If information provided by the user matches with the data in the database table then user successfully login into the website else message of login failed is displayed and user need to reenter correct information. A link to the register activity is also provided for registration of new users.

Registration Module

A new user who wants to access the webpage needs to register first before login. By clicking on register button in login activity, the register activity gets open. A new user registers by entering full name, password and contact number. A user needs to enter password again in confirm password text box for confirmation. When user enters the information in all text boxes, on the click of register button, the data is transferred to database and user is directed to login activity again.

Registered user then needs to login in order to access the web page. Validations are applied on all the text boxes for proper functioning of the web page. Like information in each text box is must that is each text box, either it is of name, contact, password or confirm password, will not be empty while registering. If any such text box is empty app will give message of information is must in each text box. Also data in password and confirm password fields must match for successful registration. Another validation is contact number must be valid one that is of 10 digits. If any such validation is violated then registration will be unsuccessful and then user needs to register again. Message that webpage will display when one of the field is empty. If all such information is correct user will be directed to login activity for login into the webpage.

Storage Module

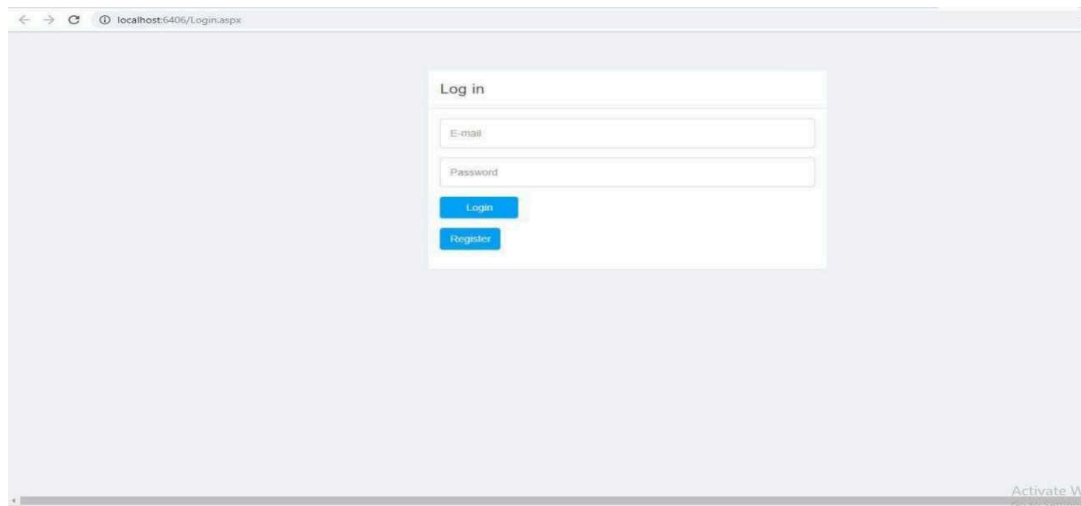
- In this module, user can store their files into three different storage server. The data owner has not control over the data after it is uploaded on cloud. In this module, the original data get encrypted into three different layer's. The data in each layer can be encrypted by using different cryptographic algorithm's and encryption key before storing them in the Cloud.

Recovery Module

In this Module, user can recover their files from three different storage server that is Cloud server, Fog server and Local machine. Here we are using Hash-Solomon code algorithm is

designed to divide data into different parts. If the one data part missing we lost the data information.

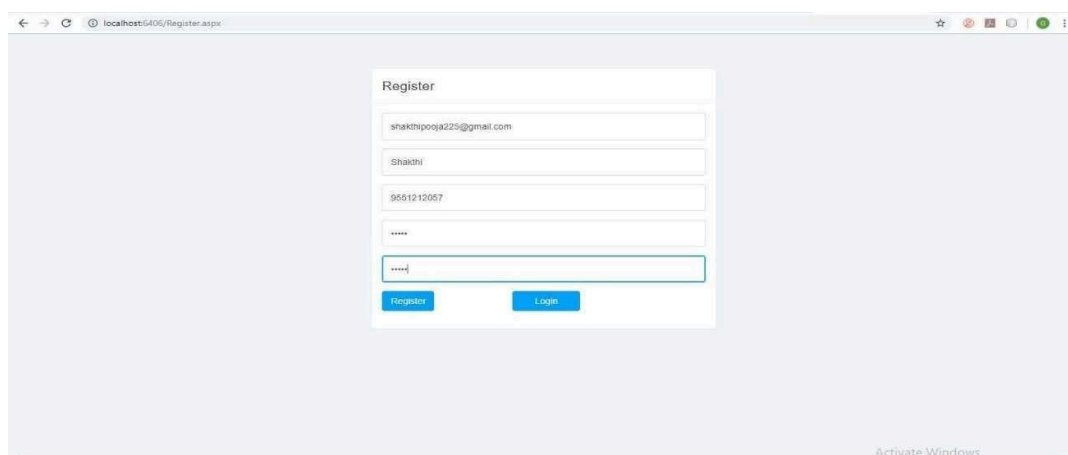
HOME PAGE



The screenshot shows a web browser window with the address bar displaying 'localhost:6406/Login.aspx'. The main content area features a 'Log in' form. The form has two input fields: 'E-mail' and 'Password'. Below these fields are two buttons: 'Login' and 'Register'. The 'Login' button is highlighted with a blue border. The background is a light gray color.

Fig.No: 4.1 Home Page

REGISTRATION PAGE



The screenshot shows a web browser window with the address bar displaying 'localhost:6406/Register.aspx'. The main content area features a 'Register' form. The form has four input fields: 'E-mail' (containing 'shakthipooja225@gmail.com'), 'Username' (containing 'Shakthi'), 'Password' (containing '9551212057'), and 'Confirm Password' (containing '****'). Below these fields are two buttons: 'Register' and 'Login'. The 'Register' button is highlighted with a blue border. The background is a light gray color.

Fig.No: 4.2 Reegistration Pag

LOGIN PAGE

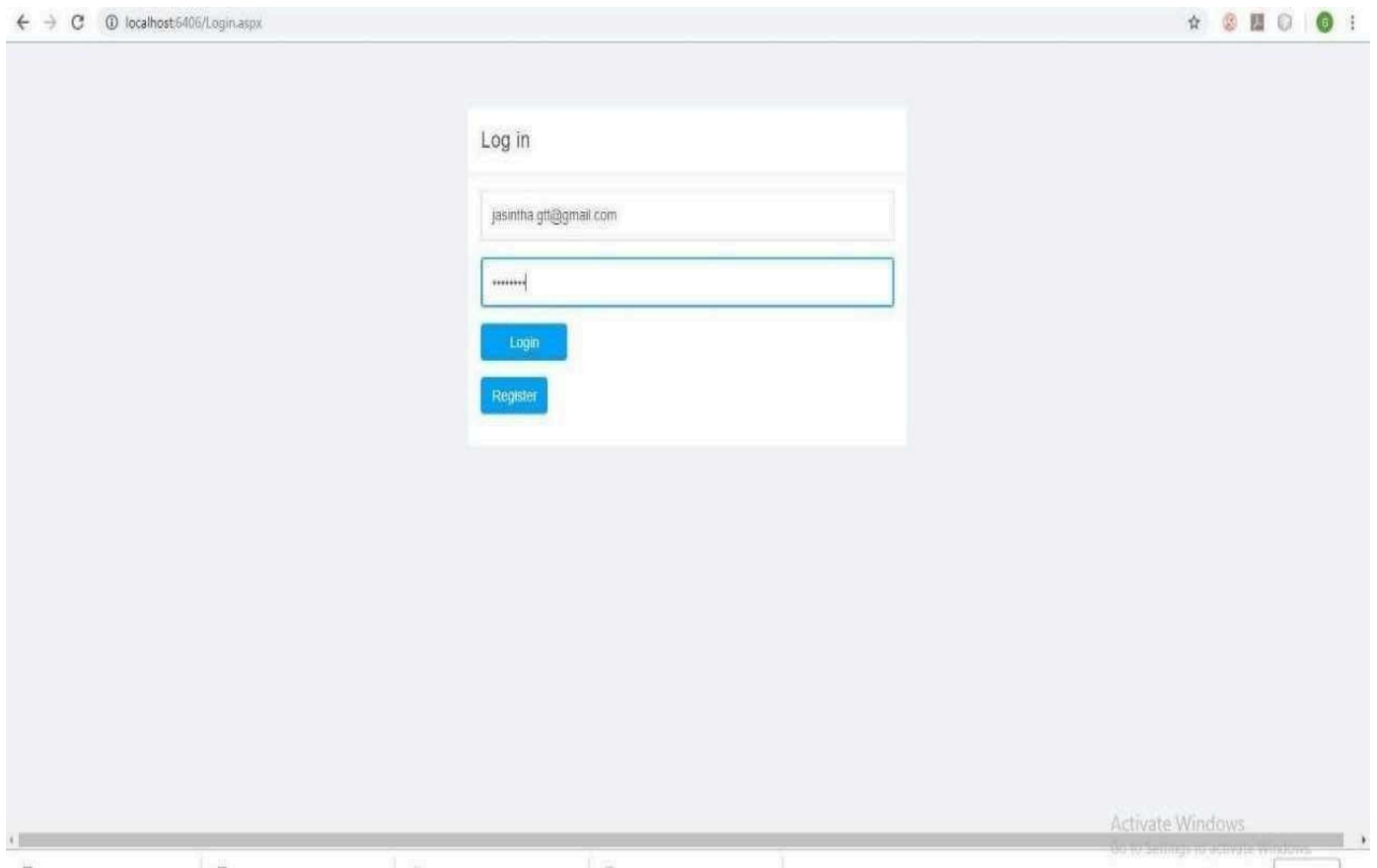


Fig.No: 4.3 Login Page

REFERENCES:-

[1]

P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50-50, 2009.

[2]

H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587-1611, 2013.

[3]

J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined

network (sdn) and cloud computing environments," in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969-2974.

[4]

H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397-1409, 2014.

[5]

Y. Li, T. Wang, G. Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130-143.

