International Journal of Innovations & Research Analysis (IJIRA)
ISSN :2583-0295, Impact Factor: 5.449, Volume 03, No. 01(I), January- March, 2023, pp 142-152

SECURE DATA SHARING SYSTEM USING CLOUD

Mr. Aakash Sahay*
Mr. Dhanush S**
Dr. G Sandhya Madhuri***

ABSTRACT

Now-a-days a lot of information is passing by internet. Hence the security of information has become an essential issue. Cryptography is the well-known practice to secure data over network. Steganography is a technique used to hide the message in digital media. The elliptical curve cryptography is more secure than the current cryptography models. Securing data encryption and decryption using Cryptography and Steganography techniques. Due to recent developments in stego analysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using stego analysis, one can easily reveal existence of hidden information in carrier files. This project introduces a novel steganographic approach for communication between two private parties. The approach introduced in this project makes use of both steganographic as well as cryptographic techniques. In Cryptography we are using RSA. In Steganography we are using Image Steganography for hiding the data. And we also use Mutual Authentication process to satisfy all services in Cryptography i.e., Access Control, Confidentiality, Integrity, Authentication. In this way we can maintain the data more securely. Since we use RSA algorithm for securing the data and again on this we perform Steganography to hide the data in an image. Such that any other person in the network cannot access the data present in the network. Only the sender and receiver can retrieve the message from the data.

Keywords: *Cryptography, Cloud Computing, Data Sharing.*

Introduction

There has been a rapid progress in Cloud Computing. Cloud Computing delivers a wide range of resources like computational power, computational platforms, storage and applications to users via internet. The major Cloud providers in the current market segment are Amazon, Google, IBM, Microsoft, Salesforce, etc,. With an increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user.

Below, we have described the two main states that hold your data is out in the Cloud: when the data is in motion (transit) and when the data is at rest, where the data is much expected to be more secure. The below illustrated are the two main scenarios which we have focused to understand the security of the data in the Cloud.

Regarding this area of study, most of the research papers followed a normal traditional literature survey method. Few papers gave an innovative idea and proposed a security model. However, there are very few works, which considered the opinions of various security experts in Cloud Computing. This study proposes that, reader gets the true reflection of the security practices followed by various Cloud Computing companies in the current era. There are very few papers which focus on the security techniques for specified applications. Our work provides more knowledge in this dimension and also predicts the future threats likely to be faced by Cloud Computing and solutions to these threats.

[*] MCA, Department of Computer Applications, Dayananda Sagar University, Bangalore, India.
[**] MCA, Department of Computer Applications, Dayananda Sagar University, Bangalore, India.
[***] Assistant Professor, Department of Computer Applications, Dayananda Sagar University, India.

Objectives

The main aim of this research work is to identify and understand the security issues which affect the performance of Cloud Computing. Also, to understand the security techniques which are being used to mitigate these security issues. Thereby providing the standard guidelines for the Cloud service providers and as well as Cloud users.

The main objectives of this research are:

- To understand the security issues and to identify the appropriate security techniques those are being used in the current world of Cloud Computing.
- To identify the security challenges those are expected in the future of Cloud Computing.
- To suggest some counter measures for the future challenges to be faced in Cloud Computing.

Existing System

The SecureDBaaS architecture is tailored to cloud platforms and does not introduce any intermediary proxy or broker server between the client and the cloud provider. SecureDBaaS relates more closely to works using encryption to protect data managed by UN trusted databases. In such a case, a main issue to address is that cryptographic techniques cannot be natively applied to standard DBaaS.

- **Disadvantages of Existing system**
    - Even though they using secure DBaaS means Distributing data among different secure but its functions cannot be taking advantage of secret sharing outsourced to an un trusted cloud provider. providers and it give more
    - It cannot Store them in encrypted format.
    - When considering scenarios where multiple clients can access the same database concurrently.

Proposed System

The Secure Data Sharing in Clouds (SDSC) methodology that provides: data confidentiality and integrity; access control; data sharing (forwarding) without using compute-intensive re encryption; insider threat security; and forward and backward access control. The SDSC methodology encrypts a file with a single encryption key

In the future, work continued in several directions. First is great comparisons needed between revocation schemes proposed for attribute-based encryption to understand better and improve the performance in various circumstances.

- **Advantages of Proposed System**
    - To improve good Quality of Service (QoS).
    - Distributing data among different providers and taking advantage of secret sharing.
    - Every user having the own master key
    - Better Accessibility

Literature Survey

Title: Character Based Encryption and Decryption using Modulo Arithmetic - Amrita Sahu

For the encryption and decryption of images, a few researchers suggested a new key generation algorithm based on palm prints. With the help of our system, two parties can communicate securely over an open network, even if many people are listening in. This system offers trustworthy security.The key characteristics of the suggested asymmetric picture encryption system can be summed up as follows:

- Image lossless encryption.
- Less complicated computations.
- Convenient realization is .
- Selecting an appropriate matrix size based on the size of the image.
- Integer arithmetic and logic operations are used in the encryption/decryption system.

Title: A Novel Approach of Image Encryption and Decryption by Using Partition and Scanning Pattern - Monisha Sharma

This method's ability to satisfy the principles of Confusion and Diffusion, as well as the fact that a correct guess of the encryption key renders decryption impossible. This encryption is simple to implement in hardware and simply needs integer arithmetic. This is a novel technique for encrypting images, in which the pixels in the image are rearranged according to a basic, predetermined pattern. This study examines.

Currently used partitioning and scanning patterns that are connected to scan methodology are used for image encryption and decryption. Spatial accessing approach, on which the SCAN language is built, may produce a variety of scanning pathways. In this study, an overview of the encryption and decryption algorithms is presented. The algorithms are implemented in the MATLAB environment and tested on a variety of photos. Index Terms: Scanning, Partitioning, Decryption, and Image.

Title: Security Model for Preserving Privacy over Encrypted Cloud Computing - Kamara, S. and Lauter, K.

The privacy and security of data are currently the most essential concerns for any data owner, especially when private data is outsourced to a publicly accessible cloud server in an area that is not widely recognised as being trustworthy. In order to prevent information leaks or disclosure, we shall encrypt any sensitive or private data before uploading it to the server.

In comparison to the findings of earlier studies in terms of accuracy, privacy, security, key generation, storage capacity as well as trapdoor, index generation, index encryption, index update, and finally files retrieval depending on access frequency, we will propose a new model called Secure Model for Preserving Privacy Over Encrypted Cloud Computing (SPEC).

The pixels in the image are rearranged in accordance with a fundamental, preset pattern in this unique method of image encryption. This research investigates

System Study & Design

Feasibility Study

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

Three key considerations involved in the feasibility analysis are :

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

Let us see about each feasibility in detail:

- **Economic Feasibility**

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus, the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

- **Technical Feasibility**

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

- **Social Feasibility**

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

System Design

Modules

- **Data Owner**

It is responsible to generate and encrypt the shared data, define access structures, and divide encrypted data into blocks. It is responsible to generate and encrypt the shared data, define access structures, and divide encrypted data into blocks

It is responsible to generate and encrypt the shared data, define access structures, and divide encrypted data into blocks. This module helps the owner to register those details and also include login details. This module helps the owner to upload his file with encryption using RSA algorithm

- **User Login**

It is responsible to download and decrypt the shared data for utilization. In the scheme only the authorized DR is able to download shared data from CSS and decrypt the data. This module includes the user registration login details. This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query.

- **Cloud Server**

Cloud servers comes in Cloud Storage Servers (CSS) and Cloud Manage Servers (CMS) based on their roles. CSS is responsible for storing shared data, block tags and supply the data integrity proof.

- **Steganography**

Steganography is the practice of hiding a secret message inside of (or even on top of) something that is not secret.

System Architecture

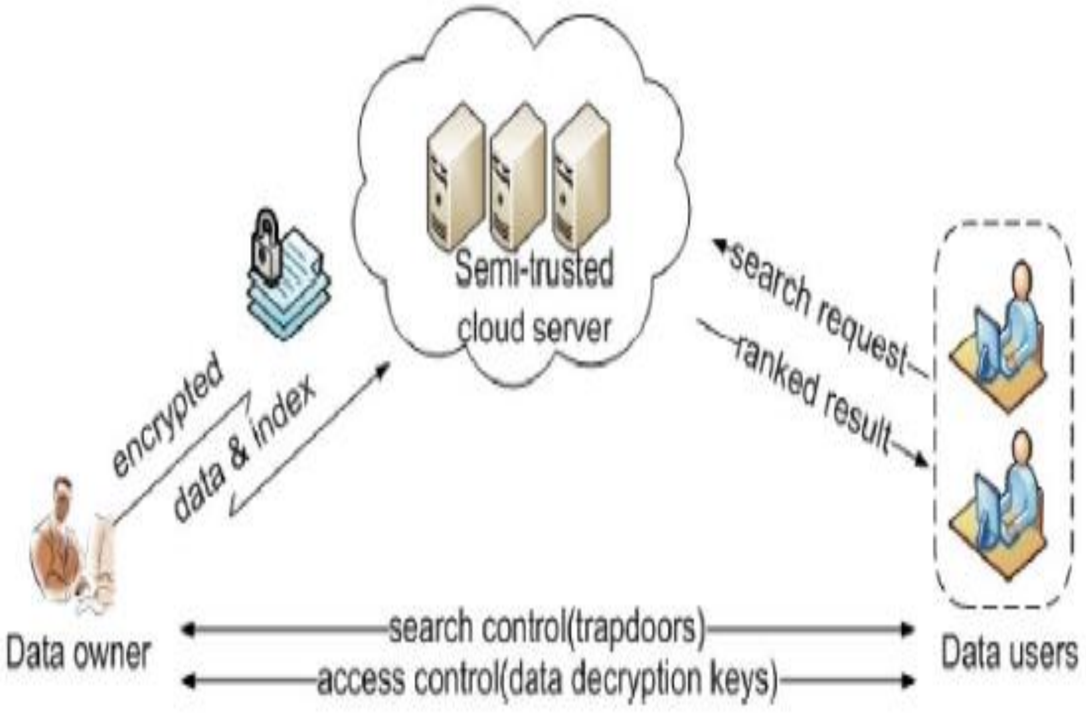


Fig. 1: System Architecture

Data Flow Diagram

- The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
- The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
- 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 detail.

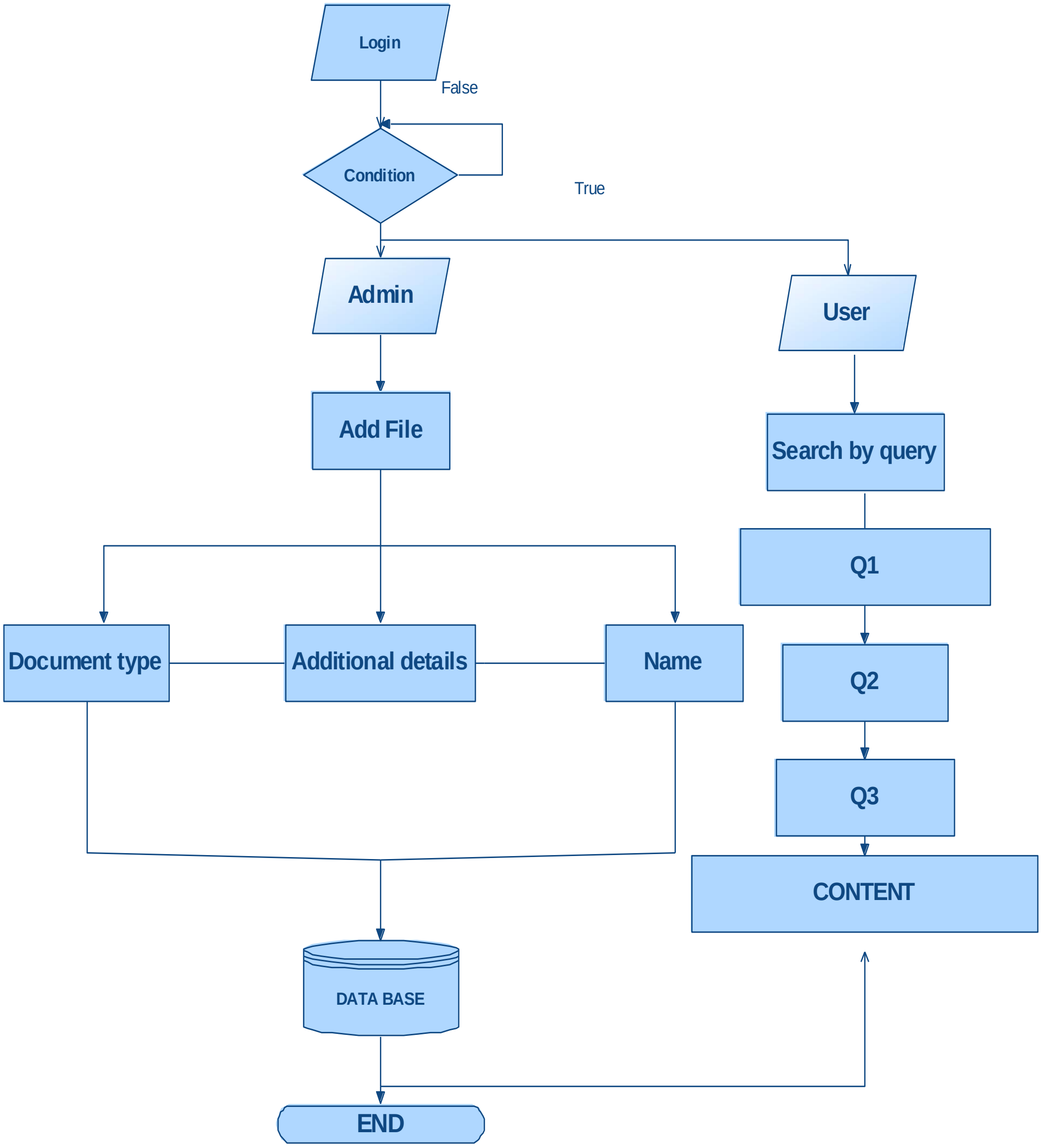


Fig. 2: Data Flow Diagram

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.

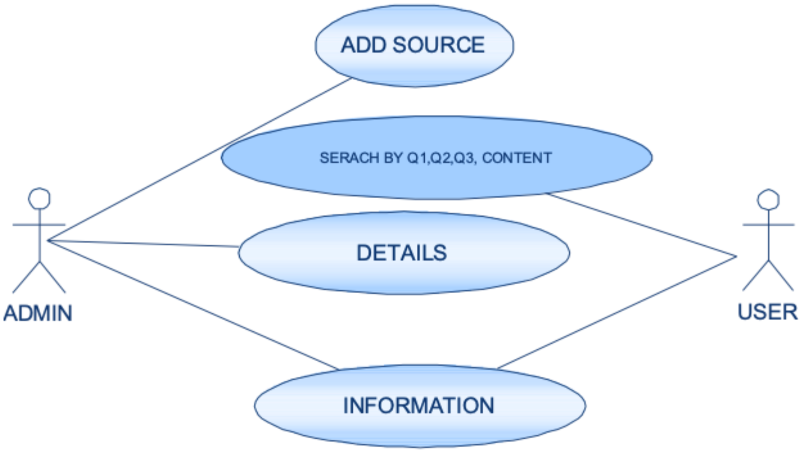


Fig. 3: Use Case Diagram

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.

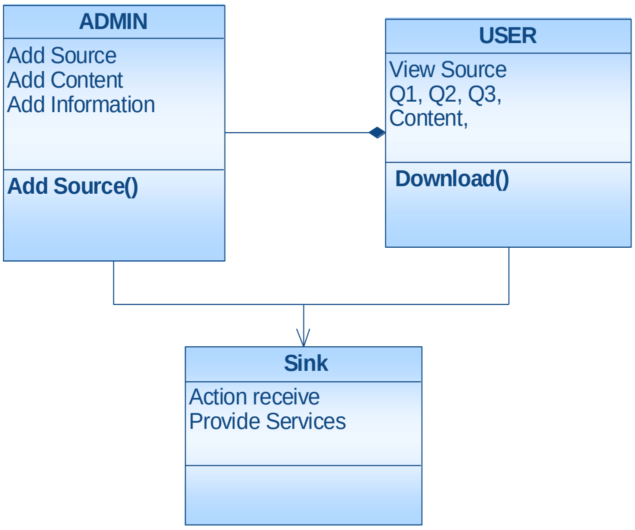


Fig. 4: Class Diagram

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.

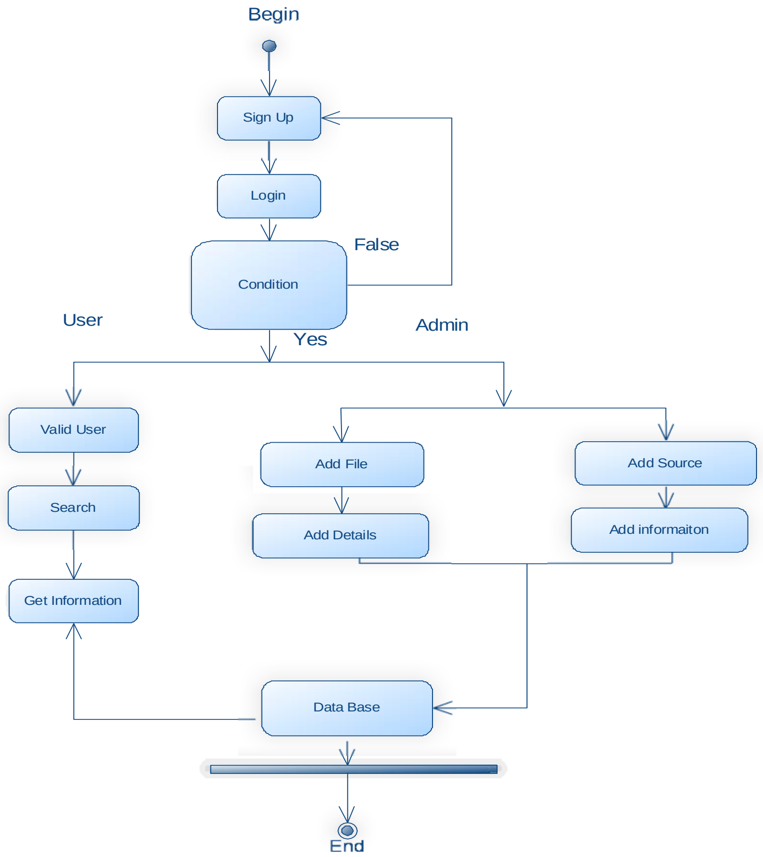


Fig. 5: Activity Diagram

Database Tables

The following are the database tables used in the system:

Fieldname	Datatype
Name	nvarchar(50)
Pass	varchar(50)
Email	varchar(50)
DOB	Date
Gender	varchar(50)
Role	varchar(50)
Loc	varchar(50)
Skey	varchar(50)
Pno	varchar(50)

Field Name	Data Type
File	nvarchar(50)
Keyword	varchar(50)
Filetype	varchar(50)
Filename	nvarchar(50)
CDate	Date
Owner	varchar(50)
Size	varchar(50)
Data	varchar(50)
Frank	varchar(50)
File_key	varchar(50)

Field Name	Data Type
Fname	nvarchar(50)
Keyword	varchar(50)
Uname	nvarchar(50)
Owner	varchar(50)
Status	varchar(10)
Dkey	varchar(10)

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.

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.

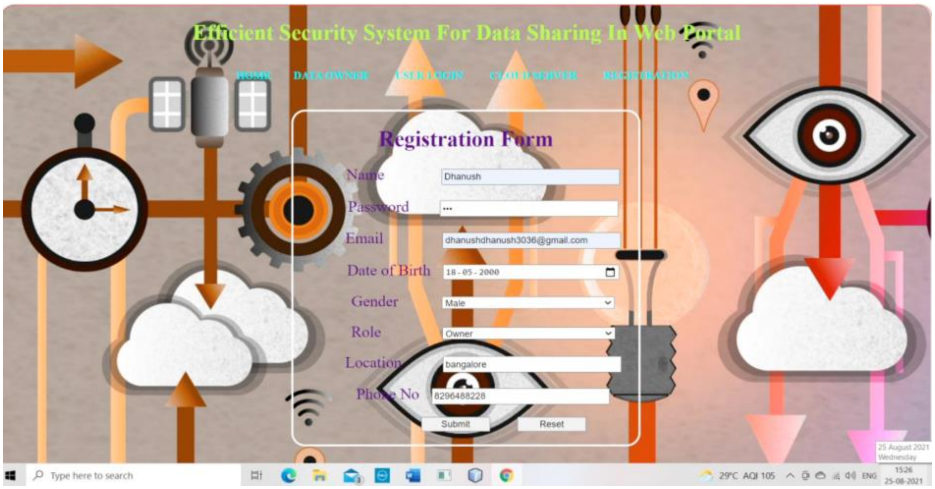
Features to be Tested

- 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.

Test Cases

Testcase Number	Testing Scenario	Expected result	Result
	Registration Testing		
TC – 01	Clicking submit without entering details	Alert "Enter the name, it cannot be empty"	Pass
TC – 02	Clicking submit without entering Name	Alert "Enter the name, it cannot be empty"	Pass
TC – 03	Clicking submit without entering password	Alert "Please fill Password"	Pass
TC – 04	Clicking submit without entering email id	Alert "Please fill email id"	Pass
TC – 05	Clicking submit without entering phone number	Alert "Please fill contact number"	Pass
	Login Testing		
TC – 06	Clicking submit without entering login details	Alert "Please enter the username and password"	Pass
TC – 07	Clicking submit without entering password	Alert "Please enter the password"	Pass

Implementation

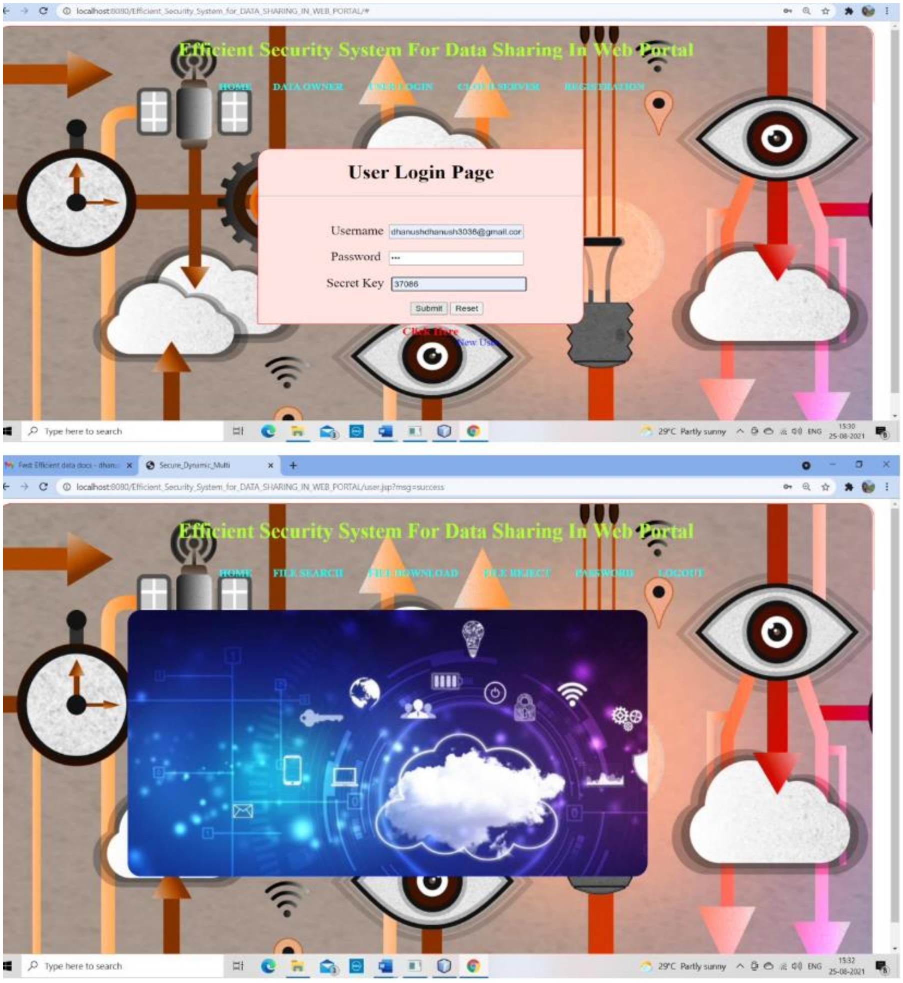


Efficient Security System For Data Sharing In Web Portal

Registration Form

Name: Dhanush
Password: •••
Email: dhanushdhanush3036@gmail.com
Date of Birth: 18-05-2000
Gender: Male
Role: Owner
Location: bangalore
Phone No: 8296488228

Fig. 6: Sample output - 1



localhost:8080/Efficient_Security_System_for_DATA_SHARING_IN_WEB_PORTAL/#

Efficient Security System For Data Sharing In Web Portal

User Login Page

Username: dhanushdhanush3036@gmail.cor
Password: •••
Secret Key: 37086

localhost:8080/Efficient_Security_System_for_DATA_SHARING_IN_WEB_PORTAL/user.jsp?msg=success

Efficient Security System For Data Sharing In Web Portal

Fig. 7: Sample Output – 2

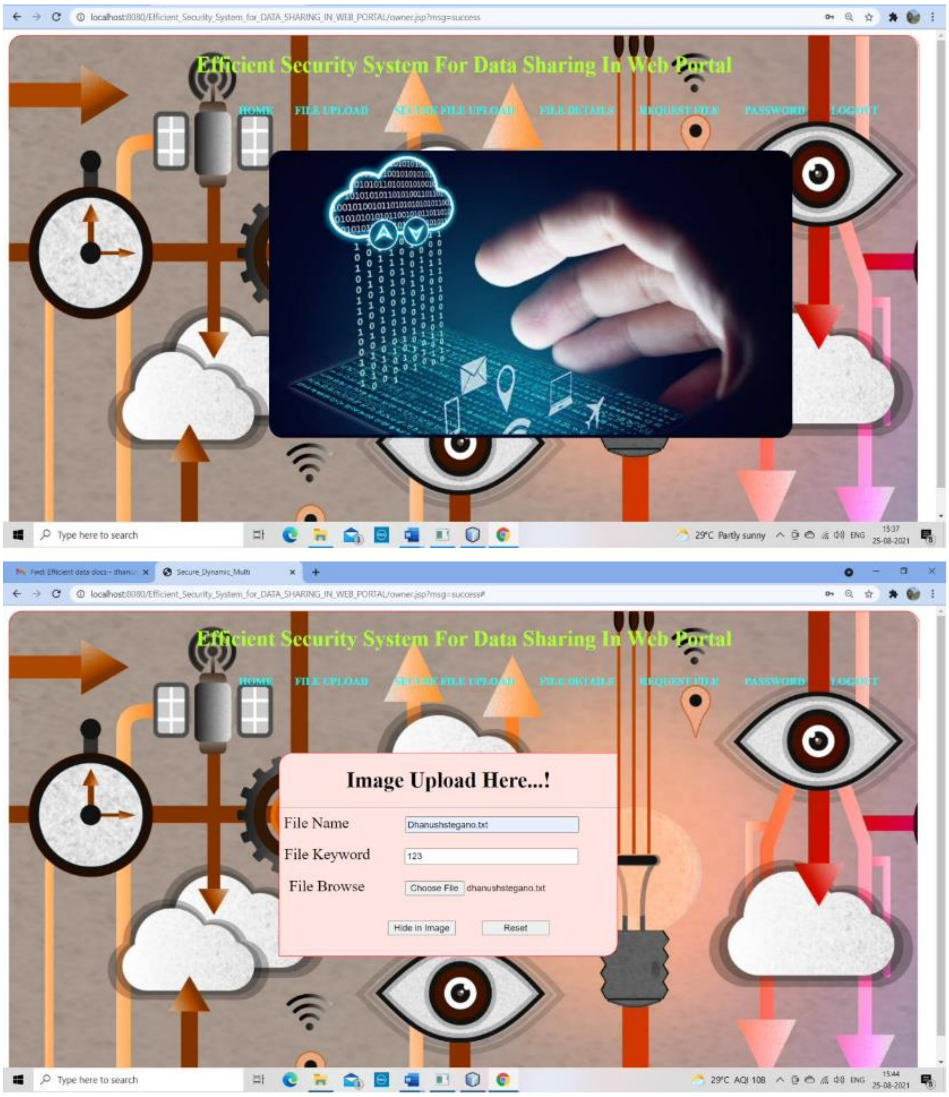

localhost:8080/Efficient_Security_System_for_DATA_SHARING_IN_WEB_PORTAL/owner.jsp?msg=success
Efficient Security System For Data Sharing In Web Portal
HOME
FILE UPLOAD
SECURE FILE UPLOAD
FILE DETAILS
REQUEST FILE
PASSWORD
LOGOUT
Type here to search
localhost:8080/Efficient_Security_System_for_DATA_SHARING_IN_WEB_PORTAL/owner.jsp?msg=success#

Image Upload Here...!

File Name: Dhanushstegano.txt

File Keyword: 123

File Browse: Choose File dhanushstegano.txt

Hide in Image | Reset

Fig. 8: Sample output – 2

Conclusion

Augmented Reality kits are available over the internet to download for companies and individual users to have simpler access to the technology. By all this we cannot conclude that a steep inclination is possible in AR technology. The major challenge of AR is the software compatibility and less support for integration.

Augmented Reality in simpler terms is increasing the reality of actual objects which we see using our eyes or devices like smartphones. The answer to the question on how is it so popular or trending is that it can impactfully offer a remarkable experience either of learning, measuring the three-dimensional surfaces, or studying the medical statistics of crisis situations comprising of the greatest complications.

References

1. Lo, ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari, “A Secure Cloud Computing Model Based on Data Classification”, Elsevier Procedia Computer Science, vol. 52, pp. 1153-1158, 2015.

2. Elli Kartsakli, Angelos Antonopoulos, Aris S. Lalos, Stefano Tennina, Marco Di Renzo, Luis Alonso and Christos Verikoukis, “Reliable MAC Design for Ambient Assisted Living: Moving the Coordination to the Cloud”, IEEE Communications Magazine, vol. 53, no. 1, pp. 78-86, 2015.

3. Yongdae Kim, Adrian Perrig and Gene Tsudik, “Group Key Agreement Efficient in Communication”, IEEE Transactions on Computers, vol. 53, no. 7, pp. 905-921, July 2004.

4. Anita Kanavalli, P Deepa Shenoy, Venugopal K R, L M Patnaik, A Flat Routing Protocol in Sensor Networks, International Conference on Methods and Models in Computer Science, New Delhi, ISBN: 978-14244-5051-0, pp. 1-5, December 1416, 2009.

5. Arshdeep Bahga and Vijay K. Madisetti, “Analyzing Massive Machine Maintenance Data in a Computing Cloud”, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1831- 1843, October 2012.

6. P.Krithika, G.Linga Dilipan and M.Shobana, “Enhancing Cloud Computing Security for Data Sharing within Group Members”, IOSR Journal of Computer Engineering (IOSR-JCE), vol. 17, no. 2, pp. 110- 114, Ver. V, MarApr. 2015.

□❍□