Accessing cloud data with time constraint and conjunctive keyword for e-health

*Mokshada Birari, Ninad Katkar, Namrata Dhumal, Aparna Bamane, Prof. Harsha Bhute
1,2,3,4Sinhgad College of Engineering, Pune

Abstract:
An Electronic Health Record(HER) system is very important in healthcare sector to store the patient data in a secure form its like an application. The privacy of the data is the main problem from user side which can stop or effect other development or system. The searchable encryption system is the technology which can be useful for security protection and operability functions together, which can be useful in e-health record system. In this paper, we are introducing a conjunctive keyword search approach for the development, it a cryptographic technique. We applied designated tester and timing enabled proxy-reencryption technique. Which is time dependent. It can give a patient partial access right to operate search function with time limit. The time period for a user to search can decrypt the encrypted data can be controlled. The delegate or user can be automatically cancelled from the access and search authority after a specified period of time. It can also support the conjunctive keyword search to avoid the attacks on data, in that only a designated tester is used to find the existence of the keywords. We developed a system model and a security model for the proposed timing enabled proxy-reencryption scheme to show that it is an efficient scheme proved secure in the standard model. The comparison and extensive simulations demonstrate that it has a low computation and storage overhead.

Keywords: *Searchable encryption, time control, conjunctive keywords, designated tester, e-health, resist offline keyword guessing attack.*

Introduction:

The main objective is that Cloud computing offers a new way of service provision by re-arranging various resources over the Internet. The most important and popular cloud service is data storage. In order to preserve the privacy of data Users, data are often stored in cloud in an encrypted form. However, encrypted data gives new challenges for cloud data Storage services, which is hard for big data storage and processing the data on cloud. Here we are searching for the keyword and we will get the data which contain that word. So we are encrypting the data saved on cloud. To maintain the privacy References.

Problem Definition:

In this project we are using cloud computing for storage. In the recent years storage is a biggest issue in a organizations, so to secure the data and get at any time we use cloud. We are applying encryption to the data to

avoid the security issue. And in this we are assigning time to the designated tester in conjunctive keyword search.

Objectives

We can use this project in hospital system to save data confidentially on cloud. In Hospital there is a need0 to save data confidentially. So here the patient can get the require data by searching the keyword.

System design:

Data Flow Diagram 0:

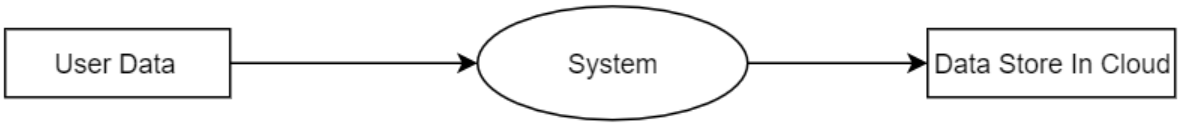


Fig 1.Data Flow Diagram 0

Data Flow Diagram 1:

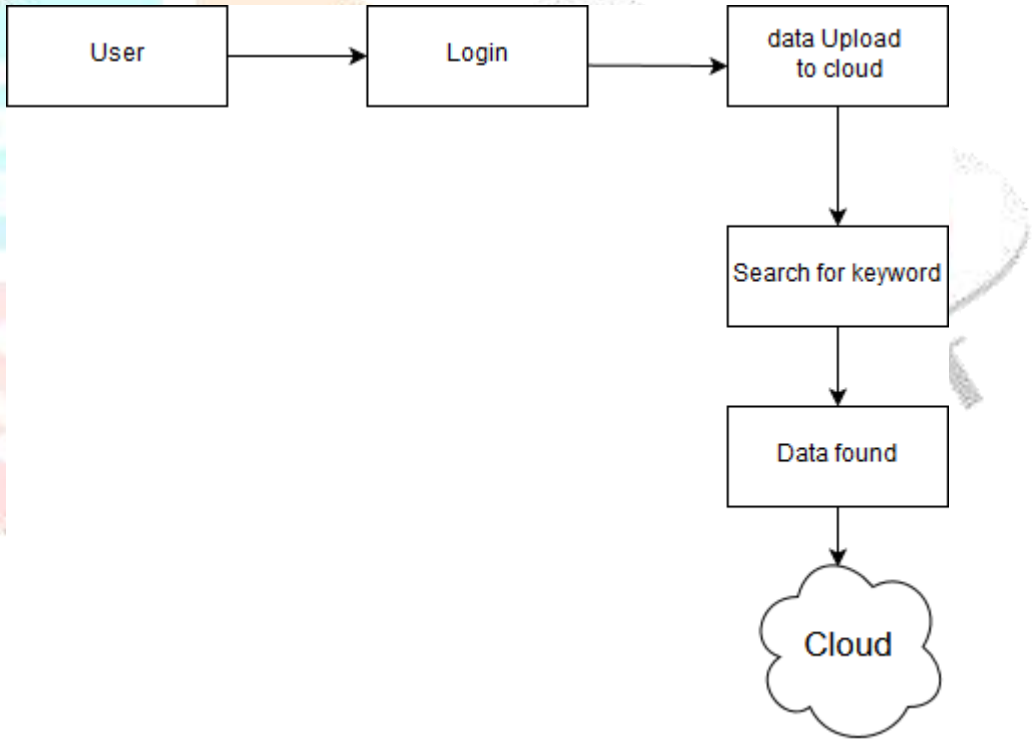


Fig 2.Data Flow Diagram 1

Data Flow diagram 2:

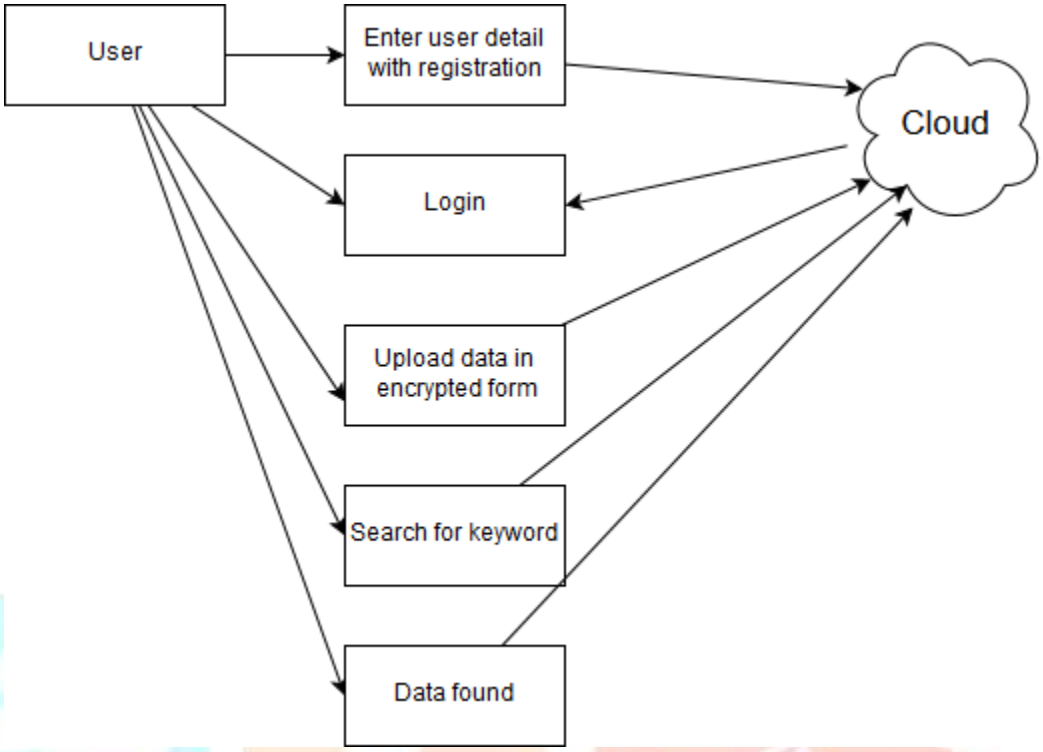


Fig 3.Data Flow Diagram 2

ER Diagram:

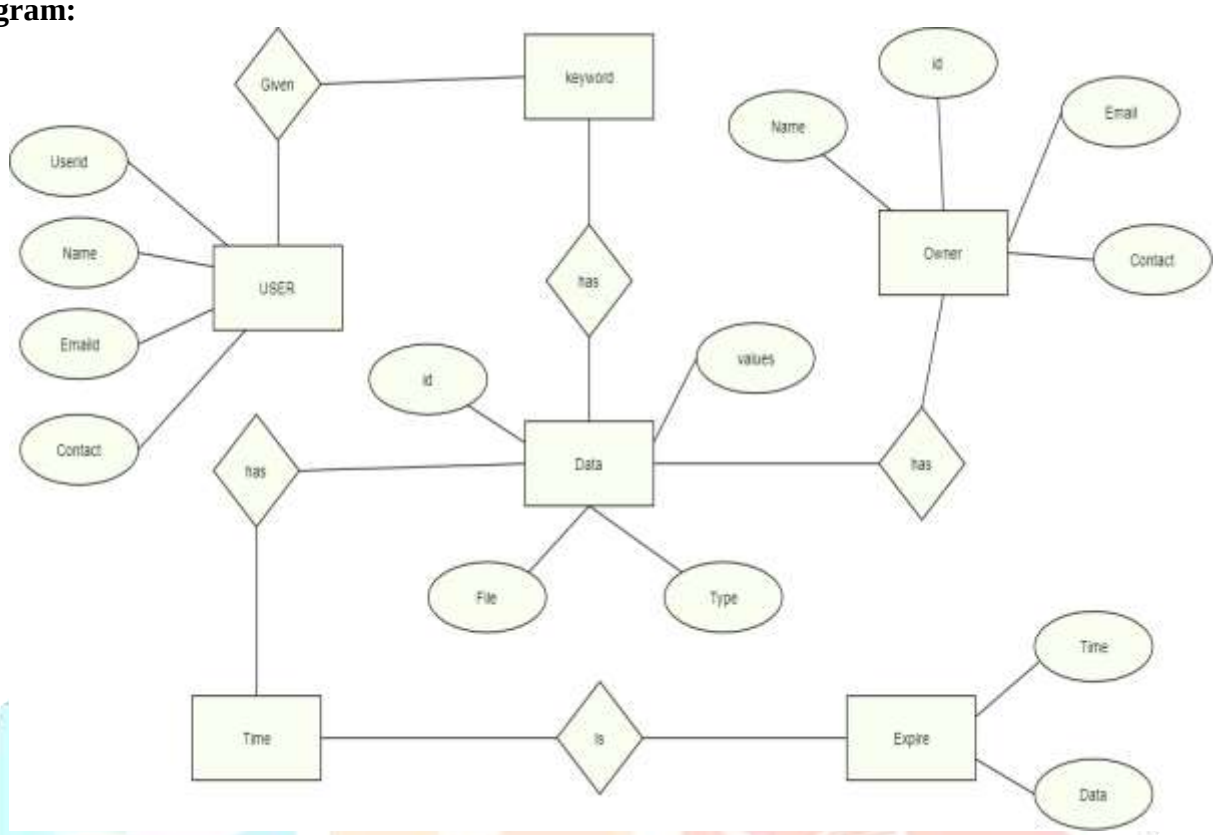
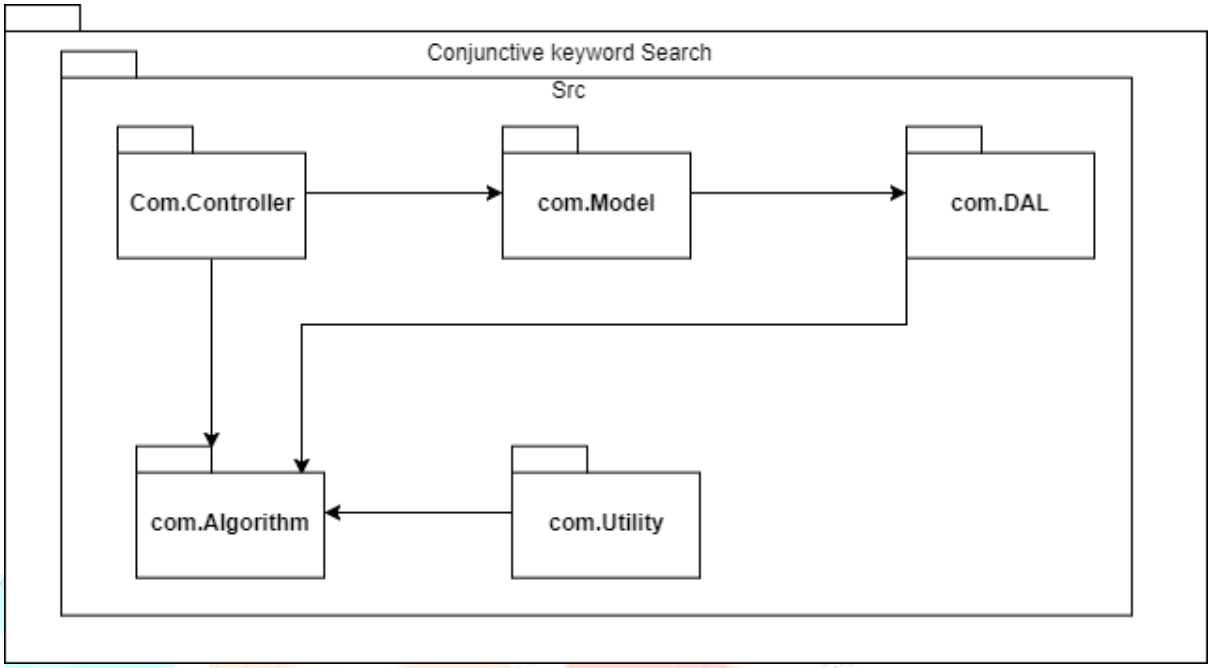


Fig ER Diagram

Package diagram:



Class Diagram:

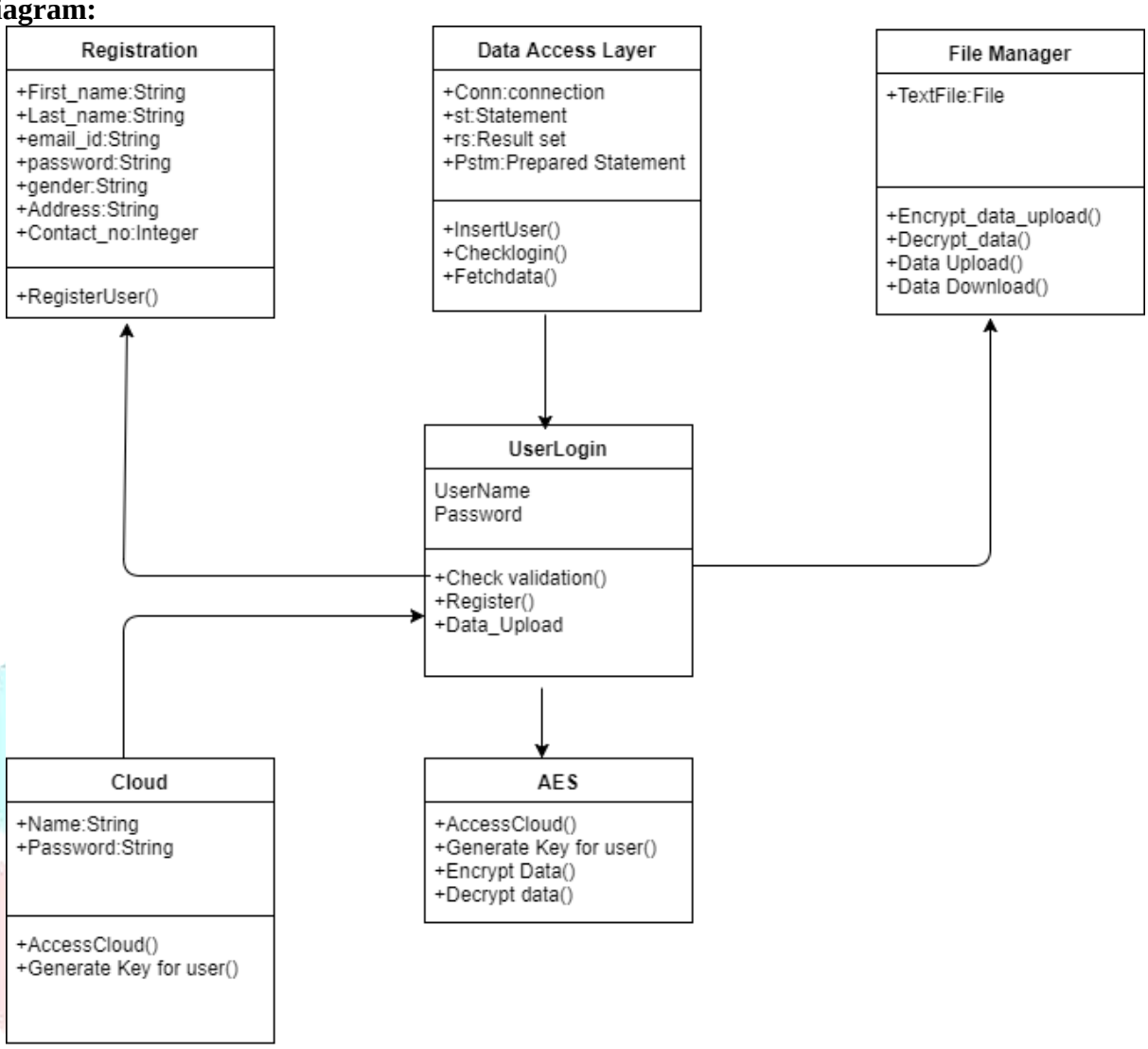


Fig Class Diagram

Sequence Diagram:

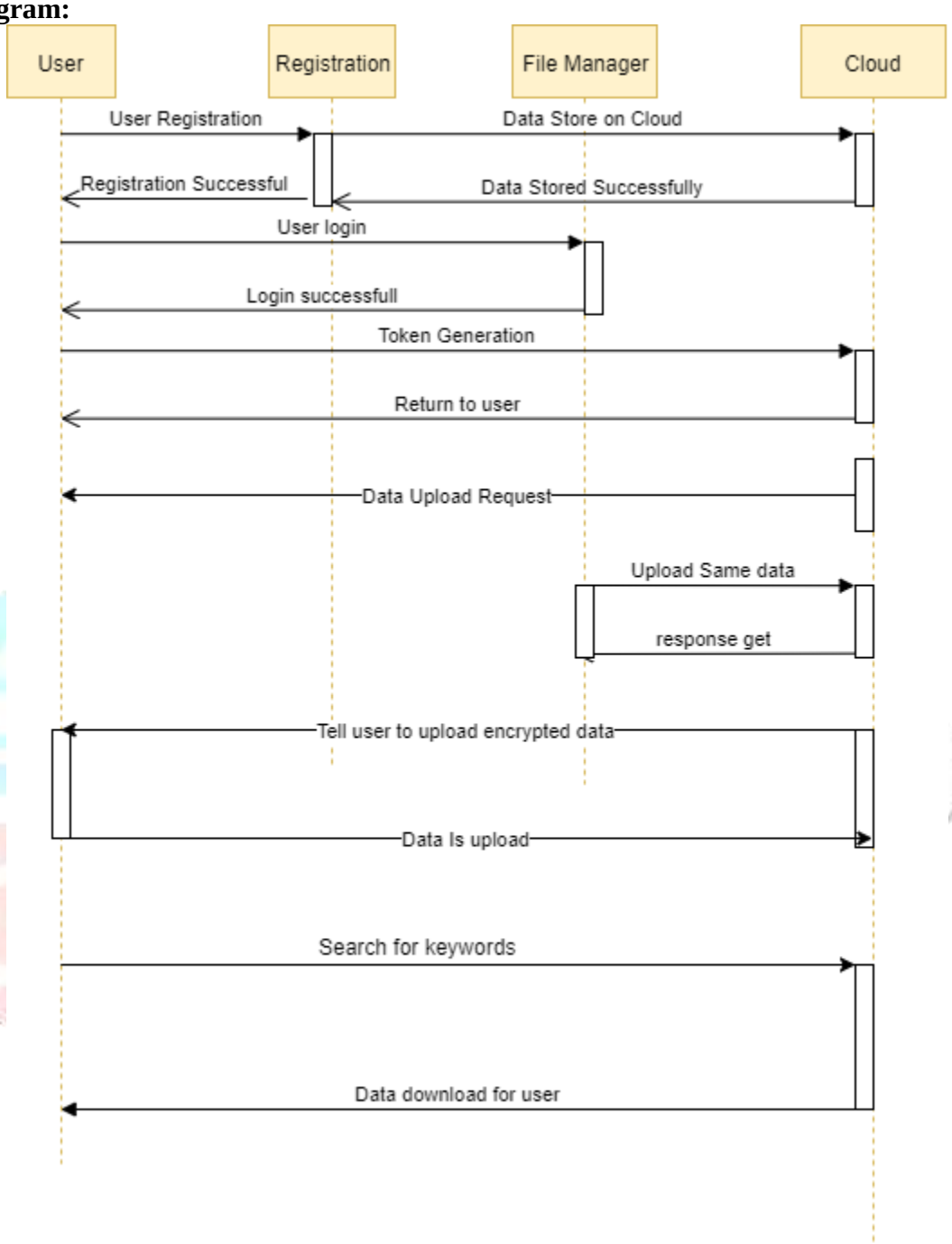


Fig. Sequence Diagram

Activity Diagram:

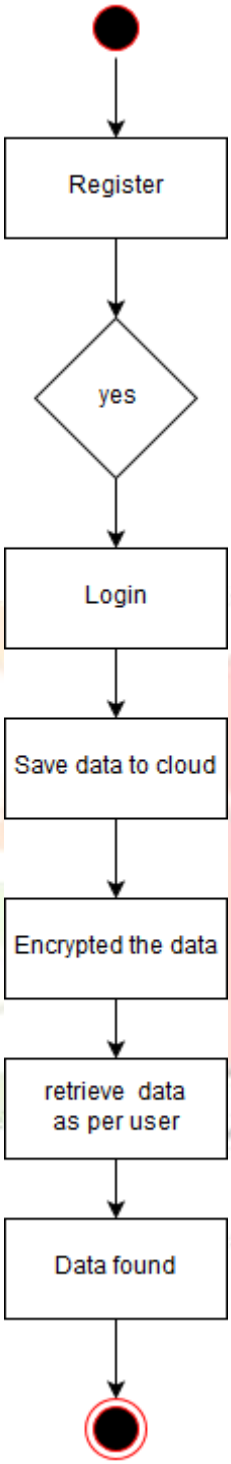


Fig. Activity Diagram

System Architecture

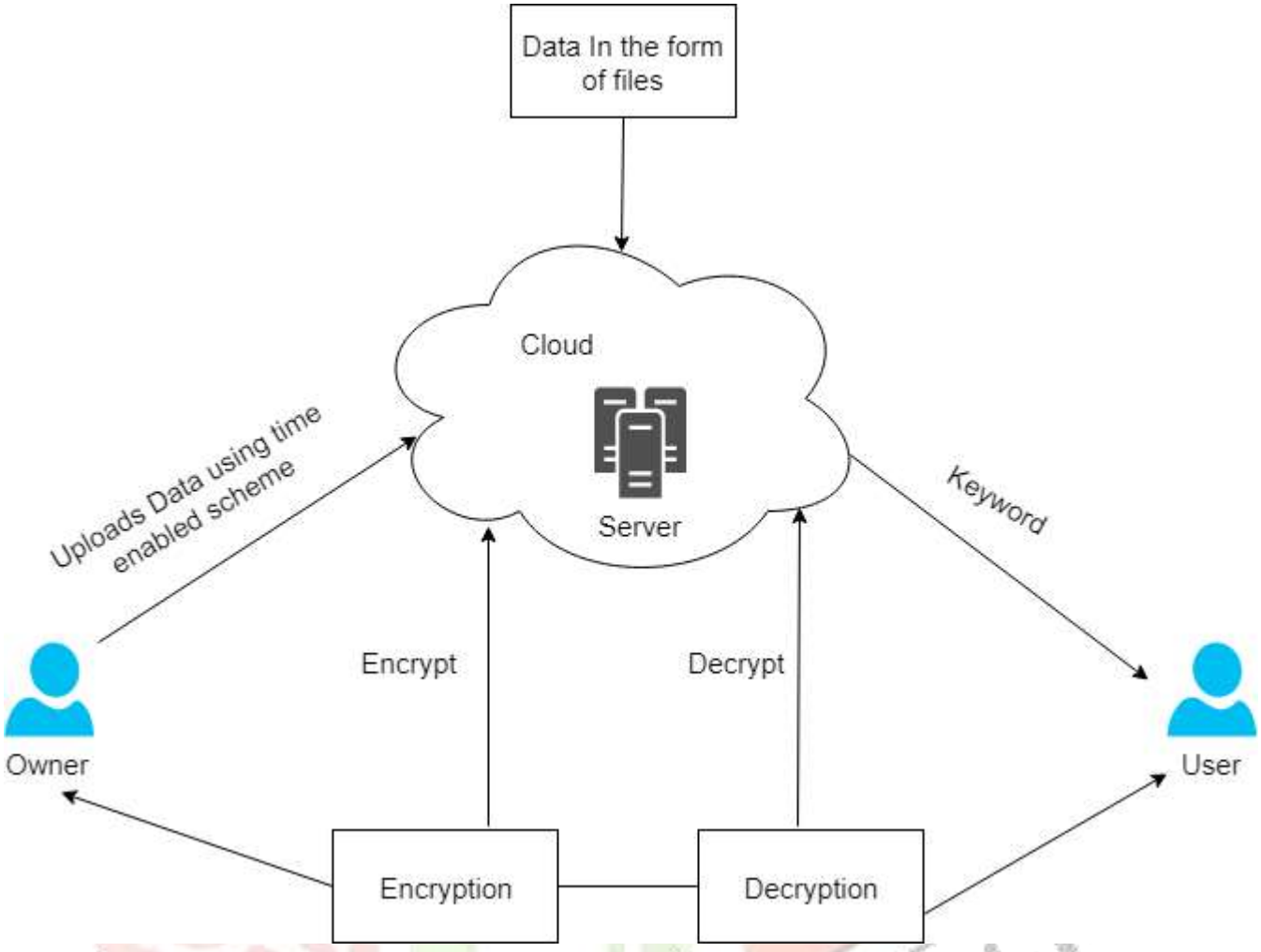


Fig 1: System Overview

In the above system overview the data is uploaded by the data owner. Here time enabled and conjunctive keyword technique is used. Owner will upload the data with timing enabled proxy reencryption. In that your access to the file will be limited to particular time. User will get the conjunctive keyword on his/her email id. Only then user can get the access to the file in that while uploading the file we are performing encryption and downloading we are performing decryption.

Related Works

1) Efficient Verifiable Public Key Encryption with Keyword Search Based on KPABE :

Year: 2014

Author Name:

- P. Liu,

- J. Wang,
- H. Ma,
- H. Nie,

Description: This paper propose a new scheme which "removes secure channel" and construct a novel method for verifying the searched result from the cloud server based on key policy attribute-based keyword search(KP-ABKS) of VABKS. It can be effectively to verify the correctness and integrity of the data file which the data user desired for.

Limitations: How to search the encrypted data without decrypting them is the issue.

2) Designing a system for patients controlling providers' access to their electronic health records: organizational and technical challenges:

Year: 2015

Author Name:

- J. Leventhal, J.
- Cummins,
- P. Schwartz,
- D. Martin,
- W. Tierney.

Description: This paper describe the technical and organizational challenges faced in capturing patients preferences for patient-controlled EHR access and applying those preferences to an existing HER.

Limitations: To apply fair information is risky

3) Public key encryption schemes supporting equality test with authorization of different granularity :

Year: 2012

Author Name:

- Q. Tang

Description: This paper extend work about public key encryption schemes supporting fine-grained authorization (FG-PKEET), it correct some flaws) and discuss how to extend the proposed cryptosystem to support approximate equality test.

Limitations: Lacks in security.

4) Proxy Re-encryption with Keyword Search: New Definitions and Algorithms :

Year: 2012

Author Name:

- W. Yau
- R. Phan
- S. Heng
- B. Goi,.

Description: This paper introduce a new cryptographic primitive, called proxy re-encryption with keyword search, In this paper, a concrete construction is proposed, which is proven secure in the random oracle model, based on the modified Decisional Bilinear Diffie–Hellman assumption

Limitations: Since the resulting scheme is no longer proven secure in our security model.

5) An Uninstantiable Random-oracle-model Scheme for a Hybrid encryption Problem :

Year: 2010

Author Name:

- M. Bellare
- Boldyreva
- Palacio

Description: This paper presents a deduplication storage system over cloud computing. Our deduplication storage system consists of two major components, a front-end deduplication application and Hadoop Distributed File System.

Limitations: Issue of whether such schemes can be securely instantiated, and, if so, how, remains less clear.

6) Off-line key-word guessing attacks on recent keyword search schemes over encrypted data :

Year: 2014

Author Name:

- J. Byun
- H. Rhee
- H. Park
- D. Lee

Description: This system presents keyword search scheme over encrypted documents allows for remote keyword search of documents by a user in possession of a trapdoor (secret key). A data supplier first uploads encrypted documents on a storage system, and then a user of the storage system searches documents containing keywords while insider (such as administrators of the storage system) and outsider attackers do not learn anything else about the documents.

Limitations: anyone (insider/outsider) can retrieve information of certain keyword from any captured query messages..

7) Generic construction of designated tester public-key encryption with keyword Search :

Year: 2012

Author Name:

- H. Rhee
- J. Park
- D. Lee

Description: This paper provides two generic transformations to construct a designated tester public-key encryption with keyword search scheme using two identity-based encryption schemes. We also identify the properties of identity-based encryption that are sufficient to provide the confidentiality and consistency in designated tester public-key encryption with keyword search.

Limitations: does not meet the confidentiality condition, then the privacy of e-mail messages is not guaranteed.

8) Security models for delegated keyword searching within encrypted contents :

Year: 2012

Author Name:

- W. Yau
- R. Phan
- S. Heng
- B. Goi,

Description: This paper propose a Public key encryption with keyword search (PEKS) scheme, first proposed by Boneh et al., which enables to search publicly encrypted messages for keywords without revealing any information about the message.

Limitations: The issue of PEKS schemes being vulnerable to keyword guessing attacks (KGAs)

9) The Random Oracle Methodology, Revisited :

Year: 2002

Author Name:

- R. Canetti
- O. Goldreich
- S. Halevi

Description: We take a critical Look at the Relationship between The security of cryptographic Schemes in the Random Oracle Model, and The security of the Schemes that Result from implementing the random oracle by so called cryptographic Hash functions.

Limitations: Implementation of the random oracle results in insecure schemes.

10) Public key encryption with keyword search :

Year: 2004

Author Name:

- D. Boneh
- G. Di Crescenzo
- R. Ostrovsky
- G. Persiano

Description: This paper proposes Problem of searching On data that is encrypted Using a public Key system. it define The concept of public key encryption with keyword search and give several constructions.

Limitations: Since the resulting scheme is no longer proven secure in our security model.

Limitation of Study:

The only limitation of the system is that here we gave time enabled proxy-re-encryption to data so here there is a time limit to the access that file so in future we are going to increase the time limit so that user can access the file.

Design of the Study

- Input: File in the form of text/Doc.
- Output: File
- Functions :

1 Upload the file in the encrypted form.

2 File gets uploaded on cloud.

3 File is Encrypted by the server that is proxy server.

4 At the time of file upload user enters a keyword, and that keyword is used to download the file.

- Success Conditions: File in decrypted format.
- Failure Conditions: Time period to user.

Tools Used

- **Software Requirement:**

- Operating System : windows 8 and above.
- Application Server : Tomcat5.0/6.X
- Language : Java
- Front End : HTML, JSP
- Database : MySQL

- **Hardware Requirement:**
  - Processor : Intel i3/i5/i7
  - RAM : 4 GB (min)
  - Hard Disk : 20 GB(min)

Statistical Technique Used

We have developed Login and Registration which manages the user profiles (Owner, User, Admin, Proxy Server), here the owner registers and logins uploads the file on cloud in encrypted format. The file is saved on cloud and visible to everyone. Proxy server encrypts the file. Admin can see all the file details that which owner uploaded which files. At the time of file download user gets a conjunctive keyword to get access of that file.

Algorithm

- **ECC**: This algorithm is used to get a encrypted key for user.
- **Data Encryption Standard**: In our system, we have used DES to provide encryption to the uploaded files. Along with that we will be using conjunctive keyword to download the file.

Data Encryption Standard:

```
Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])
begin
byte state[16];
state = in;
AddRoundKey(state, round_key[0]);
for i = 1 to Nr-1 stepsize 1 do
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state, round_key[i]);
```

end for

SubBytes(state);

ShiftRows(state);

AddRoundKey(state, round_key[Nr]);

end

Elliptic Curve Cryptography(ECC):

1. add some extra data to the end of the input

set the initial sha-1 values

for each 64-byte chunk do

extend the chunk to 320 bytes of data

perform first set of operations on chunk[i] (x20)

perform second set of operations on chunk[i] (x20)

perform third set of operations on chunk[i] (x20)

perform fourth set of operations on chunk[i] (x20)

end

return sha-1 values as a key.

Our Approach:

The system will work in three operating modes:

1. Owner:

In this module file is uploaded on cloud by user here the file saves in the encrypted form.

2.User:

In this module user registers and logins and gets the access to the file. Here the user gets the file in the decrypted format. At the time of file download the user has to add the conjunctive keyword which is send to hiss/her mail-id.

3. Admin:

In this module the admin can see all the file details that who uploaded which file etc.

4. Proxy Server :

In this module the the server encrypts the file using DES algorithm.

Experiment Result:
This system will collect the file which a user want and that file is in decrypted format.

Future scope:

In this project we can developed a system which will save the data on cloud and and download the data. In that we also added the functionality of file deduplication so that same data will not be saved on cloud. and this will save the space and and optimize the time. At the time of file download there is a concept of conjunctive keyword so that we will download the file only by providing the keyword to the particular file. In the future we can give the security to file so that we can open the mail of file by providing a security access key.

Acknowledgment: (optional)
It gives us great pleasure in presenting the preliminary project report on 'Accessing cloud data with time constraint and conjunctive keyword for e-health '.
I would like to take this opportunity to thank my internal guide Prof. H. A. Bhute for giving me all the help and guidance I needed I am really grateful to them for their kind support. Their valuable suggestions were very helpful.
I am also grateful to Prof. M. P. Wankhade, Head of Computer Engineering Department, *Computer Department, Sinhgad college of Engineering, Pune*, for his indispensable support and suggestions.
In the end our special thanks to Prof. …….for providing various resources such as laboratory with all needed software platforms,

Mokshada Birari
Ninad Katkar
Namrata Dhumal
Aparna Bamane
(B.E. Computer Engineering).

Conclusion:
In this paper, we have proposed a novel re-encryption technique with timing enabled and testing enabled encryption on data. And the data is going to stored on cloud. this scheme to realize the timing enabled privacy-preserving keyword search mechanism for the EHR cloud storage, which could support the automatic delegation revocation. The experimental results and security analysis shows that our scheme holds much higher security than the existing solutions with a reasonable overhead for cloud applications. To the best of our knowledge, until this is the first searchable encryption scheme with the timing enabled proxy re-encryption function for the privacy–preserving HER cloud record storage. The solution could ensure the confidentiality of the EHR and the resistance to the KG attacks. It has also been formally proved secure based on the standard model under the hardness assumption of the truncated decisional.

Reference:

[1] J. C. Leventhal, J. A. Cummins, P. H. Schwartz, D. K. Martin, and W. M. Tierney, "Designing a system for patients controlling providers' access to their electronic health records: Organizational and technical challenges," *J. General Internal Med.*, vol. 30, no. 1, pp. 17–24,
2015.

[2] Microsoft. *Microsoft HealthVault*. [Online]. Available: http://www. healthvault.com, accessed May 1, 2015.

[3] Google Inc. *Google Health*. [Online]. Available: https://www. google.com/health, accessed Jan. 1, 2013.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. EUROCRYPT*, vol. 3027. Interlaken, Switzerland, May 2004, pp. 506–522.

[5] Q. Tang, "Public key encryption schemes supporting equality test with authorisation of different granularity," *Int. J. Appl. Cryptogr.*, vol. 2, no. 4, pp. 304–321, 2012.

[6] P. Liu, J. Wang, H. Ma, and H. Nie, "Efficient verifiable public key encryption with keyword search based on KP-ABE," in *Proc. IEEE 9th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Nov. 2014, pp. 584–589.

[7] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *Inf. Sci.*, vol. 238, pp. 221–241, Jul. 2013.

[8] M.-S. Hwang, S.-T. Hsu, and C.-C. Lee, "A new public key encryption with conjunctive field keyword search scheme," *Inf. Technol. Control*, vol. 43, no. 3, pp. 277–288, 2014.

[9] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Theory Cryptogr. Conf.*, vol. 4392. Amsterdam, The Netherlands, Feb. 2007, pp. 535–554.

[10] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 262–267, 2011.

[11] J. W. Byun and D. H. Lee, "On a security model of conjunctive keyword search over encrypted relational database," *J. Syst. Softw.*, vol. 84, no. 8, pp. 1364–1372, 2011.