Effective And Secure-Sharing of Medical Record In Cloud-Computing Using Key-Aggregation Crypto-System And Searchable Method

Nikshubha M.V[1], Dr.Anand[2]
[1] Dept of MCA
[2]Assitant professor, Dept of MCA
[1, 2] NMAMIT, Nitte

Abstract- *In the present scenario the health care centres stores data on cloud for accessing it all over the environment where they actually needed for fast service and rapid elasticity. For the security purpose in data sharing effective encryption keys are required. While accessing selected data documents are required to be encrypted with their respective keys. When these data's are used by doctors, they will use secure keys.*

This work focuses on performing single aggregate key for reducing key size. But it will not provide searchable encryption for flexible data sharing. This system works constant single aggregate key for sharing large number of document and that key will be used as a single key to access cloud document which is encrypted. This will contain keywords which are extracted by the document to search in the document. The main advantage of this system is reduces storage overhead by reducing number of keys used and key size.

Keywords- aggregate key, Personal health records, encryption keys, decryption key, Cloud storage.

I. INTRODUCTION

Cloud storage is gaining reputation lately. For the privateness of information the firms nowadays makes use of cloud for storing the information. In traditional way it turned into rely upon the unique server to get admission to facts, this way become not comfortable as the data privateness became no longer relaxed and there was from work of technical personnel. Data sharing is an vital in cloud storage. For example, staffs may have get admission to to touchy information which they will misuse. The fundamental problem is how to proportion encrypted records. For this, users can down load the encrypted facts from the garage, decrypt them, then use for sharing, however it loses the cost of cloud storage. Users ought to make the sharing procedure delegate to others via this it allows them to access from server at once. This proposed venture will assist to proportion partial data from cloud. This gadget uses single consistent key for decryption for set of ciphertexts. Here the one can mixture any set of mystery keys and cause them to as compact as a unmarried key, but encompassing the electricity of all of the keys being aggregated.

In this example, the name of the game key holder can release a constant-size combination key for bendy picks of ciphertext set in cloud garage, however the other encrypted documents out of doors the set continue to be personal. This compact combination key may be conveniently despatched to others or be stored in a clever card with very restricted secure garage.

For protective facts privateness, touchy statistics needs to be encrypted before outsourcing, which obsoletes conventional data usage based totally on plaintext key-word search. Thus, allowing an encrypted cloud facts search provider is of paramount importance. Considering the huge number of statistics users and files in the cloud, it is important to permit more than one key phrases inside the search request and return documents within the order in their relevance to these key phrases..

II. LITERATURE SURVEY

Security and privacy is the biggest problem while the files of patients we upload on the cloud and when we adopt it. This section deals with the existing literature works. For the better improvement of reliability and scalability while sharing the data on the cloud this is based on attribute based encryption.

To improve scalability this system uses approach one will have to many methods. This has the ability to convert the cipher text encrypted under the public key for users. But this converts only cipher texts according to instructions so the owner has to trust proxy. When the file increases their respective keys too will be increased. So by this way the method will be having too many encryption and decryption.

The proposed system enables access over the data. For enabling secure and flexibility of data sharing on the cloud, encryption keys should be managed efficiently.

The proposed system providing:

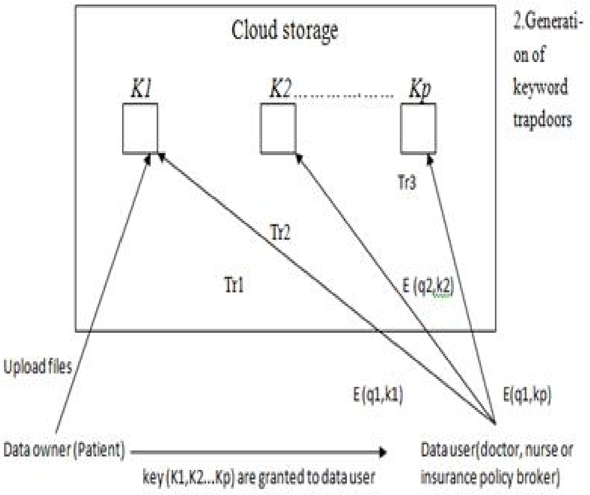
- The method selective sharing of data requires to maintain encrypted with different keys.
- The data users such as doctors will securely store the received key and then submit the keyword to the cloud server to perform keyword based search on the authorized encrypted file.
- The current system reduces key size by generating aggregate key, but this doesn't provide searchable encryption on files, which requires flexible sharing of data.
- This system will maintain single aggregate key for many documents and user will submit a single aggregate key to the cloud for searching the files over the encrypted document.

III. EXISTING SYSTEM

The patient record will be maintained by the patients to the cloud which mainly eliminates the dependency to the physical storage and sharing of information to the doctor. For outsourcing system of cloud it has mainly featured for security and data privacy. The patients while uploading the record will encrypt the data and while the user downloads that file will be in decrypting information. This avoids malicious users.

Limitations:

- Single key is maintained for multiple files.
- Hackers can hack the files easily by applying brute force method.
- This will demand individual encryption keys for the different files, for this reason this requires large number of keys to be distributed over the key users.
- Searching is difficult.
- Relay on cloud server for encryption.
- This increases number of keys and as the files increases.


Cloud storage
K1
K2…………………
Kp
2.Generati-on of keyword trapdoors
Tr3
Tr2
Tr1
E (q2,k2)
Upload files
E (q1,k1)
E(q1,kp)
Data owner (Patient)
key (K1,K2...Kp) are granted to data user
Data user(doctor, nurse or insurance policy broker)

Traditional system of sharing data on cloud

IV. PROPOSED SYSTEM

Here the patient will provide single aggregate key for sharing the number of records with the data users such as nurse, doctor etc. so that data user will use single keyword trapdoor instead of searching the whole encrypted cloud file. So in this system, the keyword based search and decryption method is clearly achieved by sharing single aggregate key instead of multiple keys.

The proposed system is based on :

- Multiple-key searchable encryption scheme.
  - Each file is encrypted with different key.
  - Index is created which contains keywords.
  - Using key files can be searched.
  - Advantage is eliminates association attack.
- Key-aggregate cryptosystem
  - Aggregate key is created for multiple files.
  - Maintains one key which has deciphering path to decrypt .
  - The key is maintained by the owner.
  - It helps for selective sharing.
  - Search is performed on encrypted data.
  - This has high level security and flexibility.

V. PRELIMINARIES OF THE PAPER

In this section, we describe the critical issue-combination cryptosystem [1] superior with the resource of manner of Chu et al. For affected man or woman controlled encryption.

This scheme includes 5 algorithms as follows:

- Setup [1k, n]: To installation scheme this set of rules can be taking walks. As an enter it'll take safety parameter and quantity of classes of affected character statistics. It outputs the general public parameter.
- KeyGen: To generate public and grasp-mystery key [pk,msk] this set of rules will run.
- Encrypt [pk, i, record]: The algorithm will run by affected person or statistics users who want to encypt report. As input it's going to take public key(pk), index(i), report. Output could be encyped file.
- Extract [msk, S]: To generate aggregate key this algorithm might be run by means of affected person to provide decryption rights for advantageous set of ciphertext . It will take master mystery key and set of indices.

VI. IMPLEMENTATION DETAILS

Platform and Technology . The following technologies used:

Operating System: windows 7,8,10.

Database: Simple DB and S3-Simple storage Service
Software: Visual Studio .Net [Framework 4.0 and above]

Datasets:

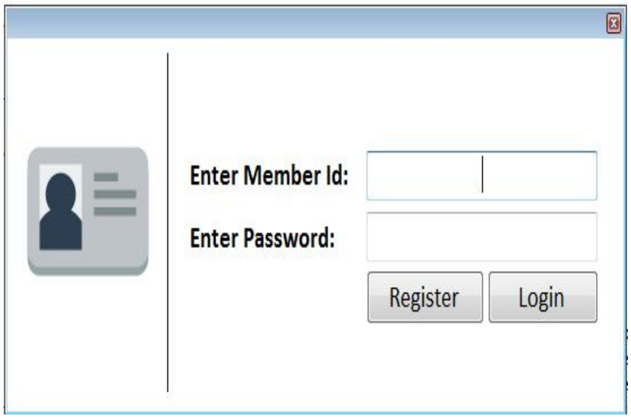
We collected different records that evaluate the real world information. The records collected from different hospitals and that are arranged in a structure as per the requirements given by patients.

VII. FINAL OUTCOMES

The authorized users register themselves and getting started with the application. The application based on the sharing of patient health records. The patient will share the test records and he will upload it to the cloud. The data user will use the information. The files with index will be encrypted and send to the cloud.

Login page

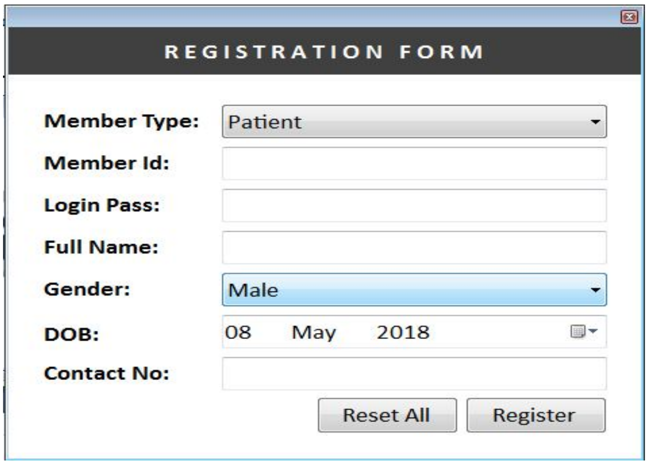
Owner or user register or login form:



Enter Member Id:
Enter Password:
Register Login

Description: Data user or patient gets register or login with all the information. They will be assigned with the member id and the password. By this the code behind will be recording in the amazong simple DB.

Owner or User registration form:

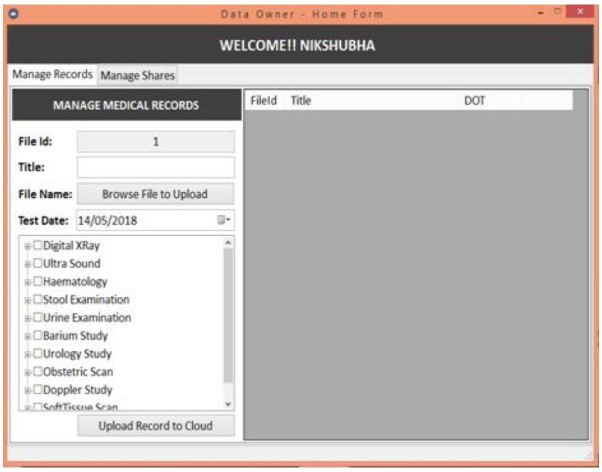


REGISTRATION FORM

Member Type: Patient
Member Id:
Login Pass:
Full Name:
Gender: Male
DOB: 08 May 2018
Contact No:
Reset All Register

Description: Data owner and patient will give all his information and gets registered. Only the patient gets the master key and from that master key the file keys are derived and in the cloud the bucket is created to store the records.

Health record upload module before uploading:



File Id: 1

Title:

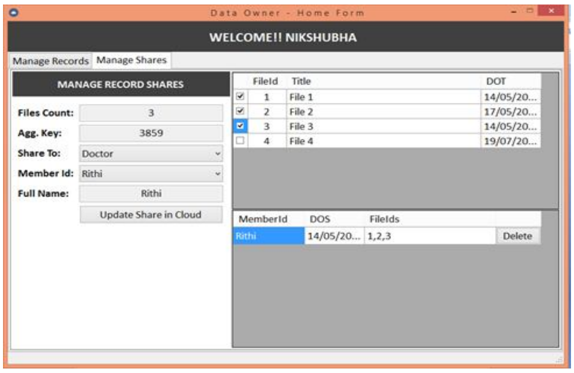
File Name: Browse File to Upload

Test Date: 14/05/2018

- □ Digital XRay
- □ Ultra Sound
- □ Haematology
- □ Stool Examination
- □ Urine Examination
- □ Barium Study
- □ Urology Study
- □ Obstetric Scan
- □ Doppler Study
- □ SoftTissue Scan

Description: The patient will upload the file which may be word text, image, pdf. He will select the tests he has undergone. This will be uploading to cloud. While uploading the encrypted file and the index file will be uploaded.

Record sharing module:



Files Count: 3

Agg. Key: 3859

Share To: Doctor

Member Id: Rithi

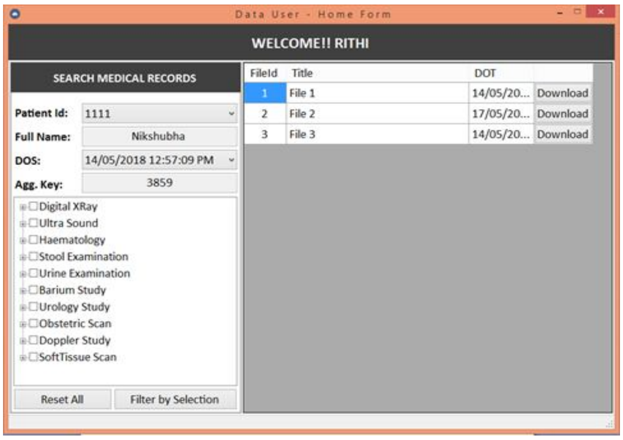
Full Name: Rithi

	FileId	Title	DOT
☑	1	File 1	14/05/20...
☑	2	File 2	17/05/20...
☑	3	File 3	14/05/20...
□	4	File 4	19/07/20...

MemberId	DOS	FileIds	
Rithi	14/05/20...	1,2,3	Delete

Description: The data owner will select the files which he want to share to the doctors according to the date of the day he shares and he will upload to the cloud. The owner has even the option to delete the file after he upload to the cloud. In this case the aggregate key will be generated for the files he want to share. Everything will be uploaded to cloud.
And maintains information in it.

Document retrieval module:



Patient Id: 1111

Full Name: Nikshubha

DOS: 14/05/2018 12:57:09 PM

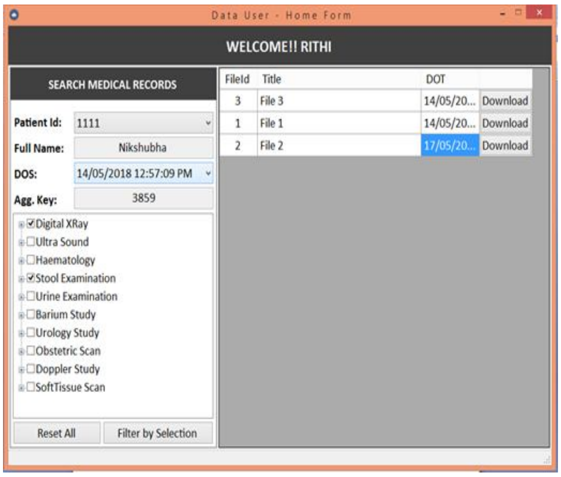
Agg. Key: 3859

- □ Digital XRay
- □ Ultra Sound
- □ Haematology
- □ Stool Examination
- □ Urine Examination
- □ Barium Study
- □ Urology Study
- □ Obstetric Scan
- □ Doppler Study
- □ SoftTissue Scan

FileId	Title	DOT	
1	File 1	14/05/20...	Download
2	File 2	17/05/20...	Download
3	File 3	14/05/20...	Download

Description: The form of record user is going to decrypt the record which will be uploaded by the patient. He will use the symmetric key for downloading of record using the users private key.

Document which can see by user:



Patient Id: 1111

Full Name: Nikshubha

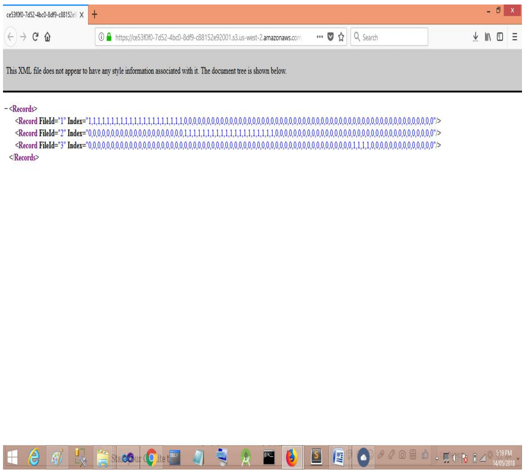
DOS: 14/05/2018 12:57:09 PM

Agg. Key: 3859

- ☑ Digital XRay
- □ Ultra Sound
- □ Haematology
- ☑ Stool Examination
- □ Urine Examination
- □ Barium Study
- □ Urology Study
- □ Obstetric Scan
- □ Doppler Study
- □ SoftTissue Scan

FileId	Title	DOT	
3	File 3	14/05/20...	Download
1	File 1	14/05/20...	Download
2	File 2	17/05/20...	Download

Document which are in encrypted format:



https://ce53f0f0-7d52-4bc0-8df9-c88152e92001.s3.us-west-2.amazonaws.com

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <Records>
    <Record FileId="1" Index="1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0"/>
    <Record FileId="2" Index="0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0"/>
    <Record FileId="3" Index="0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0"/>
  </Records>
```

Description: The files if the hacker downloads will be in encrypted format, so that users cannot decrypt it.

VIII. CONCLUSION AND FUTURE SCOPE

The primary trouble inside the present surroundings is privacy and facts sharing, the proposed gadget is based on asymmetric-key cryptosystem for hierarchy of affected person records and having access to the information in the cloud. By using this device affected person is wanted to distribute a unmatched mixture key at the same time as sharing a huge range of file with extraordinary customers like medical doctors and nurse, etc. They will use the unmatched mixture trapdoor for having access to everywhere in the statistics. The end result might be confirmed based totally at the performance for comfy and scalable sharing of records on cloud storage. In this gadget it'll generate unmatched aggregate trapdoor for plenty keys with the aid of having key-word search approach. This reduces wide variety of trapdoors for multi-key phrases. Federated clouds have become famous in recent times, however our scheme can't be immediately carried out.

IX. ACKNOWLEDGEMENT

Thanks to my guide Dr. Anadh R who gave support me in all ways for this paper.

REFERENCES

[1] Programming amazon web services :S3,EC2,SQS,FPS and SimpleDB.

[2] Books on Amazon Simple Storage Service (S3) Getting Started by Kindle Edition.