ELECTRONIC HEALTH RECORD(EHR) SERVICES USING QR CODE IN CLOUD COMPUTING

Mrs.S.Gayathri[1], Santhosh Kumar.N[2], Ranjith Kumar.G[3]

[1]Assistant Professor, Computer Science And Engineering, Jeppiaar SRR Engineering College, Tamil Nadu, India
[2]UG Student, Computer Science And Engineering, Jeppiaar SRR Engineering College, Tamil Nadu, India
[3]UG Student, Computer Science And Engineering, Jeppiaar SRR Engineering College, Tamil Nadu, India

ABSTRACT

The main goal of our project is to design a mobile application for patients through web-based application management that acquires secure access to patient records through cloud storage service. Admin can remotely store patient data to the cloud with safe and secure cloud storage through and Patient can easily access their data which are stored in cloud based on EHR Service management. Remote data integrity of health record is proposed to guarantee the integrity of the secured data stored in the cloud. In some common cloud storage systems, cloud file might contain some sensitive information. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared file unable to be used by others. In this paper we propose a remote document reference id automatically convert to the QR code then just scan user module then download the particular document integrity that realizes data sharing with sensitive information hiding. Signatures are used to verify the file in the phase of integrity health records.

Keyword: -*EHR service Management, Attribute Based Encryption (ABE),*

1. INTRODUCTION

An Electronic Health Record (EHR) is an electronic rendition of a patient's wellbeing history that archives all the applicable clinical subtleties over some undefined time frame and is kept up by medicinal services suppliers. EHRs assist associations with giving improved medicinal services benefits via robotizing understanding data access and the executives. In 2003 the U.S. Establishment of Medicine distributed an accord study report, Key Capabilities of an Electronic Health Record System. EHR records patient's essential details, analyze, meds, vaccination history, lab and radiology reports, specialist notes and other therapeutic certainties alongside patient's close to home subtleties. In light of the HL7 EHR Functional Model, we distinguished the key data fields in an average EHR framework and referenced in our framework structure. The Health Information Technology for Economic and Clinical Health (HITECH) Act sets security gauges that each restorative supplier ought to conform to while giving quality wellbeing administrations. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) directs the administration and appropriation of therapeutic records by setting up benchmarks for saving the security and protection of medicinal wellbeing information. Cloud based EHR benefits in the United States are required to conform to these administrative gauges thus should guarantee upgraded information assurance joined with a consistent client experience that cloud administrations offer. This additionally necessitates they actualize exacting access control components to guarantee unapproved access by any client is precluded by their EHR administration. Consequently EHR frameworks regularly scramble their dataset and approach limited to just the parental figures legitimately treating the patient. There are frequently situations, as when the patient's wellbeing abruptly weakens, that require records be made accessible to pros (who could be remote) or other parental figures who probably won't have beginning access to the patient's wellbeing records. Existing approval models follow a patient centric approach

where the EHR information approval must be endorsed by the patient. This isn't commonsense in each situation and also the patient may not be in a state to give this approval when required. Henceforth there is a need to build up an approval designation system where by the patient approves the supplier access to his/her EHR and the supplier thus appoints this approval to proper workers or partners to get to the information.

2. EXISTING SYSTEM

The Existing concept is a proper authorization delegation mechanism to use cloud-based EHR Service management using Attribute Based Encryption (ABE) in web technologies that involves the combination of using semantic web technic with attributes based schemes.

Existing Algorithm:-

Attribute Based Encryption (ABE).

3. PROPOSED SYSTEM

We propose a remote document reference id automatically convert to the QR code then just scan user module then download the particular document integrity that realizes data sharing with sensitive information hiding. Signatures are used to verify the file in the phase of integrity health records.

Proposed Algorithm:- QR code generate Algorithm

3.1. Architecture Diagram

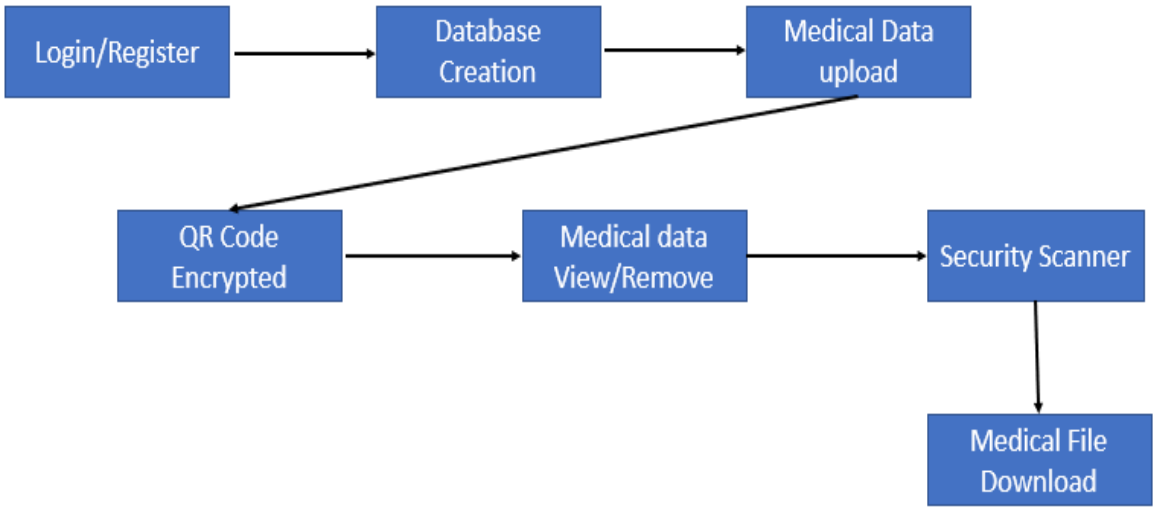

Fig-1: Architecture Diagram

4. SYSTEM HARDWARE AND SOFTWARE

Hardware Used

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the system does and not how it should be implemented.

PROCESSOR	:	Intel Core i3.
RAM	:	4 GB DDR2 RAM
MONITOR	:	15" COLOR
HARD DISK	:	100 GB

Software Used

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the team's and tracking the team's progress throughout the development activity.

Front End	:	ANDROID XML, JAVA
Back End	:	SQLITE
Operating System	:	Windows 07
IDE	:	Eclipse, Android Studio

.

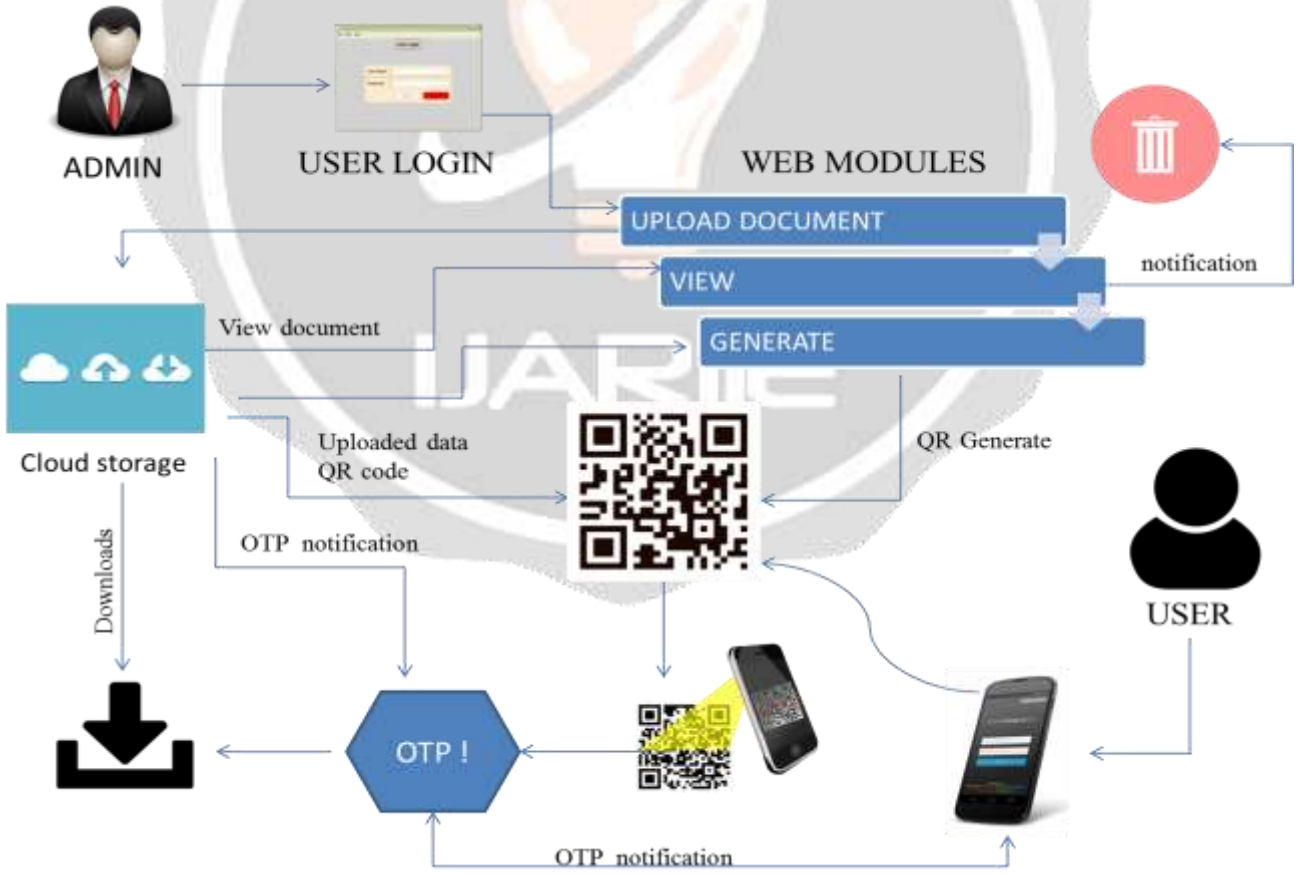

Fig-2: Detailed Diagram

5. WORKING

MODULES:

- Login / Registration.
- Database Creation.
- Medical Data upload
- QR Code Encrypted
- Medical data View/Remove
- Security Scanner
- Medical File Download

- **LOGIN & REGISTRATION:**

We design to develop login and signup screen. Android used xml to develop classical screens in our application. The modules describe signup page contains email id or user name, password and conform password those kind of details should be stored in database. Login screen contains email id or username and password when the user to login the app it should be retrieve the data to the database and combine based on user input if its match user name and password to allow in the app otherwise alert and show a message to the user

- **DATABASE CREATION:**

User email id or user name and password have been stored after registration. Android used SQLite Database for storing and fetching user application details

- **MEDICAL DATA UPLOAD:**

To upload the user information in storage cloud in secure data are user information, Medical record information and patients details etc.…

- **QR CODE ENCRYPTOR:**

We have created a QR code generate a using Encrypt the value like medical records data and patients details that can be create are login users.

- **MEDICAL DATA VIEW / REMOVE:**

Medical data view/remove that process can be used on logged user view a medical data and incase that data can remove. But original values not delete in permanent.

- **SECURITY SCANNER:**

Security scanner like the three security can be using the projects are security patch, unique QR code Reader and Make QR code that particular person can be used in application.

- **MEDICAL FILE DOWNLOAD:**

We have to create a medical file download are overall data stored in cloud the specific user medical record finds to view and download the particular user records.

6. EXPERIMENTAL RESULTS

The result involves the design and implementation services are platform independent and provide aggregated patient information with robust data searching, retrieval, etc., Stronger authentication mechanisms can help prevent unauthorized access by using QR code patterns of use.

7. APPLICATIONS

- In Hospital Based System
- In Banking Sector for security Purpose
- Airlines and transport based system
- In Educational Institute
- Computerized Library System

8. CONCLUSION

We propose a remote document reference id automatically convert to the QR code then just scan user module then download the particular document integrity that realizes data sharing with sensitive information hiding. Signatures are used to verify the file in the phase of integrity health records.

9. REFERENCES

[1]. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE transactions on parallel and distributed systems, vol. 24, no. 1, pp. 131–143, 2013.
[2] S. Chandra, V. Karande, Z. Lin, L. Khan, M. Kantarcioglu, and B. Thuraisingham, "Securing data analytics on sgx with randomization," in European Symposium on Research in Computer Security (ESORICS), 2017, pp. 352–369.
[3] F. Schuster et al., "Vc3: Trustworthy data analytics in the cloud using sgx," in IEEE Symposium on Security and Privacy. IEEE, 2015, pp. 38–54.
[4] J. A. Evans, "Electronic medical records system," Jul. 13 1999, uS Patent 5,924,074.
[5] E. H. Shortliffe et al., "The evolution of electronic medical records," ACADEMIC MEDICINE-PHILADELPHIA-, vol. 74, pp. 414–419, 1999.
[6] M. Lavin and M. Nathan, "System and method for managing patient medical records," Jun. 30 1998, uS Patent 5,772,585.
[7] S. Narayan, M. Gagne, and R. Safavi-Naini, "Privacy preserving ´ ehr system using attribute-based infrastructure," in CCSW, 2010.
. [10] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.
[11] D. S. Roche, A. Aviv, and S. G. Choi, "A practical oblivious map data structure with secure deletion and history independence," in Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016, pp. 178–197.
[12] E. Stefanov, M. Van Dijk, E. Shi, C. Fletcher, L. Ren, X. Yu, and S. Devadas, "Path oram: an extremely simple oblivious ram protocol," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 299–310.
[16] L. Kagal, T. Finin, and A. Joshi, "A policy language for a pervasive computing environment," in Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on. IEEE, 2003, pp. 63–74.
[17] L. K. J. N. R. S. W. H. W. Tim Finin, Anupam Joshi and B. Thuraisingham, "Rowlbac - representing role based access control in owl," in 13th Symposium on Access control Models and Technologies. ACM Press, June 2008.
[18] J. M. Bradshaw, A. Uszok, M. Breedy, L. Bunch, T. Eskridge, P. Feltovich, M. Johnson, J. Lott, and M. Vignati, "The kaos policy services framework," in Proc. 8th Cyber Security and Information Intelligence Research Workshop, 2013.