# Delegated Authorization Framework For EHR Management Using QR Code Encryption

K.GANESH[1], R.KARTHIK[2], MAHESWARI[3]

*1 Student, Computer science and engineering, Anand Institute of Higher Technology, Chennai, India.*
*2 Student, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India.*
*3 Professor, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, 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.*

**Keywords**—*EHR Service Management, QR code, unique scanner .*

## 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. LITERATURE SURVEY

### LITERATURE SURVEY 1

**CONCEPT USED**

The motives behind the adoption or rejection of Electronic Health Records (EHR) systems in the USA by medical offices. The current health care system in the United States suffers from high expenditures and poor quality. The Patient Protection and Affordable Care Act, passed in 2010, attempts to save costs and improve quality of care by offering incentives to use Electronic Health Records systems. Part of the reform by this law is dependent on the use of technology in managing patient medical and health records. The objective is to reduce redundancy and increase quality by sharing medical information amongst different health organizations like hospitals, physician offices, laboratories and clinical institutions.

### LITERATURE SURVEY 2

**CONCEPT USED**

It is based on Access control mechanisms are vital to the privacy preservation and information security in electronic medical record system. In this paper, we analyze the existing drawbacks in traditional access control models firstly and outline the characteristics of next generation access control UCON. Then we apply the idea of UCON to electronic medical record system to meet the challenge of confidentiality, privacy preservation and data integrity. Then the novel access control formalisms of electronic medical record are presented. Various applications are presented to demonstrate its effectiveness.

### LITERATURE SURVEY 3

**CONCEPT USED**

It describes Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to

unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers.

## 3. EXISTING SYSTEM

Above list of papers were surveyed for several factors with respect to our proposed idea. The factors include cost efficiency, processing efficiency, time efficiency, system maintenance, customer satisfaction. Out of all the above paper reference the 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. Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes.so the existing system security is very less.

## 4. PROPOSED SYSTEM

In this 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. QR code proves to be too expensive for many applications as compared to other tracking and identification methods, such as the simple barcode. In addition to that we add a security like OTP generation for that particular patient to access the patient records through patient handheld device. This way we give more security to access the particular document via more security.

## 4.1 IMPLEMENTATIONS

### 4.1.1 LOGIN & REGISTRATION:

In this module 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.


### 4.1.2 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.


### 4.1.3 MEDICAL DATA UPLOAD:

In this module, to upload the user information in storage cloud in secure data are user information, Medical record information and patients details etc.…


### 4.1.4 QR CODE ENCRYPTOR:

In this module, 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.

### 4.1.5 SECURITY SCANNER:

In this module are 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.


### 4.1.6 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.

## 5. CONCLUSION AND FUTURE ENHANCEMENTS:

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.

In future it will also enhance our framework to include the EHR data exchange and routing functionality that are essential for inter organizational EHR frameworks. There are numerous extra security and protection issues that can be tended to that we leave for future work. For instance, more grounded confirmation systems can help to avoid unapproved access by an assailant.

**6.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.

[8] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.

[9] M. Joshi, S. Mittal, K. P. Joshi, and T. Finin, "Semantically rich, oblivious access control using abac for secure cloud storage," in Edge Computing (EDGE), 2017 IEEE International Conference on. IEEE, 2017, pp. 142–149.

[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.