International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

# Sharing of PHR on Cloud Using Attribute Based Encryption and Access by QR-Code

**Sagar Pagar, Rahul Yadav, Sumeet Boraste, Harshal Bairagi.**

*Guided By Prof. A. G. Khairnar,*
*Department of Information Technology, Nashik District Maratha Vidya Prasarak Samaj's Karmaveer Adv. Baburao Ganpatrao Thakare College of Engineering.*

---

**Abstract -** 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. It help the Patient to stores his data on the cloud. 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 patient's 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. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. And we introduced a new technique which is known as "Break Glass method" which is used in case of emergency.

Keywords: Personal health records, cloud computing, data privacy, attribute-based encryption.

## 1. INTRODUCTION

Personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft Health Vault Recently, architectures of storing PHRs in cloud computing have been proposed. 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.

## 2. PROBLEM STATEMENT

With the rapid development of the cloud computing, personal health record (PHR) has attracted great attention of many researchers all over the world recently. However, PHR, which is often outsourced to be stored at a third party, has many security and efficiency issues. Therefore, the study of secure and efficient Personal Health Record Scheme to protect users' privacy in PHR files is of great significance. Focusing on drawbacks and inadequacies of existing process, definitely there is a need of an efficient system which ensures data security.

## 3. SYSTEM DESIGN

In the proposed system, the personal information of the patient will be stored in a form of data on cloud which will be stored in an encrypted format on the cloud for security purposes. Attribute Based Encryption (ABE) will be used for the process of encryption. This encrypted data will be saved on secured cloud. A QR code will be generated using attributes like patient name and Patient ID. To extract the data from the cloud the user will be required to scan the QR code to access the data. After authentication the decrypted data will be displayed to the authenticated user. The PHR can be shall be accessed by using an mobile application. The decision of granting access rights of this PHR will given to the patient. The patients, doctors will have a right for modification of the information whereas pharmacists will only have right to replace the prescribed medicine. The blow diagram shown below will give a clear idea of our proposed system.

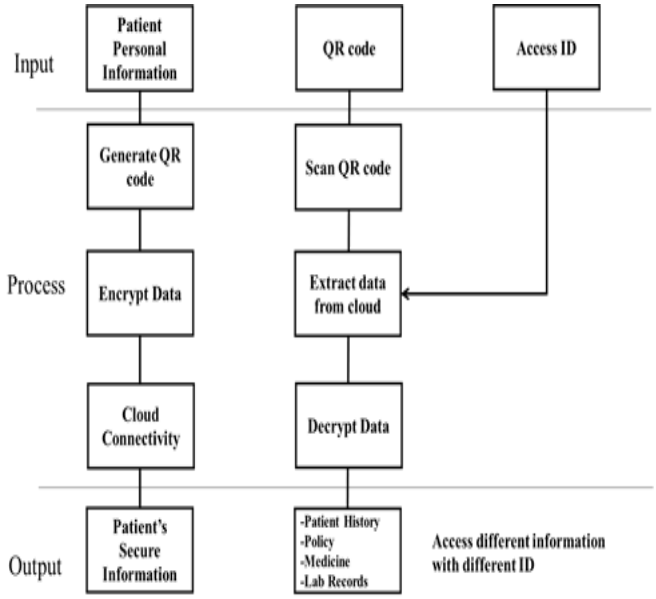



Figure 1: System Diagram

Personal Health Record: 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. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of his/her medical records and can share his/her health data with a wide range of users, including healthcare providers, family members or friends.

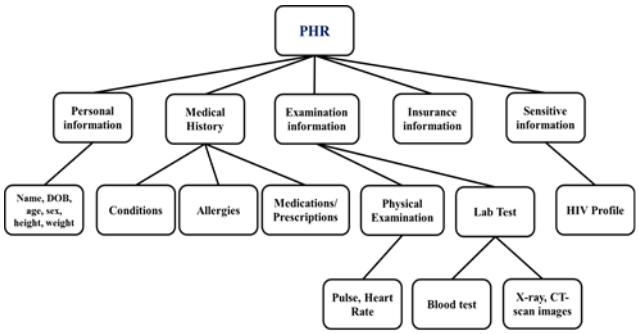



Figure 2 : Components of PHR.

QR-Code: The foursquare Quick Recognition (QR) code consists of coding region and functional regions. The coding region is described by some characters, which represent the data, version, format, and so on. The functional regions are the combination of localization graph, correcting graph, separator and some seeking graphs, which would not be used for data encoding. The region of four module wide around the QR code image is named as blank, which has the same reflective index with light-colored modules. The most remarkable regions are three graph blocks used for image seeking. The three graph blocks locate at the top left comer, left lower comer and the top right comer of the QR code image, respectively.

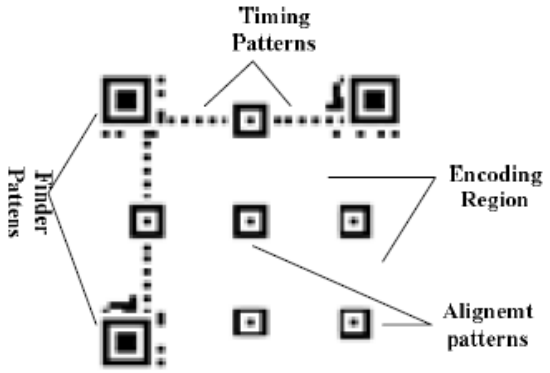
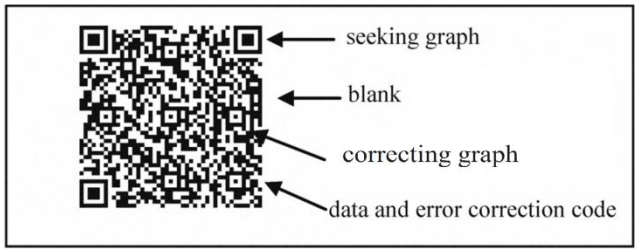



Figure 3 : Structure of QR code



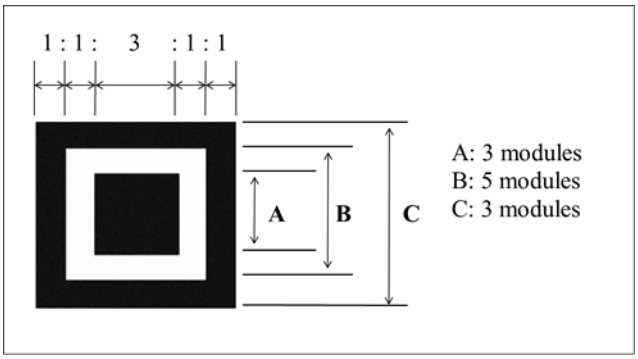




Figure 4 : The structure of the seeking graph block in QR code image

The seeking graph is made of three overlapped homocentric squares, including 7x7 dark-colored modules, 5x5 light-colored modules and 3x3 dark-colored modules. The width proportion of the modules is 1: 1: 3: 1: 1. Because the relationship of these three modules appears seldom in practical process of image seeking, we use them to define the position of the seeking graphs and obtain the image

information. The separators situated between the seeking graph blocks and coding region. They are one-module width and light-colored. The localization graph consists of dark-colored and light colored module arranged alternately which align to a row and a column. They can express the density of characters, version and decide the basic coordinate position of modules. The correcting graph is composed of three overlapped homocentric squares, too. They are dark-colored, light-colored and dark colored modules arranged from exterior to interior respectively. The specification of them are 5x5, 3x3, a dark colored module in the center. Only Version 1 of QR code image lack of localization graph, the others have their respective localization graphs. These localization graphs of QR code image arranged by symmetry in a diagonal position and can be used to correct the coordinate value of current region in barcode image recognition.

Flow of QR-Code Recognition:

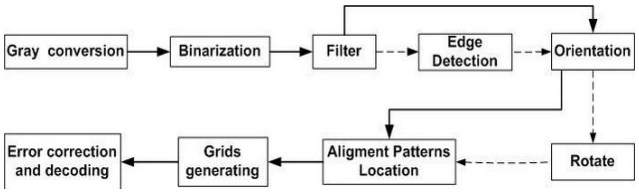



Figure 5 : Flow of QR-Code Recognition Algorithm

Many researchers have dealt with QR code image during last decades, but the process speed of it is always a problem hard to increase. We proposed a novel detection method of QR code in the paper according to the characteristics of QR code shape. Figure shows the flow of QR code image processing. The main processes include image seeking, localization adjustment and image recognition.

## 4. CONCLUSIONS

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

## ACKNOWLEDGEMENT

With all respect and gratitude, we would like to thank all the people who have helped us directly or indirectly for the completion of the project “Sharing of PHR on Cloud Using Attribute Based Encryption and Access by QR-Code ". We express our heartily gratitude towards Prof. A. G. Khairnar for guiding us to understand the work conceptually and also for her constant encouragement to complete the project. Our association with her as a student has been extremely inspiring. We would like to give our sincere thanks to Prof. H. V. Patil, Head of the Department of Information Technology for her technical support and constant encouragement. We would also like to extend our sincere thanks to our Principal Dr. K. S. Holkar for his help and support in all respects. We would also like to thank all our staff members and collogues who helped us directly or indirectly throughout our dissertation work.

## REFERENCES

[1] Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE “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, January 2013

[2] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” Proc. ACM Workshop Cloud Computing Security (CCSW ’09), pp. 103-114, 2009.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM ’10, 2010.

[4] C. Dong, G. Russello, and N. Dulay, “Shared and Searchable Encrypted Data for Untrusted Servers,” J. Computer Security, vol. 19, pp. 367-397, 2010.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’10), 2010.

[6] L. Ibraimi, M. Asim, and M. Petkovic, “Secure Management of Personal Health Records by Applying Attribute-Based Encryption,” technical report, Univ. of Twente, 2009.

[7] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, “Spins: Security Protocols for Sensor Networks,” Wireless Networking, vol. 8, pp. 521-534, Sept. 2002.