Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024

# MEDICAL DATA APPLIED QR CODE FOR PRIVACY PROTECTION USING AES ALGORITHM, ONE TIME PASSWARD PROTOCOL AND QR CODE GENERATOR ALGORITHM

**Kirti T. Kamthe, Prasad Bhosle, Rutika Shah,** Department of Computer Engineering , Trinity College of Engineering and Research, Savitribai Phule Pune University, India

**ABSTRACT:**
Medical data are an ever growing source of information generated from hospitals consisting of patient records in the form of hard copies which can be made easier and convenient by using QR Code of the patient details. Our aim is to build a Health-care Portal system which will provide the features like clinical management, patient records, disease prediction and generate QR Code for every patient as per there updated disease information.
There is a growing concern in the medical field, both on the side of physicians and other care providers as well as on the insurance and payer side about the impact medication non-adherence has on health care outcomes and costs. The widespread uses of smartphones at an unprecedented rate have revolutionized the way people access to information particularly in the health care sector. The use of mobile healthcare applications is a dynamic field and has received great attentions lately. This development provides mobile technology more attractive for mobile health (m-health) applications. The m-health is defined as a wireless telemedicine involving the use of mobile telecommunications and multimedia technologies and their integration with mobile healthcare delivery systems. Including human in authentication protocols, while guaranteeing, is not simple in light of their restricted capacity of calculation and remembrance. We exhibit how careful visualization outline can improve the security as well as the convenience of authentication. We propose health care service for generate QR Code through web/android application.
**Keywords:** QR (Quick Response) Code, healthcare, mobile health (m-health), Health Monitoring, QR Code Technology, Medical Records, etc.

## INTRODUCTION

In medical management, more and more information technologies are applied to improve work efficiency. For example, the hospital information management system is used to carry out a patient's basic information and medical management, the wrist one-dimensional QR code is employed to quickly read or input a patient's identity (ID) and so on. Information technology brings convenience while at the same time there are certain secure drawbacks in several typical scenarios because of immature technology or management vulnerability, such as, the health record transparency leaks user privacy, access to view the medical privacy record is not strictly controlled, infusion confirmation is without technical authentication, patient wrist ID is easy to be forged, payment is not convenient and so on.[5]
The objective of this project is information. to develop a system where a person can enter his/her medical The system mainly focuses on the ability to quickly access information in case of any emergency. The users will be able to see the details of the person who needs any kind of medical attention. The system provides the information of the person, which includes his recent medical records and also personal details.
Most current e-/m-healthcare systems require doctors (or system administrators) to participate in medical information processing, which brings two problems: low effectiveness caused by manual operations and privacy violation due to doctors' contact with users' private data. A medical expert system that can automatically analyze users' clamber private data but reduce doctors' participation can address these two problems, particularly for the application of general physical examinations. [8]

Even with perfect access control mechanisms, frequent human intervention will always cause a higher risk of privacy reveal in e-/m-healthcare. As a major component of e-/m-healthcare systems, the development of a medical specialist system is another focus of this paper.
A safe and good e-/m healthcare framework to defend against hostile attacks and risk is highlighted for available applications of the informationalzed healthcare industry. Moreover, a challenge remains concerning how to effectively process the ever-growing volume of healthcare data and protect data privacy but maintain low sensor network overhead .[2]
Therefore, how to achieve medical data collection, transmission, processing and presentation has become a critical matter in e-healthcare applications, in which a variety of wireless sensor nodes and terminal devices play important roles in network data collection and connection. Furthermore, the evolution of m-health (mobile-health) technology has made it possible for people to together information about their health status easily, anytime and anywhere using smart mobile devices .[2]

## 2.LITERATURE SURVEY

Krzysztof Czuszynski, Jacek Ruminski [1], In this paper an application of QR codes to exchange of laboratory results is presented. The secure data exchange is proposed between a patient and laboratory and between Electronic Health Records and patient. Limitations: The interaction between professional healthcare and patient can be improved, since physician can receive a file with complete set of test results from the patient and comment them in reply.[1]
Paschou Mersini, EvangelosSakkopoulos, Athanasios Tsakalidis [2], In this work, they have described an integrated system, developed for use by the healthcare personnel within healthcare facilities, adapted to smart phones, tablets and handheld devices. Key goal is to facilitate doctors, nurses and the involved personnel throughout the facility, regardless of the existence of network connection in the area using a typical smart phone. Limitations: Disease prediction and medicine prescriptions by specific doctor is not being implemented.[2]
Ran Wei, Zhimin Yang [3], It represent the interaction between patient and doctor based on Android. Its superb performance on mobile terminals makes it potential that patients area unit able to access the hospital server to get the mandatory suggestion about the symptoms and move with there own mobile terminals, whereas doctors will track patients whenever and where potential or build a diagnosing of alert depends on the observation knowledge from the hardware of mobile terminals. Limitations: System has lacking, such as in the monitoring module, when the objects in the camera changes in a large scope, the amount of coded data increases quickly which will affect the system efficiency decrease.[3]
Sudha.G and Ganesan.R [4], It is created for accessing the medical multimedia data of patients when the user is in mobility. The mobile have less memory to store a data. So to access the large database with security, we use the My Sql database in server system. This connectivity is create with the help of server program. It make certain authentication and security in accessing database. Limitations: The mobile application can be developed with context aware, adaptability, delay should be decreased.[4]

## 3.RELATED WORK

**Relevant Objectives**

- To develop a system where a person can enter his/her medical.
- To see the details of the person who needs any kind of medical attention.
- To quickly access information in case of any emergency.

### 5.1 Algorithm

**Reed–Solomon Error Correction Algorithm**

QR code [1], abbreviated from Quick Response Code, is the trademark for a type of matrix barcode or two dimensional barcode. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which

can be read by an imaging device (such as a camera, scanner, etc.) and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image.

Fig.2: QR Code

Reed-Solomon is an error-correcting code that is widely used for data transmission and storage applications. It was introduced by Irving S. Reed and Gustave Solomon in 1960. The Reed-Solomon algorithm is particularly well-suited for correcting errors in data that is transmitted or stored in a noisy or unreliable environment, such as CDs, DVDs, QR codes, and various communication systems.

Here are the key concepts behind the Reed-Solomon algorithm:

1. Symbols and Finite Fields:`
   - Reed-Solomon operates on symbols from a finite field. The symbols are typically binary for digital communication or bytes for data storage applications.
   - The finite field arithmetic is crucial to the functioning of the algorithm.
2. Codewords and Message Polynomial:
   - Data is divided into "blocks," and each block is treated as a polynomial with its coefficients being the data symbols.
   - The original data is encoded into codewords, which are essentially the evaluations of the polynomial at various points.
3. Error Correction:
   - Reed-Solomon introduces redundancy by adding extra symbols to the original data.
   - These redundant symbols are derived from the coefficients of the polynomial.
   - When errors occur during transmission or storage, the algorithm can use the redundancy to correct these errors and reconstruct the original data.
4. Syndrome Calculation:
   - The receiver calculates syndromes based on the received codeword and compares them to detect errors.
   - The syndromes provide information about the discrepancies between the received codeword and the ideal codeword.
5. Error Location and Correction:
   - The syndromes are used to find the error locations in the received codeword.
   - Once the error locations are determined, the algorithm corrects the errors by adjusting the values of the received symbols.

Reed-Solomon codes are widely used in various applications, including CDs, DVDs, QR codes, barcodes, and communication systems. They provide a powerful and efficient method for error detection and correction in situations where data integrity is crucial.

**QR Code Representation**:

Nowadays, when smart phones equipped with cameras are very common, conveying message via QR code has become popular. As the aim was to transfer data from a document to a mobile phone in a feasible way it was a rational choice to apply this standard to our purposes. This standard of graphical

data representation, established in 1994, can hold even 2953 Bytes on a 177 by 177 modules pattern. It possesses an attribute in encoding data resistant for slight code distortions. There were set up four error correction levels and the higher the level, the less is storage capacity. [5] The levels L, M, Q and H allow retrieving the whole message when up to 7, 15, 25 and 30% respectively of the QR image is destroyed. The priority was in getting as much space for data as possible, not particularly in damage resistance. That is why the level L was acclaimed as sufficient.

**AES Algorithm:**

AES stands for Advanced Encryption Standard and is a majorly used symmetric encryption algorithm. It is mainly used for encryption and protection of electronic data. It was used as the replacement of DES(Data encryption standard) as it is much faster and better than DES. AES consists of three block ciphers and these ciphers are used to provide encryption of data.

- **Wireless Security:** Wireless networks are secured using the Advanced Encryption Standard to authenticate routers and clients. WiFi networks have firmware software and complete security systems based on this algorithm and are now in everyday use.
- **Encrypted Browsing**: AES plays a huge role in securing website server authentication from both client and server end. With both symmetric and asymmetric encryption being used, this algorithm helps in SSL/TLS encryption protocols to always browse with the utmost security and privacy.
- **General File Encryption:** Apart from corporate necessities, AES is also used to transfer files between associates in an encrypted format. The encrypted information can extend to chat messages, family pictures, legal documents, etc.
- **Processor Security:** Many processor manufacturers enable hardware-level encryption using the likes of AES encryption to bolster security and prevent meltdown failures, among other low-profile risks.

**One-Time Password Protocol:**

Authentication, the process of identifying and validating an individual is the rudimentary step before granting access to any protected service (such as a personal account). Authentication has been built into the cyber security standards and offers to prevent unauthorized access to safeguarded resources. Authentication mechanisms today create a double layer gateway prior to unlocking any protected information. This double layer of security, termed as two factor authentication, creates a pathway that requires validation of credentials (username/email and password) followed by creation and validation of the One Time Password (OTP). The OTP is a numeric code that is randomly and uniquely generated during each authentication event. This adds an additional layer of security, as the password generated is fresh set of digits each time an authentication is attempted and it offers the quality of being unpredictable for the next created session. The two main methods for delivery of the OTP is:

**SMS Based:** This is quite straightforward. It is the standard procedure for delivering the OTP via a text message after regular authentication is successful. Here, the OTP is generated on the server side and delivered to the authenticator via text message. It is the most common method of OTP delivery that is encountered across services.

**Application Based**: This method of OTP generation is done on the user side using a specific smartphone application that scans a QR code on the screen. The application is responsible for the unique OTP digits. This reduces wait time for the OTP as well as reduces security risk as compared to the SMS based delivery.

**Problem Statement and Solving approach**

- To overcome the problem of patients, we have implemented the system where a user/patient hides their information in QR code and the system will provide the patient with a unique ID to access when that patient/user is in the processing case. Doctors identify symptoms and assign treatment options to patients.
- The pharmacist will scan the hat's QR code and administer the medicine to the patient/user.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024

Finally, there is the insurance service. Develop specific plans based on the patient's perspective.

- The proposed system's attention to the safety of the user's patient is an extreme requirement for healthcare applications and their insurance plans, especially in the case of patient privacy, if the patient is inconvenienced.

The architecture of the system is simplified and represented in the figure b. This schematic representation of the architecture shows the processes, services and related activities that happen in the entire system. This is a consolidated representation of what happens at what point of time in which device in the system.

**Architecture**

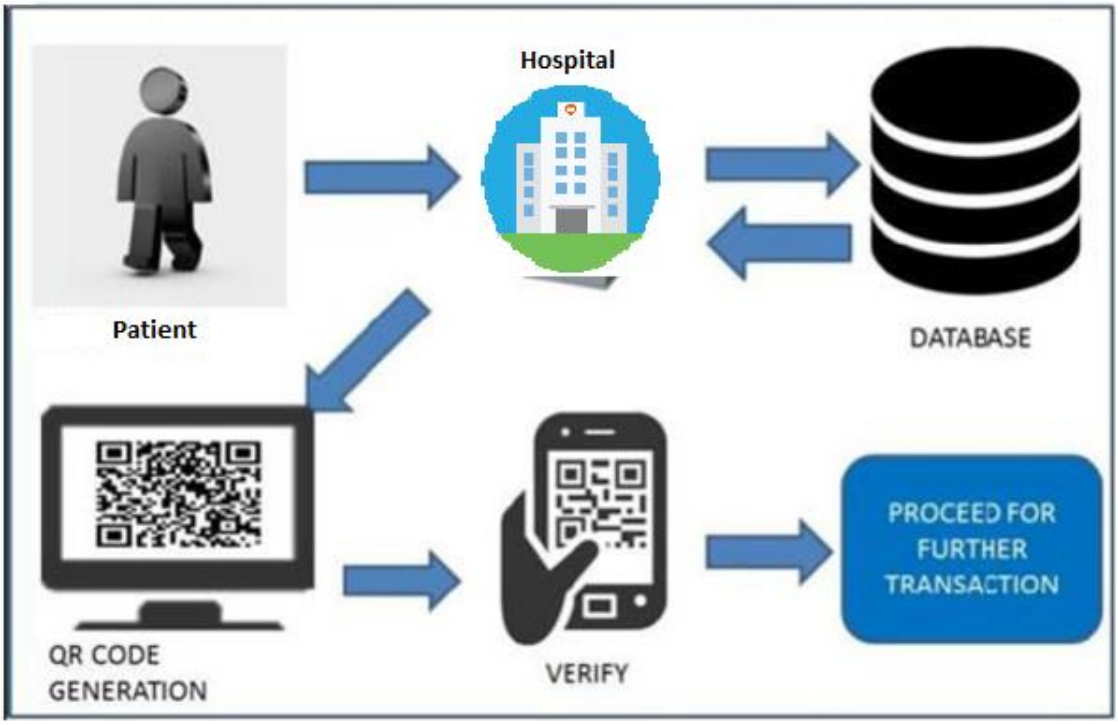



**Fig 1: System Architecture**

## 4.OBJECTIVES

Focus on improving security, protecting privacy, ensuring usability, and advancing the state of the art in QR code security technology.

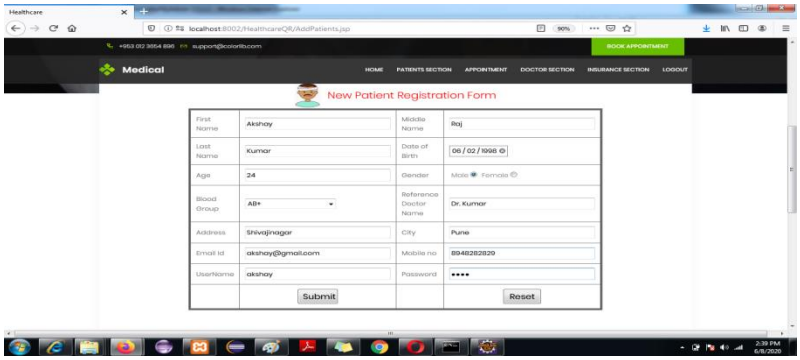
## 5.RESULTS

This paper involves dividing a secret image into multiple shares, which individually reveal no information about the original image but collectively can be used to reconstruct it. By applying this concept to QR codes, the idea is to increase the security of the encoded information.

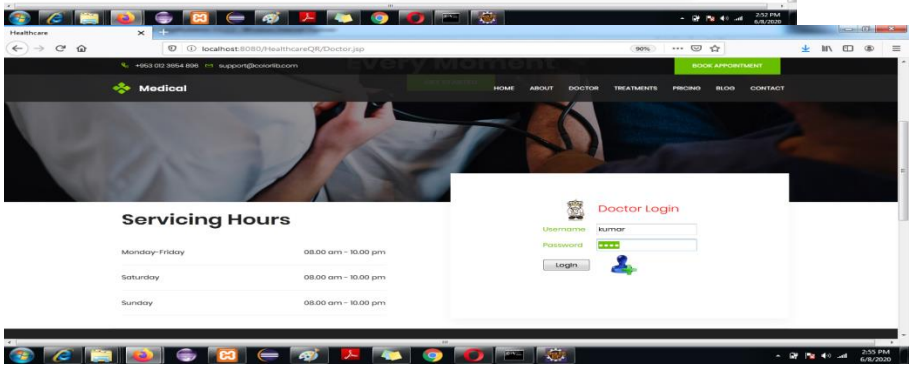
1. Generation of Shares, 2. Distribution, 3.Reconstruction ,4. Enhanced Security ,5. Application:

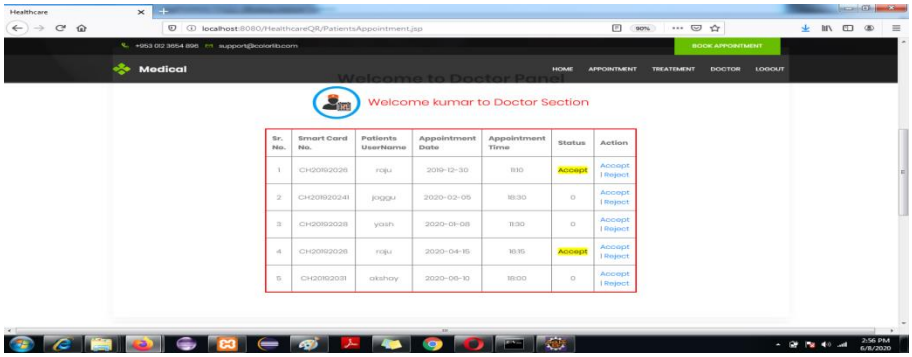
This approach could significantly improve the security of QR codes, providing a more robust method for safeguarding sensitive information encoded within them. However, practical implementation would require consideration of factors such as the number of shares needed for reconstruction, the distribution of shares, and the potential for errors or loss of shares. Additionally, ensuring user-friendliness and compatibility with existing QR code readers would be essential for widespread adoption.

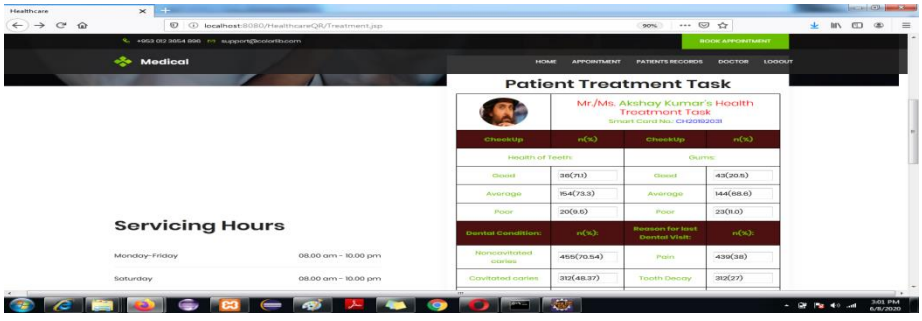
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024



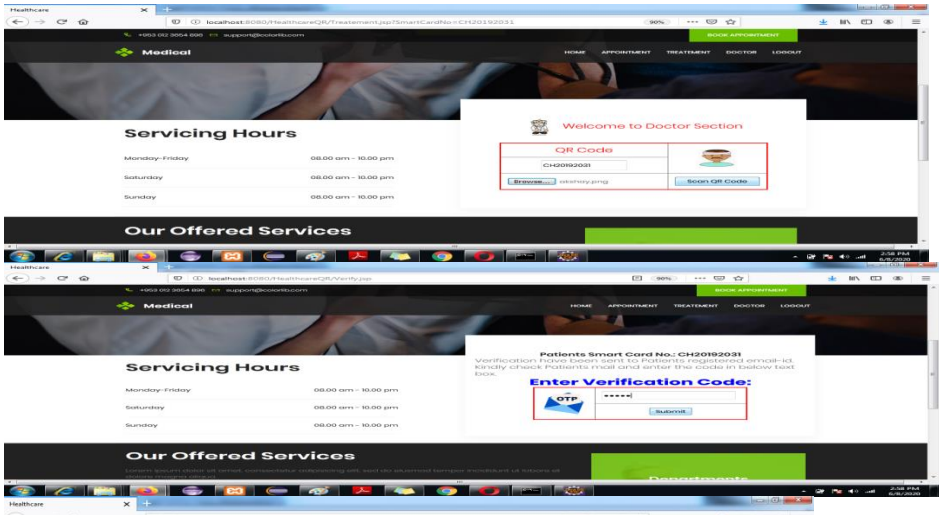




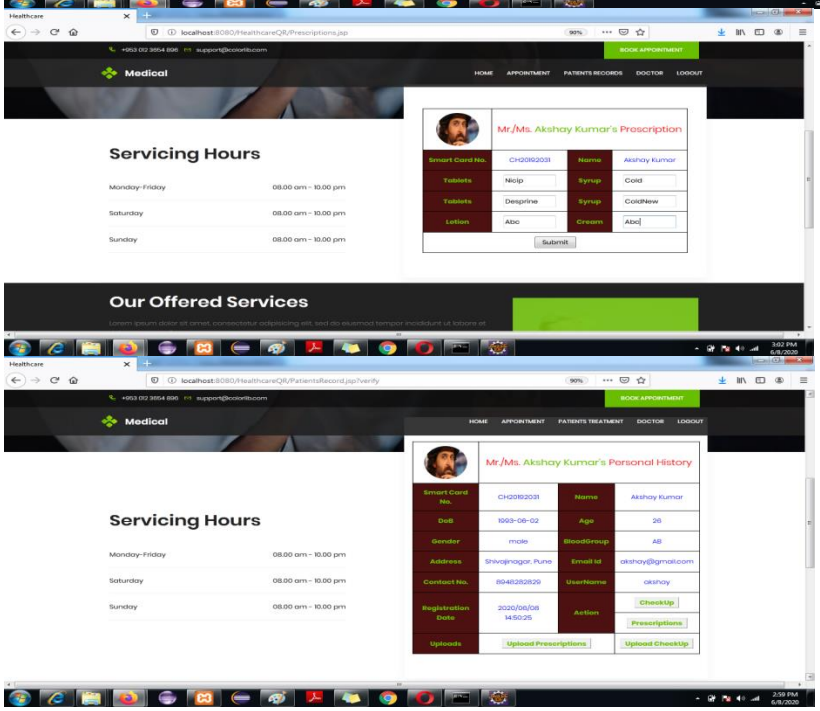



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024



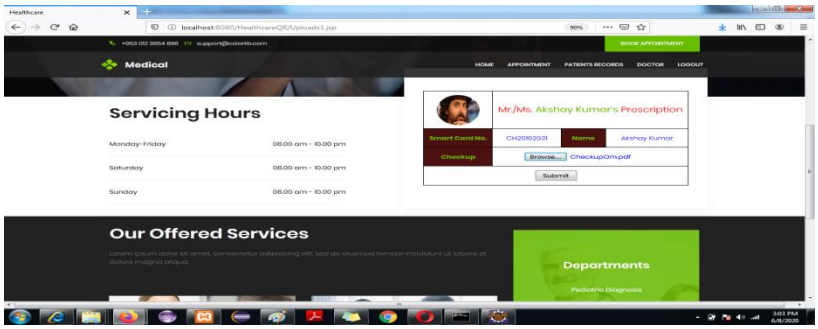




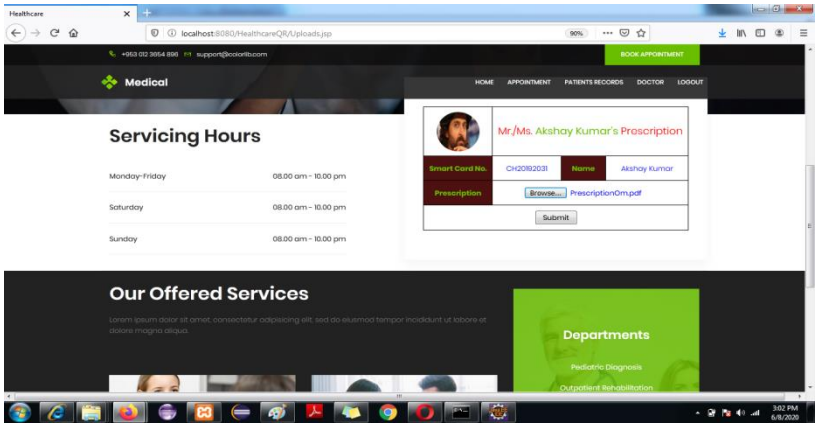








Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024




## 6.CONCLUSION

In this system we implemented In medical management, more and information technologies are applied to boost work efficiency. In this proposed system, based on the analyses of the security lacking of medical management technology, we exploit the idea of applying Quick Response (QR) code to secure medical management and boost many medical management security through make use of information security technology. Apart from saving time, the proposed solution allows for better planning in the laboratories, which are updated in time for referrals and can schedule their tasks more effectively. A fully working prototype has been designed, developed and evaluated with encouraging results. The proposed system enables better time management of the health personnel, exceeding office work is reduced and a more holistic care is provided to the patient. Overall, the operation of the healthcare unit is improved, easy integration with other healthcare facilities is enabled and functionality of the HIS is enhanced altogether.

## References

**[1]** Krzysztof Czuszynski, Jacek Ruminski, "Interaction with medical data using QR-codes", 978-1-4799-4714-0/14/$31.00 ©2014 IEEE

**[2]** Computer Engineering & Informatics Department, Paschou Mersini, EvangelosSakkopoulos, Athanasios Tsakalidis, "APPification of Hospital Healthcare and Data Management using QRcodes", Email: {paschou, sakkopul, tsak}@ceid.upatras.gr

**[3]** N. Bhuvaneswari, Latha .M, Ranjith .E; International Journal of Advance Research, Ideas and Innovations in Technology, "Doctor Patient Interaction System for Android", @ 2017, www.IJARIIT.com All Rights Reserved.

**[4]** Chen et al. BioMed EngOnLinehttps://doi.org/10.1186/s12938-019-0674-x, "Collaborative and secure transmission of medical data applied to mobile healthcare", Weimin Chen1,2 ,Zhigang Chen1* and Fang Cui.

**[5]**W. Song, Y. Lu, X. Yan, *et al.*, "Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions," *Journal of Real-Time Image-Processing*, pp.1-16, 2017.

**[6]** G. Wang, F. Liu, W. Q. Yan, "2D Barcodes for visual cryptography," *Multimedia Tools and Applications*, vol. 2, pp. 1-19, 2016.

**[7]** C. N. Yang, D. S. Wang, "Property Analysis of XOR-Based Visual Cryptography," *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 24, no. 12 pp. 189-197, 2014.

**[8]** J. C. Chuang, Y. C. Hu, H. J. Ko, "A Novel Secret Sharing Technique Using QR Code," *International Journal of Image-Processing*, vol. 4, no. 5, pp. 468-475, 2010.