Private Data Sharing and Document Authentication Using 2Level QR Code in Pathology Laboratory

S.N.Zaware[1], Mrunal Khatavkar[2], Tejal Jagtap[3],Poonam Waghmare[4]
[1, 2, 3, 4] Department of Computer Engineering
[1, 2, 3, 4] AISSMS IOIT

Abstract- *The QR code i.e. Quick Response code is mainly designed to store information. This system is designed to utilize this property of QR code but in a different manner. Pathology laboratory is a place where patient's medical reports are prepared and these reports are confidential and private which can't be accessed without authorization. In some cases where crime is done and medical reports are the only proof, in those cases confidentiality is very important. Hence this system is providing that privacy and security using 2LQR code which is made up of public and private level. Report is stored in QR code and is only accessible by lab assistant and intended doctor so that doctor can scan the QR code printed on the patient's report and verify that decoded report which can't be edited. Also it can be sent over the network by preventing from malicious attacks.*

Keywords- QR code,2LQR code, pathology laboratory, private, confidential, security,public. Malicious attacks.

I. INTRODUCTION

Current practices in almost all sectors are to secure confidential data while sending over the network. As well as to store information in secure manner and preventing it from malicious attacks are important issues now-a-days. Pathology laboratory is one of those sectors. They have to maintain privacy, confidentiality which is a daunting task. Because these labs are legally required to securely store and transmit electronic data of patients regularly. Also there are some cases in which data or report can be stolen for illegal purposes. Some crucial cases where DNA reports or fingerprint reports are very important, in those matter reports have to be very confidential and secure. Hence to improve the security methods, this system is designed.

QR code is an image of a matrix barcode that stores data in two dimensions. Data is presented in a square dots with specific pattern in both vertical and horizontal dimensions. QR scanner is a device which can read this image and retrieve the stored data based on the pattern of square dots. Denso Wave had invented QR code in 1994 by for vehicles tracking during manufacture. Several standards for data encoding in QR codes have been defined, the last standard is ISO/IEC 18004:2006 Information technology -- Automatic identification and data capture techniques -- QR Code 2005 bar code symbols specification. Now a days QR code scanners are present in smartphones. Camera in the smart phone captures an image of the QR code, then the pattern is analyzed by QR code scanner to retrieve the encoded data and display it in a useful form.

Although QR codes have many advantages, there are several security risks associated with them. Intruders can attack with the help of QR codes targeting QR scanners (smart phones) and violating users' privacy. Attackers can reach sensitive information such as: login passwords of emails and social networks, contacts information, photos, videos and banking accounts. Attackers can take full control of mobile devices, they can enable microphone, camera, GPS and even use smart phone devices in future attacks as a part of botnet or DDOS attacks.. Example of possible attacks are phishing attacks in which users are redirected into fake web sites, fraud attacks in which attackers can create fake posters and advertise for unreal commodity or special offers, malware propagation,, command injection, and SQL injection attacks. Other possible scenarios of attacks can be performed using malicious QR codes. There is increasingly important need for security and protection techniques to overcome these security threats.

The main problem of QR codes is that they are not human readable, they can only be read using specific machines i.e. scanners. And the main drawback of QR code is it is public that means it can be accessed by anyone.

The purpose of this system is mainly to enhance security and transfer data securely to only authorized user, doctor in this case. This QR code system has 2 levels that is public and private. Due to 2 levels are introduced in QR code, security is increased. In addition to it this will be helpful for patients as well as doctors that they don't have to carry hard copies of reports and no one can see or access that report unless and until they have the authority to see the report. Also for pathology lab assistants, they can transfer reports secured in QR code to patients through network.

II. RELATED WORK

This section includes papers related to secure QR code system and their advantages.

Raed M. Bani-Hani , Yarub A. Wahsheh, Mohammad B. Al-Sarhan have been proposed secure QR code system.

It uses server based security algorithm. Also it creates QR Code for Malicious Contents Isolation. This paper presents secure QR code system which is backward compatible with general QR code and useful for user's privacy and user's identity. This system introduces a little delay for user's verification and document integrity.

Modern QR code security applications have been explained by K.Saranya, R.S.Reminaa, S.Subhitsha. this paper described various applications of QR code like in Aadhar card system for identification purpose. It uses SQRC technology to securely data sharing applications.

Iuliia Tkachenko, William Puech, Christophe Destruel , Olivier Strauss, Jean-Marc Gaudin, and Christian Guichard have proposed a new developed QR code i.e. 2LQR code with additional storage capacity in which black modules are replaced with textured patterns. This paper presents 2 level QR code which has overcome the drawbacks of general QR code. It increases data storage capacity, also enhances privacy of data as well as document authentication facility. Private message sharing is the main intension of this system.

Somdip Dey,Asoke Nath and Shalabh Agarwal have implemented their security method using QR code in their college. QR code is printed on bottom of the student's mark sheets. Hence though anyone have changed the mark sheet,by scanning QR code printed on mark sheet , we can get original one. Hence frauds can be minimized.

By examining all these papers , this system have been used a new algorithm to improve system's performance related to security.

III. SYSTEM STRUCTURE

This section contains the overall structure of the system and algorithms used in the system. Also it contains flow of the system, how system works efficiently.

3.1. Overall design of the system

Proposed system is mainly designed for pathology lab assistant who is generating the report and doctor who has to verify the report. Lab assistant generates the patient's report. After successful generation of the report, assistant has to login the system. After successful login, report has to be imported into the system for generating the QR code. System has additional facility to create the report in system's software. The report should be in word format.

After successful import, QR code is generated. Data in the QR code is encrypted data and no one can decrypt it without authorization. This secure QR code is printed below the original report and this report is then handed over to intended patient.

When this report with printed QR code is seen by the doctor, doctor has to verify it's integrity and hence doctor has to scan the QR code and check whether data in QR code and report is same or not. This verification is done with authorization of doctor. For authorization, OTP is sent to mail id of the doctor after scanning QR code. After OTP verification, actual data is decrypted and data is shown to doctor and doctor can easily verify the data on report and embedded data in QR code.

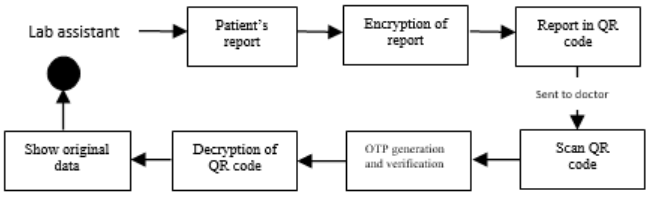


Fig. Overall structure of system

3.2. Algorithms used

In this section, we have described PSR algorithm and its working.

3.2.1. PSR algorithm:

This algorithm includes 3 phases, Positioning, Substitution and Randomization.

Stepwise procedure:

A. Positioning

1. Source file and key level has to be entered by user.
2. Key should be in range between 0-9. This condition should be satisfied.
3. Fetch a valid encryption string of alphabets from database.
4. Encrypt the Source file on basis of string accessed.
5. Generate a key for user on the basis of length of file.
6. Overall the formula for key generation will be-

$$\sum_{i=0}^{n} \text{GKey} = \sum_{i=0}^{n} (\text{Filelen} + \text{UserKey} + \text{SSymbol})$$

Where,

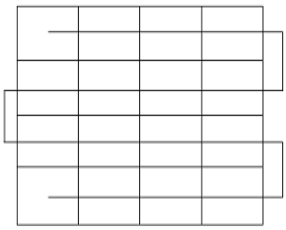
GKey=Generated key
Filelen=Length of file
UserKey=Key of user
SSymbol=Special symbol

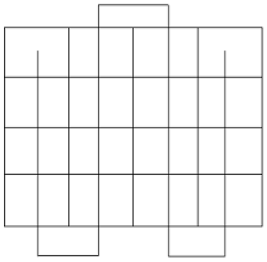
B. Substitution

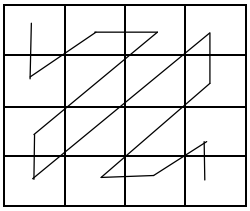
This technique is based on the shift provided by the user for replacing the character. Due to this feature more complexity gets added and it will be very difficult to attacker to find out exact logic of encryption.

1. First we have to take positional encrypted and user key
2. Then divide the file into block of 64 byte length.
3. Substitute the character on basis of shift.
4. Store it in array.
5. Use array for third procedure i.e. random pattern.

Various random patterns are like as follows:







C. Randomization

1. 64 bytes array is taken as input for this step.
2. Apply the randomized pattern coding (zigzag) to this array.
3. Combine all arrays to form a single file of encrypted text.
4. Private encryption key is generated for future use for decoding.

3.2.2. OTP generation

OTP i.e. One Time Password can be used only one time when user login to the system. That means OTP is valid for only one login session. In this system, to verify authenticated user additional security is provided in terms of OTP. While decrypting the patient's report, system sent an OTP to mail id of intended user and after successful verification, original report is seen.

This system uses TOTP i.e. Time based OTP where current time and shared secret key is used. Both server and client runs TOTP. For this server and client need to be roughly synchronized.

The current timestamp is turned into an integer time-counter. It is done by defining the start of an epoch (T0) to incrementing timestamp (TS). For example:

TC = floor((time(current) − time(T0)) / TS),
TOTP = HOTP (Secret_Key, TC),
TOTP_Value = TOTP mod 10d, where d is the desired number of digits of the one-time password.

IV. MODERN APPLICATIONS

This system has various applications especially where high rate security is needed.

In government sectors, various documents like income certificate, cast certificate, cast validity is made for individuals. However, there are many cases in which people change their certificates for gaining financial benefits. In this case this system can be implemented. If QR code is printed along with certificate, frauds will be detected immediately.

In universities, mark sheets can be printed with QR code in which whole result is embedded. Whenever there is a case in which student changes mark sheet for getting job or for other purpose, this misuse can be caught easily.

In banking, various information details like account number, passwords can be encrypted with QR code.

In various industries also, employee details, their documents can be stored in QR code hence it doesn't need to carry even hard copy also and only by scanning QR , we can get all the information about that employee.

V. CONCLUSION

This system is designed especially for security related to medical reports. The main purpose of this system is to hide patient's report and this report can easily be sent over the network without any risk.

Security and confidentiality get enhanced due to such kind of implementation. Only QR code can be sent instead of whole report. Patient only need to carry only QR code in his smartphone. And it has no chance to misplace or any third person can see it.

Data encryption algorithm has to implement this concept is based on mainly random generated key. As it is random, pattern of cipher text can't be recognized by attacker.

System can be developed further for various sectors like government, military, education sector etc. Also by including images this system can be developed. Colored QR code will be the additional attractive part for this system.

REFERENCES

[1] Iuliia Tkachenko, William Puech,"Two-Level QR Code for Private Message Sharing and Document Authentication," IEEE transactions on information forensics and security, vol. 11, no. 3, march 2016 .

[2] P. Srinivasarao1, B. Chaitanya," Data Encryption and Decryption Process using PSR Methodology and Performance Analysis with RSA" International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 3, March 2013

[3] Somdip Dey, Asoke Nath," Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System", 978-0-7695-4958-3/13 $26.00 © 2013 IEEE DOI 10.1109/CSNT.2013.112 ,2013

[4] K.Saranya, R.S.Reminaa," Modern Applications of QR-Code for Security", 978-1-4673-9916-6/16/$31.00 ©2016 IEEE

[5] Raed M. Bani-Hani, Yarub A. Wahsheh," Secure QR Code System", 978-1-4799-7212-8/14/$31.00 ©2014 IEEE

[6] Jing Yang, Yue Zhang," QR Codes and Authentication Protection", 978-1-4799-6776-6/15/$31.00 ©2015 IEEE

[7] Mona M Umaria,G.B Jethava" Enhancing the data storage Capacity in QR code using Compression Algorithm and achieving security and Further data storage capacity improvement using Multiplexing", 978-1-5090-0076-0/15 $31.00 © 2015 IEEE

[8] Ms. E.Kalaikavitha,Mrs. Juliana gnanaselvi,"Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology", Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

[9] "New Secured Steganography Algorithm using Encrypted Secret Message inside QRTM Code: System implemented in Android Phone" by Sayantan Majumdar, Abhisek Maiti, AsokeNath

[10] Zhang Yongjun,"Research and Implementation of the Optimization RS Decoding Algorithms for QR Code Decoding", 978-1-4673-0915-8/12/$31.00 ©2012 IEEE

[11] Akhil N.V Athira Vijay Deepa S Kumar," QR Code Security using Proxy Re-Encryption",978-1-5090-1277-0/16/$31.00 ©2016IEEE

[12] Trisha Chatterjee, Tamodeep Das, Shayan Dey,Asoke Nath, JoyshreeNath," Symmetric key Cryptosystem using combined Cryptographic algorithms -Generalized modified Vernam Cipher method, MSA method and NJJSAA method:

[13] TTJSAalgorithm", 978-1-4673-0126-8/11/$26.00 c2011 IEEE

[14] [ttp://www.scholastic.com/teachers/top-teaching/2012/09/ways-use-qr-codes-education

[15] http://www.uwlax.edu/urc/jur-online/pdf/2012/probst.ali.pdf

[16] http://www.educatorstechnology.com/2012/06/qr-codes-are-gaining-momentum-in-todays.html