

A Survey on Cryptography Based QR code authentication

Ronak M. Parmar¹, Krupal J. Panchal²

¹Student , Computer Engineering Department, L.J. Institute of Engineering & Technology, Gujarat, India

² Assistant Professor, Information & Technology Department, L.J. Institute of Engineering & Technology, Gujarat, India

ABSTRACT

In era of technology data security and information sharing is prime concern. Cryptography is a technique used to encrypt and decrypt information. Multiple authentication methods have been developed such smart card based system, one time password and some using biometric features. QR Code authentication technique became great tool and played an important role in the authentication process. Now these days, a QR code is applied in different application streams related to marketing, security, academics etc. and gain popularity at a really high pace. Day by day more people are getting aware of this technology and use it accordingly. The popularity of QR code grows rapidly with the growth of smart phone users and thus the QR code is rapidly arriving at high levels of acceptance worldwide.

Keywords: - QR code, QR code Authentication ,cryptography based algorithm.

1. INTRODUCTION:

The term authentication describes the process of verifying the identity of a person or entity .Using QR code for authentication is becoming quite common in recent years. QR i.e. “Quick Response” code is a 2D matrix code that is designed by keeping two points under consideration, i.e. it must store large amount of data as compared to 1D barcodes and it must be decoded at high speed using any handheld device like phones.[1]

The idea behind the development of the QR code is the limitation of the barcode information capacity (can only hold 20 alphanumeric characters). [1]

Merits of the QR code : Omni directional and Fast Scanning , Small Size, Huge Data Storage Capacity, Many Types of Data, Error correction, Direct Marking, Available for Everyone.

QR Codes are made of multiple rows and columns. The combination of these rows and columns makes a grid of modules (squares). There can be a maximum of 177 rows and 177 columns which means the maximum possible number of modules is 31,329.[7].

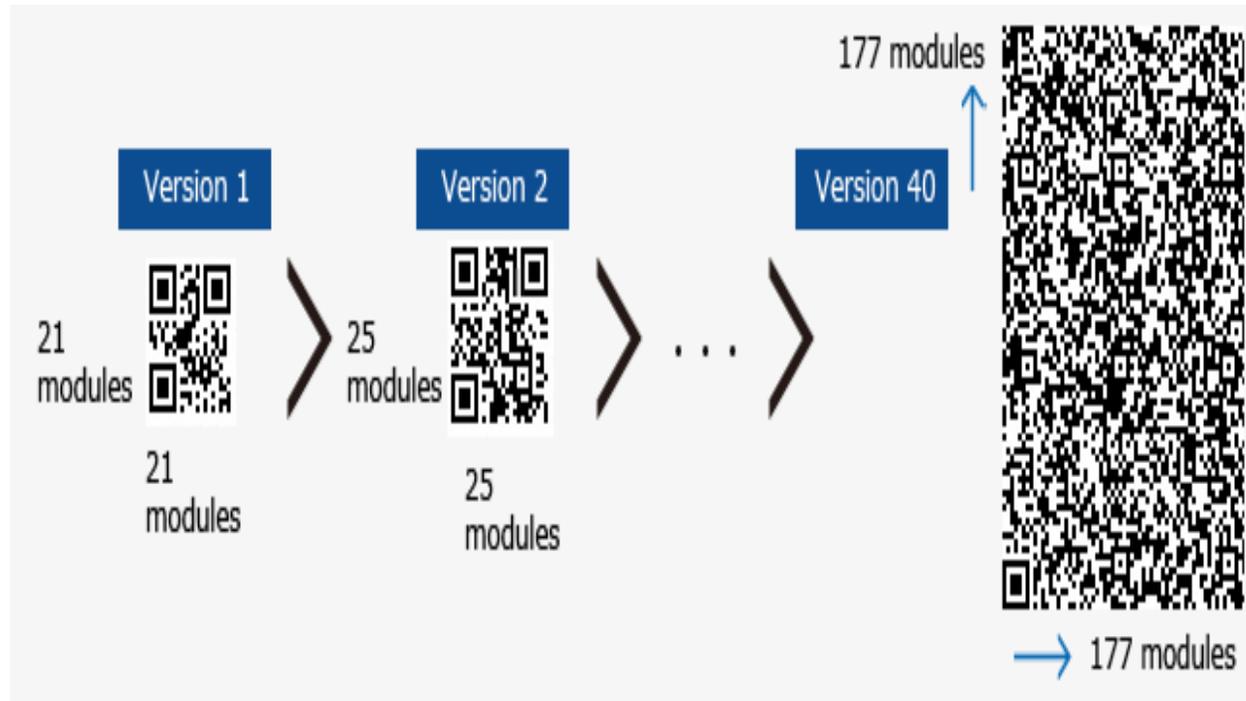


Fig.1 Versions of QR code[7]

Encrypted QR Code

Encrypted QR Code is a type of QR Code equipped with reading restricting function. This can be used to store private information and to manage a group which is capable of accessing QR Code information. Basically, an encrypted QR Code is a QR Code, which contains encrypted data. In Encrypted QR Code system, data information is encrypted by using encryption techniques and then the encrypted data is applied to the QR Code encoder (generator) which generates the QR Code. Later this QR Code is first scanned and decoded by the QR Code decoder then data information is retrieved using decryption techniques. Figure 8 show an overview of encrypted QR code mechanism.

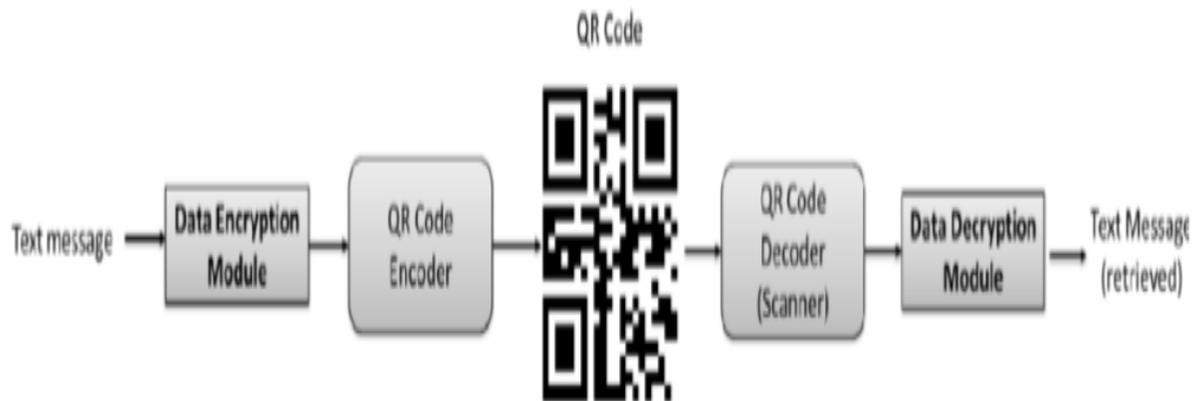


Fig.2 Concept of Encrypted QR code ¹⁷¹

2. LITERATURE REVIEW:

- In Recent years, there have been many papers published on Cryptography Based QR code authentication. QR code has emerged has a research hotspot, which is attracting researchers to contribute their work in this field. Below is the brief discussion about the methods used by different researchers for QR code authentication.

2.1 Two Factor Verification using QR-Code:A unique Authentication System for Android smart phone users.^[2]

- Brinzel Rodrigues , Anita Chaudhari, Shraddha More presented the QR based authentication system lets the user input the password,if user is authenticated then an encrypted string consisting of IMEI number of user is displayed in the form of QR code.The user uses his phone to scan the QR code and if the encrypted string is same as the IMEI number of the device the user is authenticated.

2.2 Secured Authentication using Challenge-Response and Quick-Response Code for Android Mobiles^[3].

- Ms. DhanashreePatil & Mrs. Shanti. K. Guru proposed a system leverages Optical Channel and user's cellphones to avoid password stealing attacks. Optical Channel is a safe medium to transmit information between cellphones and websites. Password is used only to access the user's mobile, and the user is authenticated without inputting any passwords to untrusted computer. In our system, each user only memorizes Open ID URL for access.

2.3 Performance Comparison between RSA and Elliptic Curve Cryptography-based QR Code Authentication^[4].

- Non Thirananant, Young Sil Lee & HoonJae Lee proposed framework mainly focuses on the use and popularity of QR Code and mobile devices. QR Code authentication increases a possibility to avoid encountering security threats with the concept "Something you have". This solution not only does provide the strong authentication method, but also in one step, giving multi-factor authentication.

2.4 QRToken: Unifying Authentication Framework to Protect User Online Identity^[5].

- Fei Xu, Sheng Han, Ying Wang, Jian Zhang, Yong Li proposed QRToken authentication framework QRToken can be used as a twofactor authentication by combine software and hardware authentication together.

2.5 Improving Fingerprint Based Access Control System Using Quick Response Code^[6].

- Xiangpeng Fu, Kaiying Feng, Changzhong Wang, and Junxing Zhang proposed to combine the one-time password (OTP) and the personalized challenge/response as the second authentication mechanism to improve the existing fingerprint based access control system.

3. COMPARATIVE TABLE:

Sr. No.	Paper Title	Method Used	Advantages	Disadvantages
1.	Two Factor Verification using QR-Code : A unique Authentication System for Android smart phone users. ^[1]	Two factor authentication	1: This paper uses the password as the 1st key of authentication and mobile phone as the 2nd key of authentication. 2: It provide security to the users against unauthorized access.	Password should be kept secure
2.	Secured Authentication using Challenge-Response and Quick-Response Code for Android Mobiles ^[2]	Challenge-Response and Quick-Response Code	The system leverages Optical Channel and user's cell phones to avoid password stealing attacks.	The Open Id Provider(OIP) will participate in the registration and login phase.The OIP is a bridge between a user and relying party.
3.	Performance Comparison between RSA and Elliptic Curve Cryptography-based QR Code Authentication ^[3]	QR code authentication	Efficient way in QR code authentication which provide strong security.	The number of characters is directly proportional to the time it takes to encode and generate QR code.
4.	QRToken: Unifying Authentication Framework to Protect User Online Identity. ^[4]	Two factor authentication	This framework supports QRToken both as a software application and as a hardware device.	Two time generation of QR code makes it complex
5.	Improving Fingerprint Based Access Control System Using Quick Response Code ^[5]	Three factor authentication	QRToken has the advantages of secure , convenient , money saving and easy to use.	The system may not scale well when the amount of users reaches a threshold.

Table -1: Comparative Table**4. CONCLUSION:**

This paper presents a comprehensive and state-of-the-art survey of Cryptography Based QR code authentication. The use of the QR code makes it difficult to be accessed modified and copied and it can be applied to many services that require authentication

5. REFERENCES:

- [1] Sumit Tiwari, "An Introduction to QR Code Technology", *IEEE International Conference on Information Technology*, 2016. doi 10.1109/ICIT.2016.38
- [2] Brinzel Rodrigues, Anita Chaudhari, Shraddha More. "Two Factor Verification using QR-Code: A unique Authentication System for Android smart phone users.", *IEEE 2nd International Conference on Contemporary Computing and Informatics*, 2016, pp.457-462.
- [3] Ms.Dhanashree Patil , Mrs.Shanti.K.Guru. "Secured Authentication using Challenge-Response and Quick-Response Code for Android Mobiles", *IEEE 2014*. ISBN No.978-1-4799-3834-6/14.
- [4] Non Thirananant, Young Sil Lee, HoonJae Lee. "Performance Comparison between RSA and Elliptic Curve Cryptography-based QR Code Authentication" *IEEE 29th International Conference on Advanced Information Networking and Application Workshops 2015* .doi 10.1109/WAINA.2015.62.
- [5] Fei Xu, Sheng Han, Ying Wang, Jian Zhang, Yong Li. "QRToken: Unifying Authentication Framework to Protect User Online Identity" *IEEE 2nd International Conference on cyber Security and Cloud Computing 2015*, doi 10.1109/CSCloud.2015.24
- [6] Xiangpeng Fu, Kaiying Feng, Changzhong Wang, and Junxing Zhang. "Improving Fingerprint Based Access Control System Using Quick Response Code ", *IEEE 2015*, ISBN No:978-1-4799-6092-7/15/.
- [7] <http://www.qrcode.com/en/about/version.html>, 29/09/2017, 5.10 PM.