Secure QR Code Scheme Based on Cryptography

Gayathri.M[1], Yogasabari.V[2], Mrs.R.Aishwarya[3]

[1, 2, 3] Dept of Computer Science and Engineering

[1, 2, 3] G.K.M College of Engineering and Technology, Chennai, TamilNadu, India

Abstract- *A QR codes are being used increasingly to share data for different purposes. In information communication, QR code is important because of its high data capacity. However, most existing QR code systems use insecure data format and encryption is rarely used. A user can use secure QR code technology to keep information secured and hidden. This paper describes an implementation of secure QR code based on cryptography. While square bar-codes can be convenient, they can also be dangerous. According to the FBI, cyber-criminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data and embedding malware to gain access to the victim's device. we proposed a secure QR code system which will allow sharing authentic personal confidential information by means of QR code verification using RSA algorithm and also allow authorizing the confidential information by means of QR code validation using RSA public key cryptographic algorithm.*

Keywords- Cryptography, decryption, encryption, QR code, secure, RSA

I. INTRODUCTION

QR codes are popular, especially during these times with the covid-19 pandemic. These QR codes are the new normal of information exchange since they allow virtual communication, which is much-needed these days. However, considering the security risks involved, ensuring privacy and security while using these QR codes is best. At present, personal information confidentiality is done by the person’s own manual unsecured way and there are chances that the information is not completely secured and hidden. Researchers have proposed to use TTJSA algorithm and Advanced Encryption Standard (AES) algorithm for legal document data hiding, message hiding, etc. However, these methods do not consider cases when personal confidential information needs to be shared securely.

The popularity of QR code is because of its high data capacity, error correction capability using Reed-Solomon error correction algorithm, fast decoding,etc. However, most existing QR code systems use insecure data format and encryption is rarely used. It is possible to use secure QR code technology to keep his important sensitive information perfectly secured at all times, without the information getting leaked to outside world, the Cryptographic algorithms can be used to make a QR code system secure.

II. RELATED WORK

S. Khairnar [1] proposed a method, Anti-Phishing framework based on Extended Cryptography and QR code and to solve the problem of phishing and done the relevant validation.

Mamtha Shetty [2] proposed a method, Hiding of Confidential Data and its Retrieval using Advanced Algorithms and QR Authentication system, for confidential encrypted data hiding in QR code using TTJSA encryption algorithm.

Nikita Gupta, Nagesh Mokashe and Mangesh Parihar [3] proposed a method, QR code: A safe and secure method of authenticating legal documents, to detect forgery of data and ensure the authenticity of data using AES algorithm.

T.Satyanarayana , and G. Swathi [4], proposed a method, Secure QR Code for Anti-Phishing System Using Mobile, to provide scalability, flexibility for secure communication between mobile device and un-trusted computer.

Zhengxin Fu, Yuqiao Cheng, Bin Yu [5], proposed a method, Visual Cryptography Scheme With Meaningful Shares and each share is meaningful and can be read by any standard QR code reader.

Ching-Nung Yang [6], proposed a method, Property Analysis of XOR-Based Visual Cryptography and easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS.

A sankara Narayanan [7], proposed a method, QR code security and analysis solution and fast scanning and provide helps.

Rutuja kakade, Nikita kasar, Shruti Kulkarani [8], proposed a method, Image steganography and data hiding in QR code and Provides security to criminal data from authorized access and tampering.

D.Sugumaran, D.Anandan [9], proposed a method , SECURED DOCUMENT GENERATION USING QR CODE AND VSS and Improves the quality of the share images, this avoids the generation of forged documents

III. PROPOSED SYSTEM

A. Overview of Proposed System

In this section, we will introduce our secure QR code scheme. In order to secure the QR code information, we proposed an improved RSA encryption technology based on the existing encryption technology to realize the concealment of the QR code pattern. Through this method of encryption, the information hidden in QR code is more difficult to be accessed by forgers. So as to achieve the purpose of hidden information more secure.

B. **Login Module**

The Login Module is a portal module that allows users to type a user name and password to log in. Administrator and user have to login before they can access the functionalities of the system.

C. RSA Key Generation Module

RSA is asymmetric encryption, in which a key needed to encrypt data is made public, but the corresponding key needed to decrypt it is kept private, for example in a file on the server to which clients connect. These keys are stored as XML format in the server machine.

Steps in RSA Algorithm:

Choose two large prime numbers (p and q)
Calculate n = p*q and z = (p-1)(q-1)
Choose a number e where 1 < e < z.
Calculate d = e-1mod(p-1)(q-1).
You can bundle private key pair as (n,d).
You can bundle public key pair as (n,e)

D. QR Code Generation Module

The module refers to the black and white dots that make up QR Code. To create a QR code is we first create a string of data bits. This string includes the characters of the original message (encrypted message in this case) that you are encoding, as well as some information bits that will tell a QR decoder what type of QR Code it is. QR code generation is preceded by some valuable parameter settings like error correction level, version, etc.

E. QR Code Decoder:

Each QR code consists black squares and dots which represent different pieces of information. When scanned, the unique pattern on the bar-code translates into human-readable data. This transaction happens in seconds. The decoder first decodes Secure QR Code to generate the encrypted form and then, uses decryption to get the confidential information.

F. QR Code Verifier

After creating your code, you will need QR code verification (also known as QR code check). These codes are required to be measured in several ways, including the corner finder patterns, alignment patterns, and clock tracks, as well as several checks in the data region. It verifies a QR code to see whether the QR code is genuine, which means the personal information is confidentially shared. In the background, we used RSA digital signature scheme for that kind of verification process. QR code usage is increasing rapidly now-a-days.

G. QR Code Validator

This component validates a QR code to see whether the QR code is valid, i.e., the personal confidential information is authorized and the personal information is confidentially hidden. The purpose of this QR Code on certificate is to validate/verify it anytime by anybody.

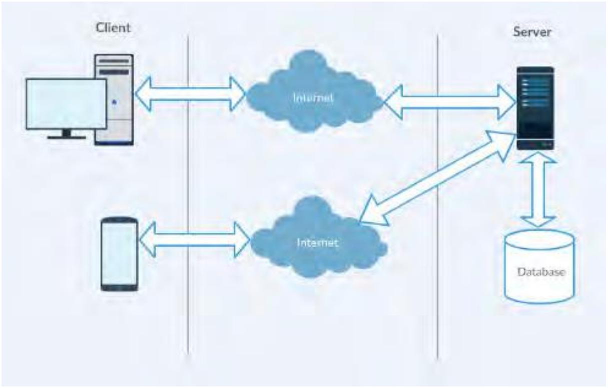
H. Contact Us Module

The Contact module allows site visitors to send emails to other authenticated users and to the site administrator.

IV. IMPLEMENTATION

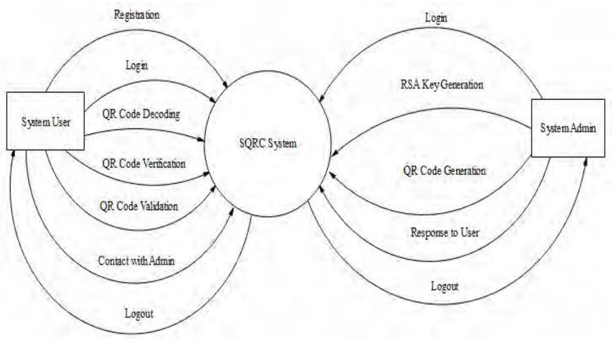
The proposed scheme is a strategic combination of QR code with RSA algorithm. This system focused on enhancing the security requirements by using QR code with RSA algorithm.It maintains key generation QR code generation as well as the system validates an encrypted QR code using the RSA Public Key Cryptography mechanism to check whether the personal confidential information in the encrypted QR code is valid. The client side (Third Party) of the application consists of the web application along with the mobile responsive feature. The web application contains a QR code validation and verification process in terms of personal confidential information validation and verification.

system architecture



the client server architecture diagram of proposed Secure QR Code System. It contains three tiers: Tier 1(presentation/user layer lies on client side), Tier 2 (application/business layer lies on web server side) and Tier 3 (data layer lies on database server side). During an application's life cycle, this three-tier approach provides benefits such as re-usability (can share and reuse the components and services), flexibility (because each tier can be managed or scaled independently, flexibility is increased), manageability, maintainability (because each tier is independent of the other tiers, updates or changes can be carried out without affecting the application as a whole), and scalability.

Context Diagram for proposed system



V. TESTING

Generally, tests were done against functional and non-functional requirements of the application following the test cases. Testing the application again and again helped it to become a reliable and stable system.

Compatibility Test

The web application was tested with different windows operating system (versions) and different web browsers respectively. This test was for compatibility for computer operating systems and mobile responsive issues.

Web Browser Compatibility Test

Web Browser	Compatibility
Google Chrome	Yes
Firefox	Yes
Internet Explorer	Yes

Mobile View Compatibility Test

Mobile	Compatibility	Device Used
HTC Desire 828	Yes	HTC (Android 5.1 Lollipop) Phone
Nokia Lumia 525	Yes	Nokia (Windows 8.1) Phone
Galaxy S5	Yes	Google Chrome Developer Device Tool
Nexus 5X	Yes	Google Chrome Developer Device Tool
Nexus 6P	Yes	Google Chrome Developer Device Tool
Galaxy Note 7	Yes	Google Chrome Developer Device Tool
Microsoft Lumia 950	Yes	Google Chrome Developer Device Tool
Nokia Lumia	Yes	Google Chrome Developer Device Tool
LG Optimus	Yes	Google Chrome Developer Device Tool
Nexus 7	Yes	Google Chrome Developer Device Tool

Validation Test

Validation was performed to check whether the developed web application solves the challenges for authenticity and confidentiality of personal sensitive information. Validation was done in order to make sure whether the implementation focused on the main features and functionality as far as hiding personal confidential information is concerned.

VI. ADDITIONAL WORK

Improving Readability

The length of the QR message is dictated by the length of the hidden message. What this means is that the hidden message cannot ever exceed the length of the actual QR message, and therefore the QR message must be long enough to accommodate this. If the digital signature can be embedded in the QR code with a smaller byte footprint, both the hidden message and QR message could be shortened, potentially increasing the readability of the secure QR codes.

Error Correction

In order to verify a particular QR code, the entire code must remain completely intact. This is an unfortunate side-effect from the implementation's abuse of the pre-existing error correction functionality of the standard QR code. On a positive note, the standard message will still remain intact as long as the combination of the obstruction and the previously corrupted portion of the code used for the hidden message do not take up more than 30% of the QR code data area. Implementing another error correction feature, such as parity bits, in the hidden message could compensate for any unintentional flaws. This would require the hidden messages to be longer.

VII. CONCLUSION & FUTURE WORK

This paper presents a designed and implemented a Secure QR Code scheme for securing the QR code information with the help of RSA cryptographic algorithm. It replaces sensitive information on paper documents with encrypted QR codes. The Secure QR Code system can be applied to a range of real-world applications that involve sensitive information sharing.

Our proposed system is fairly targeted to the web-based solution even though it has mobile view responsiveness. So, in future, this system can be developed as a mobile based application to meet the expectation of the mobile community and current technology trends.

REFERENCES

[1] Dey, S., Nath, A., Agarwal, S., "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System"
International Conference on Communication Systems and Network Technologies, DOI 10.1109/CSNT.2013.112, 2013

[2] Shetty, M., "Hiding of Confidential Data and its Retrieval using Advanced Algorithms and QR Authentication system", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676, p-ISSN: 2320-3331, Volume 9, Issue 6 Ver. II, PP 01-05 www.iosrjournals.org, Nov – Dec. 2014

[3] Gupta, N., Mokashe, N., Parihar, M., "QR code: A safe and secure method of authenticating legal documents", International Journal of Engineering Research and General Science Volume 3, Issue 1, ISSN 2091-2730, January-February, 2015

[4] Bhavar, S., Jadhav, J., Kulkarni, N., Patil, K., "Authenticate Message Hiding in QR Code Using AES Algorithm", International Engineering Research Journal (IERJ) Volume 2 Issue 1 Page 367-369, ISSN 2395-1621, 2016

[5] Satyanarayana1, T. Assoc. Professor, Swathi2, G., "Secure QR Code for Anti Phishing System Using Mobile", International Refereed Journal of Engineering and Science (IRJES) ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 2, Issue 12, PP.78-81, December 2013

[6] "QR Code Tutorial", http://www.thonky.com/qr-code-tutorial/ [last accessed on 07-12-2016

[7] "SQRC (Secret-function-equipped QR Code)", https://www.denso-wave.com/en/adcd /product/software/sqrc/sqrc.html [last accessed on 04-12-2016.

[8] Electronic Signatures in Global and National Commerce Act. the U.S. Government Printing Office, 2000.

[9] BOBMATH. QR format information, 2011. [Online; accessed March 17, 2017].

[10] DENSO WAVE. QR Code, howpublished = "http://www.qrcode.com (Retrieved: 3/16/2017)", journal=DENSO WAVE.

[11] KIESEBERG, P., LEITHNER, M., MULAZZANI, M., MUNROE, L., SCHRITTWIESER, S., SINHA, M., AND WEIPPL, E. QR code security. Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia - MoMM '10 (2010). .

[12] KOKALITCHEVA, K. Here's a secret secondary use for snapchat, May 2016.

[13] MASLENNIKOV, D. Malicious QR codes pushing android-malware.https://securelist.com/blog/virus watch/31386/malicious-qr-codes-pushing-androidmalware/(Retrieved: 3/16/2017), Sep 2011.