ISSN 2395-1621

Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System

[#1]Nikhil Nakhwa, [#2]Tushar Khude, [#3]Shashikant Dighe, [#4]Shankar Kate.

[1]niknakhawa@gmail.com
[2]tkhude10@gmail.com
[3]Shashidighe7@gmail.com
[4]Shankarkate101@gmail.com

[#1234]Department of Computer Engineering

Savitribai Phule Pune University
Navsahyadri Edu. Soc. Pune.

ABSTRACT

The QR code is Quick Response code. QR code authentication system is an open source and proof-of-concept authentication system. it use two-factor authentication technique. It combines a onetime password and QR code scanning by using camera-equipped mobile phone. QR is extremely secure for storing all the sensitive information and transmitted it as in encrypted form; still it is very easy to use and cost efficient technique. The system uses QR codes which are small two dimensional code. It en-code digital data. This system can be used for all hardware platforms that are for tablets, personal computers, laptops, camera equipped cell phones. The System will automatically generate User ID and Transaction ID for identification of user by scanning. We can read QR code even if it is partially damage. It provides high level of security and authentication with u n trusted devices. Due to these features of QR code the system can be used for various critical transactions .As a high-speed internet infrastructure is being developed and people are informationized, the financial tasks are also engaged in internet field. However, the existing internet banking system was exposed to the danger of hacking. Recently, the personal information has been leaked by a high-degree method such as Phishing or Pharming beyond snatching a user's ID and Password.

ARTICLE INFO

Article History

Received: 27th May 2016

Received in revised form :

27th May 2016

Accepted: 29th May 2016

Published online :

30th May 2016

Keywords: **Internet Banking, Security Standards, Contingency Strategies.**

I. INTRODUCTION

The Online banking is one of the most sensitive tasks performed by general internet user. Most traditional banks new offer online baking with 'peace of mind'. Although the banks heavily advertise a apparent '100% online security guarantee', typically the fine print makes this conditional a user fulfilling certain security requirements . The number of the users of the domestic banking system has-been increased steadily in the first quarter of 2009. The average usage of the service per day was 26,410,000 while the amount of dealings went beyond 26 trillion 950 million won. However, recent banks are becoming increasingly reluctant to reimburse user who fall prey to online scams such as phishing or a pharming. The first hacking incident in Korea in 2005spurred the FSS (The Korean Financial Supervisory Service) to announce a comprehensive countermeasure. One of the countermeasures that draw high attention of the financial agencies is OTP (One Time Password), one of the user confirmation methods is introduces, and Joint Confirmation Centre of OTP is established . The Online financial transaction in the present is apply a security card and public key certificate which are the methods confirming a user, and recently OTP was newly introduced. One-Time Password is a password system where passwords can only be used once and the user has to be authenticated with a new password key each time. This guarantee the safety even if an attacker is tapping password in network or a user loses it. Besides, OTP features anonymity, portability, and extensity, and enables to keep the information from being leakedts advantages made QR code very powerful and popular in security and advertisement industry.

II.REALEATED WORK

In 2002, Clarke et al. were probably one of the first to suggest the usage of camera-based devices as an alternative, more secured authentication method for critical transactions,

such as banking operations, and most particularly when connecting from untrusted computers [1]. Nowadays camera equipped smart phones around us are increasing so rapidly that mobile based authentication might become a popular method to authenticate in a short time. In traditional Barcode data capacity is around the only 16 digit. QR Code has more Data Capacity. It has Numeric Code = 7,089 characters max and Alphanumeric code = 4,296 characters max.

Fig 1 Comparisons of QR and Barcode QR codes

(Quick Response codes) were introduced in 1994 by Denso-Wave , a Japanese company subsidiary of Toyota. Initially, these codes where conceived as a quick way to keep track of vehicle parts, being nowadays extremely popular in Asian countries like Japan, South Korea, China or Taiwan and becoming more and more popular in western countries by the day. At this point, we can implement the authentication using the QR code for all platforms such as PC, tablet and mobile phones. We get the idea from the paper, related to our project and we use two factor authentication. Also by using this project we can replace the demand draft and cheque by Cash Card..

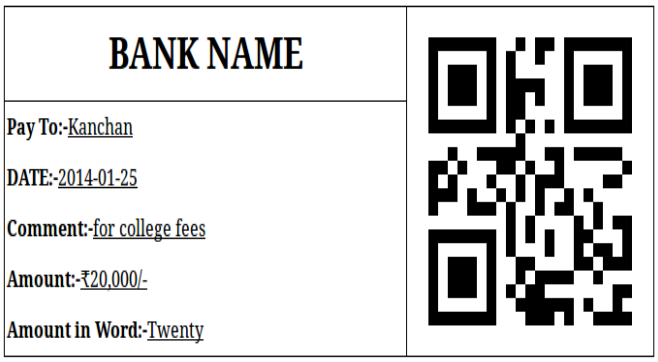

Fig 2 QR code data

A. Creation

Creation module contains User information and system generated information. For sign up process User must enter his naming details, address and valid mobile. The valid mobile is mandatory for user.After entering the naming details by the user according to the system will generate automatically unique QR code to the mobile. After the scanning of QR code and reentering QR image the the Transaction will successful.

B. Authentication

In order to provide same level of security as a web application, the system shall provide login screen on the user's hardware device. The login entered by the user will be user ID, password and scan the unique QR code. After matching the user ID, password and QR code will be sent on user's correspondence number, then QR image was re-entered by user.The values will be verified by the system prior the user having access to the system.

C. Transaction

Transaction can be done in two modes, by using Direct Transfer and by using Cash card.

a) Transfer:-In this mode we select Direct Transfer mode. Then user has to add how much Amount to be transfer and the comment that will be the reason for why to transfer that amount should add in that transfer mode. Then QR code will be scanned if it matches then only transfer will do successfully.

b) By Using Cash Card:- Instead of Demand Draft and Cheque we can use the Cash Card. In this mode we select pay to, amount pay to and comment that will be the reason for what to pay. System will genereate, Unique QR code for Cash Card ,that QR Code will be scanned ,if it matches then only transfer .

III. DATABASE ENCRYPTION

One of the major security holes in many critical systems is database security. Though attacker gets invalid access to database, one more level of security can be added by encrypting database. While displaying contents we'll decrypt data and send it to user. Any of the available encryption algorithms can be used but as there will be many database requests for banking application, encrypting-decrypting every time might put large overhead on the application. So care should be taken to choose an algorithm which would provide sufficient security with little overhead. Base-64 is one of the choices. Algorithm converts data in byte-code. Standard data representation is of 8-bits. We can take 6-bit groups and convert them into characters and replace the original data. Padding can be added in the end of data if necessary. It would represent data by 2^6=64 possible characters, so named base-64. long with security, another advantage of base 64 is that many internet system don't allow all 128 characters in 8-bit representation so, base-64 can be beneficial.

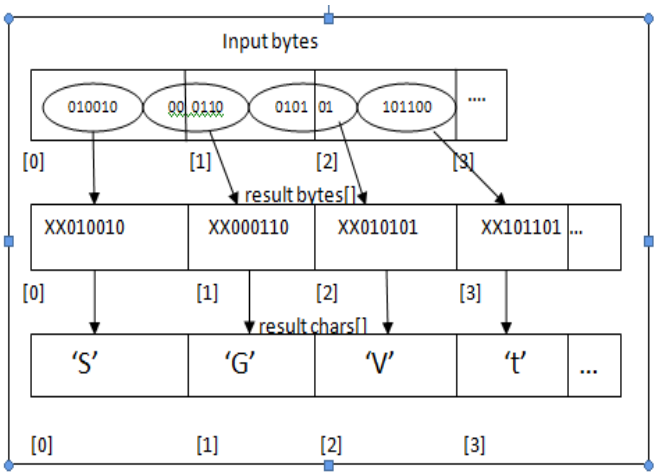

Fig.3. Base-64 working

Secure Communication Channels:

As important as application security, secure communication channels also of equal importance. Most promising way to do this would be use of digital certificates using PKI architecture for application. PKI provides an additional encryption and signature. HTTPS communication can be used for this purpose. It embeds HTTP data in SSL (Secure Socket Layer) packets. SSL group data into small chunks compresses them and then encrypts using asymmetric keys . Asymmetric keys provide high level of security for communication as one key is used for encryption and another for decryption. For management of keys, digital certificates are used which legitimate documents are provided by certification authority (CA) containing user information and keys. For asymmetric key generation, RSA (Rivets-Shamir-Adelman) algorithm is used. Public keys are embedded in digital certificates of each end. Data is sent by encrypting it with public key of receiver but can be decrypted only with private key of receiver which is kept secret, thus providing high level of security

QR-code processing: The features of this code symbol are large capacity, small printout size and high speed scanning. QR code comprised of following patterns:

finder pattern, timing pattern, format information, alignment pattern, and data cell.

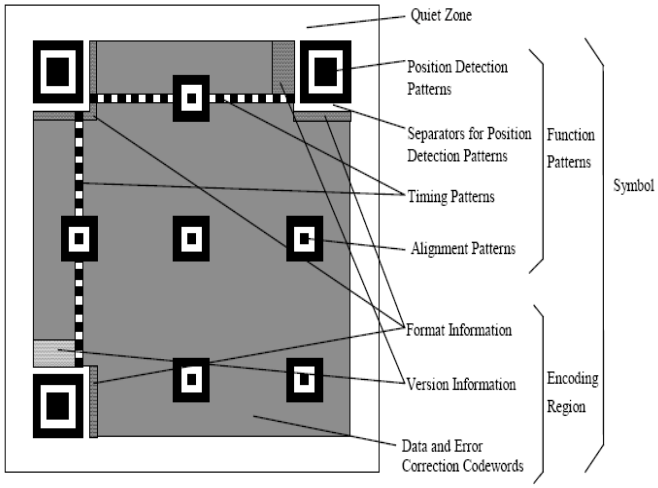

Fig. 4. Structure of QR-code

Use of QR code ensures that data will be decoded by legitimate user only as decoding device will be required to decode it.

QR-code is generated using transaction information, timestamp, random number using following steps[5]:

(I)Conversion into binary format: First we select mode in which QR-code to be generated depending on type of data: Extended Channel Interpretation (ECI) Mode 1.Numeric Mode

2. Alphanumeric Mode 3.8-bit Byte Mode

4.Kanji Mode Each of the modes has got different conversion functions to convert data into binary format. (II)Appending error correction codewords: Divide the codeword sequence into the required number of blocks to enable the error correction algorithms to be processed. Generate the error correction codewords for each block, appending the error correction codewords to the end of the data codeword sequence.on of the 4 levels of error recovery(L,M,Q,H) is chosen to generate codewords. Data blocks are arranged into QR-code according to chosen strategy: either into rectangular blocks or irregular blocks which can accommodate more data.

(IV)Masking: Data is XORed with predefined bit-string to encode, for dark and light modules to be arranged in a well-balanced manner in the symbol.

(V)Appending format information: The Format Information is a 15 bit sequence containing 5 data bits, with 10 error correction bits calculated using the (15, 5) BCH code. (VI)Appending version information: The Version Information is an 18 bit sequence containing 6 data bits, with 12 error correction bits calculated using the (18, 6) BCH code. For error detection and correction "reed-soloman" codes of data are also embedded in QR code. It gives error correction up to 30%.The generator polynomial g(x) is defined by having α, α2, ..., αt as its roots, i.e., .

g(x)=(x-α)(x-α2)….(x-αt)=g0+g1x+……+gt-1xt-1+xt The transmitter sends the N − 1 coefficients of S(x)=p(x)g(x), and the receiver can use polynomial division by g(x) of the received polynomial to determine whether the message is in error; a non-zero remainder means that an error was detected. Let r(x) be the non-zero remainder polynomial, then the receiver can evaluate r(x) at the roots of g(x), and build a system of equations that eliminates s(x) and identifies which coefficients of r(x) are in error, and the magnitude of each coefficient's error.

IV. SCANNING OF QR-CODE

The processing of QR-code detection consists of five procedures starting from image captured from camera to data extraction. Thing that makes this task challenging is that captured image may not be of good quality or might be deformed either by limitation of device or naïve user.

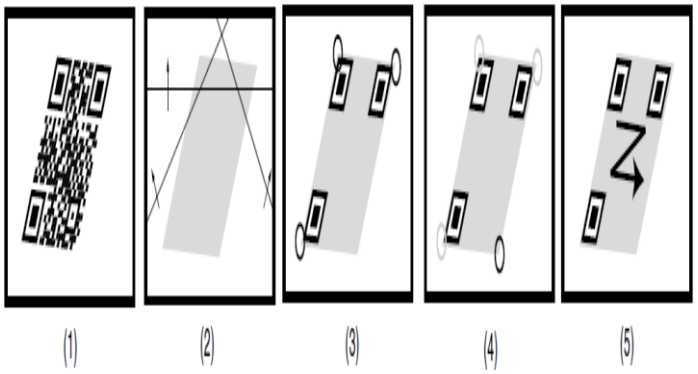

Fig. 5. Steps in QR-code scanning

Scanning can be done by using following five steps:

(I)Pre-processing: The gray level histogram calculation is adopted.

(II)Corner marks detection: Three marked corners are detected using the finder pattern.

(III)Fourth corner estimation: The fourth corner is detected using the special algorithm.

(IV) Inverse perspective transformation: Inverse transformation is adopted based on the obtained corner geometry positions to normalize the size of the code.

(V) Scanning of code: Sample the inside of code and output the normalized bi-level code data to host CPU. The input image has a deformed shape because of being captured from the embedded camera device, and we use the inverse

perspective transformation to normalize the code shape. This equation is shown as follows:

u =c0x+c1x+c2

c6x+c7y+1

v =c3x+c4x+c5

c6x+c7y+1

Where u, v coordinates is original image coordinate which is deformed and x, y coordinate is the normalized coordinate. In the above equations, coefficients c0 ∼c7 can be obtained from the following four point pairs,

(C) QR-code decoding: QR-code is encoded with encryption key, which is then decoded by private key at user and data is obtained. Decoding would be the exact opposite of the encoding scanning different sections according to format of QR-code, checking data with error correction codes, recovering lost data from redundant locations is done while decoding

A(x0, y0) ⇔A_ (u0, v0),

B(x1, y1) ⇔B_ (u1, v1),

C(x2, y2) ⇔C_ (u2, v2),

D(x3, y3) ⇔D_ (u3, v3)

Random number is matched with the number sent along with the message and if they match, message is valid. Time stamp is read from the message to get synchronized with the server. From information in QR-code like TI and T and imei-number of the mobile device, OTP is generated in the device and displayed to user. User then will enter it into desktop application and is sent to CA where also OTP for current transaction is generated and matched with the one sent by user application. If they are same transaction is completed. Other functionalities required by any banking application should be added into the applicant like user registration, managing user accounts, viewing transaction summary, etc. and application confirming authentic, secure transaction, storage and communication can be developed.

Advantages of QR code

- QR code is two dimensional and readable at any direction.
- Storage capacity of QR code is up to 4,296 alphanumeric characters.
- It is readable if they are partially damage.
- It is easy to scan with camera based device.
- QR codes are not readable by person.
- QR code can stores data which is stored in one dimensional bar code in one-tenth the space.
- QR code is providing information correctly if it is damage up to 30%.
- It can handle many types of data like numeric,

Disadvantages of QR code

- It is only readable by the machine

V. ONLINE AUTHENTICATION SYSTEM

First IMEI number and random number are encrypted using the public key. This encrypted string generates the QR code using the QR code generation function which is present in java. Now this QR code image is display on the client machine. User scans this QR code using mobile phone. After scanning, in online mode means net is available on phone the generated string (IMEI number and random number) is automatically get entered into the login page. After successful login the home page of the bank is get open. So in our system there is no need to remember the password that is combination of your IMEI number and the random number. The servers decrypts the string using the user public key and verifies that a row exists in the transactions table with our random number, and then
update the row of transaction table. The server checks then that the IMEI is correct or not and assigned that IMEI to the correct user. If the login is get successful the transaction row is deleted. It means every time the generated QR code image is different. Now the PHP session is created and when user gets logoff the session is destroyed.

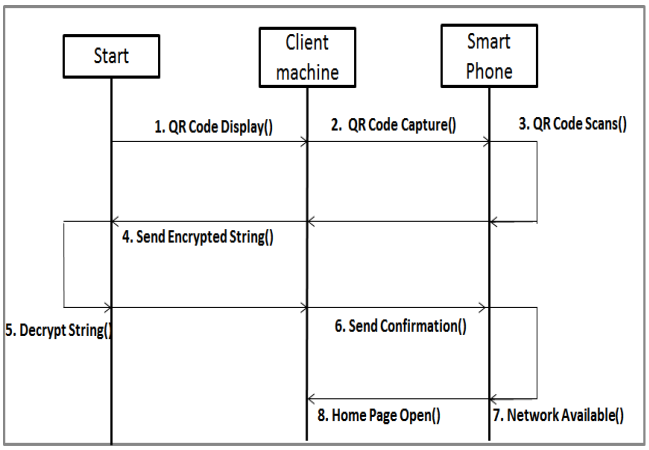

Fig. 6 Working Of or Authentication.

VI. SECURITY

In our system the security is more powerful because of the QR code and encryption algorithm. A man-in-the middle attack is not gets successful in our system because communication between the server and user is always encrypted. User name is not gets reuse or copies because user name is get deleted after the user log out. For mobile application person also need the password so there is no way for any attack because the file is not easily accessible and it is encrypted. If the untrusted person knows how to handle the internal storage then only the security problem is created. A phishing attack on the mobile phone is possible by replacing the application by another application. And the password is also get covered but without the certificate it still not possible. Another security part is timestamp, if user not able to login in given timestamp then login is not

VIII. FUTURE SCOPE

When user uses the mobile application the user need to enter the password that time size of mobile keypad is small so it may get difficult to use for some user so we can establish numeric keyboard or to use pattern authentication.

Also system can provide different method for authentication. Also we can use QR code in man applications and give them a more security.

IX. CONCLUSION

Nowadays many people are live in the developed countries. So everyone likes to work mostly on the smart phones and laptops. And because of this the use of online services are increase. For that security is most important factor. So we are developed a secure authentication system which is based on QR code. It gives the function in online and offline mode. The fact that the user does not need to carry any additional device (as she would carry the phone anyway) makes it even easier and more comfortable. Also the smart phone are now not that much costly so this application is very important , easy, and secure for online banking security application.

REFERENCES

1] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee," Online Banking Authentication System using Mobile-OTP with QR-code", Page(s): 644 – 648, Nov. 30 2010-Dec. 2 2010, E-ISBN : 978-89-88678-30-5.

2] IETF RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm, Dec. 2005.

3] AntiPhishingGroup, "Phishing Activity Trends Report", from: http://www.antiphishing.org, dec. 2008.

4] Mohammad Mannan, P. C. Van Oorschot, "Security and Usability: The Gap in Real-World online Banking", NSPW'07, North Conway, NH, USA, Sep. 18-21, 2007.

5] Eisaku Ohbuchi, Hiroshi Hanaizumi, Lim Ah Hock," Barcode Readers using the Camera Device in Mobile Phones", IEEE paper.

6] Aidong Sun, Yan Sun, Caixing Liu," The QR-code reorganization in illegible snapshots taken by mobile phones", IEEE paper.

7] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen ,"HOTP: An HMAC-Based One-Time Password Algorithm" , , RFC 4226, December 2005.

8] Teoh Chin,Yew Mazleena,Salleh Subariah Ibrahim, "Spatial Resource Analysis of Two Dimensional Barcodes", IEEE Paper.

9] R.L. Rivest, A. Shamir, and L. Adleman,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems",http://people.csail.mit.edu/rivest/Rsapaper.pdf.

10] Robert P. McEvoy, Francis M. Crowe, Colin C. Murphy, William P. Marnane,"Optimisation of the SHA-2 Family of Hash Functions on FPGAs".

11] R. Fielding, J. Gettys, J. C. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee,"Hypertext Transfer Protocol -- HTTP/1.1",Network Working Group, Request for Comments: 2616

12] David Wagner, Bruce Schneier,"Analysis of the SSL 3.0 protocol",http://www.schneier.com/paper-ssl.pdf.

13] Randy Charles Morin,"How to Base64",www.kbcafe.com.

