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]Computer Engineering,
Savitribai Phule Pune University
Navsahyadri Edu. Soc. Pune

ABSTRACT

This paper explains implementation details of online banking authentication system. Security is an important issue for online banking application which can be implemented by various internet technologies and gap between real world and virtual world can be filled up. While implementing online banking system, secure data transfer need can be fulfilled by using https data transfer and database encryption techniques for secure storage of sensitive information. To eliminate threat of phishing and to confirm user identity, QR-code which would be scanned by user mobile device can be used. QRP that is Quick Response Protocol is very secure and also very easy to use for encrypted data. QRP is very secure protocol for use on untrusted computers. Our paper is providing the detail information about developing the security system for online banking transactions using QR code. In our project we use the QR code for providing the security to the online banking authentication system. In the QR code we are storing a complex password.

Keywords: **communication, technology, QR Code TM, encryption, decryption, multimedia, internet**

ARTICLE INFO

Article History

Received :20th October 2015

Received in revised form :

22th October 2015

Accepted : 26th October,2015

Published online :

31th October 2015

I. INTRODUCTION

Now a days almost all the things we are able to do online (like banking, shopping, communicating) and in this the challenge is that while doing this things online our information is not get damaged.[3] Indeed, as the method of cracking the security code get more complex and powerful. There is need to develop more powerful security application. These powerful applications allow user to work on untrusted computers confidently. This work is based on the two way authentication system. In this the QR code provides security. QR code is the Quick Response code [5]. The existing system having security methods such as password, username, figure prints, and face detection. But in these methods security is not up to the mark, so there is need to develop such security system which provides high security.The recent Despite of wide use of current online banking system, it has many security holes as it's based on traditional password based model, no mutual authentication between user and bank server which leads to threats like phishing(stealing passwords and using them for transactions), intercepting communication lines, database hacking, etc.. To make transactions more secure but also keeping them easy for user, following authentication system can be useful. In our proposed scheme, we assume the secure communication between the user (PC) □□□service providers and service providers □□certification authority. The proposed authentication system ensures the user authentication and digital signatures using authorized certificates by using https communication between user and server. using user's transfer information (ti), requested transfer time (t) and the serial number (sn) of user's mobile device instead of security card, we generate qr-code, display it on user screen and decode it with user's mobile device to generate otp. otp is generated on server side also and otp generated by user device and by server are verified to proceed [1]. user database should also be encrypted to prevent data leakage. 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 successful.

I. QR CODE

QR code is the Quick Response code. Before the QR code there are some authentication methods are available that are- User name and password, Bar code, Finger prints ,Face identity. But user name and password are not providing more security. And the Bar codes have some limitations like bar code only stored up to 20 digits. Bar codes are only readable in one direction. Also when it gets damage it is not readable. So in bar code we are not able to stored very complex password there for bar code is not more securemethod.

Finger prints and the face identity methods are very costly and not affordable by common users. For overcome all the drawbacks of existing system the QR code is introduce. **QR codes** (Quick Response codes) were introduced in 1994 by Denso-Wave, a Japanese company subsidiary of Toyota. QR codes are two-dimensional bar codes, so they can be read from any direction in 360. It can store up to 4,296 alphanumeric characters. So it is much more than the barcode can stored. Another advantage of QR code is that it is readable after being partially damage.Its advantages made QR code very powerful and popular in security and advertisement industry.

Generation of QR Code

create a QR code is we first create a string of data bits. This string includes the characters of the original mesTsage (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.After generating the aforementioned string of bits, we use it to generate the error correction code words for the QR Code. QR Codes use Reed-Solomon Error Correction technique .

Methods

We use TTJSA encryption algorithm, which was designed by Nath et al. and is an amalgamation of three different cryptographic modules: generalized modified Vernam cipher , MSA and NJJSA , for the encryption purpose of data in the QR Code. After encrypting the data, we embed the data in the QR Code using a set of different protocols and ultimately generate the encrypted QR Code. Till now, only few articles in the concerned area are published. The proposed analysis will choose two of the algorithms namely DJSA and NJJSAA [1],[2]. By going through this work [1],[2], they propose the key generation and almost the same process for the encryption as well as a contrary multiple encryption using bit exchange, right shift and XOR operation makes the system of NJJSAA differ from DJSA. Both , results in large mathematical calculations and CPU processing. This leads to unnecessary encryption time consumption.,also gives the insight about different proportions of power consumption. TTJSA is a combined symmetric key cryptographic method, which is formed of generalized modified Vernam cipher, MSA and NJJSA symmetric key cryptographic methods.

A) Modified Vernam Cipher:-

In this step, we break the whole file into different small blocks (like in Block Cipher system []), where each block size should be less than or equal to 256 bytes. Then we follow these steps: **Step1:** Perform normal Vernam Cipher method with the block of randomized key i.e. each byte of blocks of the file + each byte of the blocks of randomized key. **Step 2:** If the pointer reaches the end of each block then after performing Vernam Cipher method, pass the remainder of the addition of the last byte of the file block with the last byte of the key to the next file block and add the remainder with the first byte of the that file block. (This mechanism is called feedback mechanism) **Step 3:** Perform Step 1 and Step 2 until the whole file is encrypted and repeat this step for random number of times. After performing the aforementioned steps, we again merge the blocks of the encrypted file and thus we get the final encrypted result of this modified Vernam Cipher method.

b) NJJSAA Algorithm

The encryption number (=secure) and randomization number (=times) is calculated according to the method mentioned in MSA algorithm [2]. **Step 1:** Read 32 bytes at a time from the input file. **Step 2:** Convert 32 bytes into 256 bits and store in some 1- dimensional array. **Step 3:** Choose the first bit from the bit stream and also the corresponding number(n) from the key matrix. Interchange the 1st bit and the n-th bit of the bit stream. **Step 4:** Repeat step-3 for 2nd bit, 3rd bit...256-th bit of the bit stream **Step 5:** Perform right shift by one bit. **Step 6:** Perform bit(1) XOR bit(2), bit(3) XOR bit(4),...,bit(255) XOR bit(256) **Step 7:** Repeat Step 5 with 2 bit right, 3 bit right,...,n bit right shift followed by Step 6 after each completion of right bit shift.

1) Algorithm of TTJSA (Encryption):

Step 1: Start
Step 2: Initialize the matrix mat[16][16] with numbers 0 to 255 in row major wise.
Step 3: call keygen() to calculate randomization number (=times), encryption number (=secure).
Step 4: call randomization() function to randomize the contents of mat[16][16].

Step 5: times2=times
Step 6: copy file f1 into file2
Step 7: k=1
Step 8: if k>secure go to Step 15
Step 9: p=k%6
Step 10: if p=0 then Callvernamenc(file2,outf1) times=times2 callnjjsaa(outf1,outf2) callmsa_encryption(outf2,file1)
Step 11: call function file_rev(file1,outf1)
Step 12: copy file outf1 into file2
Step 13: k=k+1
Step 14: goto Step 8
Step 15: End

I) Algorithm of vernamenc(f1,f2):

Step 1: Start vernamenc() function
Step 2: The matrix mat[16][16] is initialized with numbers 0-255 in row major wise order.
Step 3: call function randomization() to randomize the contents of mat[16][16].
Step 4: Copy the elements of random matrix mat[16][16] into key[256] (row major wise)
Step 5: pass=1, times3=1, ch1=0
Step 6: Read a block from the input file f1 where number of characters in the block 256 characters
Step 7: If block size < 256 then goto Step 15
Step 8: copy all the characters of the block into an array str[256]
Step 9: call function encryption where str[] is passed as parameter along with the size of the current block
Step 10: if pass=1 then times=(times+times3*11)%64 pass=pass+1
Step 11: call function randomization() with current value of times
Step 12: copy the elements of mat[16][16] into key[256]
Step 13: read the next block
Step 14: goto Step 7
Step 15: copy the last block (residual character if any) into str[]
Step 16: call function encryption() using str[] and the no. of residual characters
Step 17: Return

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

ONLINE AUTHENTICATION SYSTEM

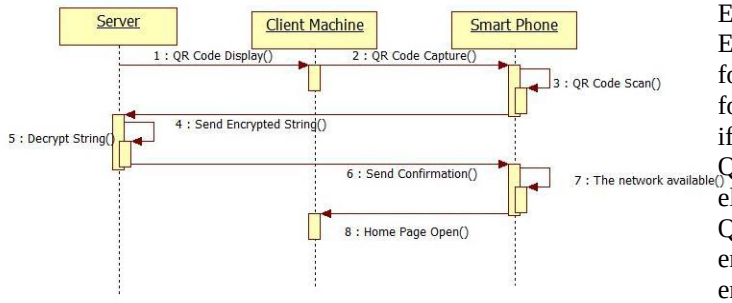
First IMEI number and random number are encrypted using the public key. This encrypted string generates the QR code using the QR code generation function which is present in java. Now this QR code image is display on the client machine. User scans this QR code using mobile phone. After scanning, in online 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.

VI. SECURITY

In our system the security is more powerful because of the QR code and encryption algorithm. A man-in-themiddle attack is not gets successful in our system because communication between the server and user is always encrypted. Username is not gets reuse or copies because username is get deleted after the user logout. 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 many applications and give them a more security.



II. EQUATIONS

Indicator	Meaning
0001	Numeric encoding (10 bits per 3 digits)
0010	Alphanumeric encoding (11 bits per 2 characters)
0100	Byte encoding (8 bits per character)
1000	Kanji encoding (13 bits per character)
0011	Structured append (used to split a message across multiple QR symbols)
0111	Extended Channel Interpretation (select alternate character set or encoding)
0101	FNC1 in first position (see Code 128 for more information)
1001	FNC1 in second position
0000	End of message

After every indicator that selects an encoding mode is a length field that tells how many characters are encoded in that mode. The number of bits in the length field depends on the encoding and the symbol version.

Formats	Mean Square Error	PSNR
.tif	9496.56	8.36
.jpg	2262.03	14.62
.png	1083.96	17.81

" Table "for NJJSA method 1) *Floyd's Error Diffusion Halftoning:*

Let P(i,j) be the original image of size n×m. Then we can calculate the errors as
follows:
for i=1 to n do
for j=1 to m do
if P(i,j)>127 then
Q(i,j)=1
else
Q(i,j)=0
End
error=255*Q(i,j)-P(i,j)
P(i,j+1)=7/16*error
P(i+1,j+1)=1/16*error
P(i+1,j)=5/16*error
P(i+1,j-1)=3/16*error
End
End
for i=1 to n do
for j=1 to m do
if P(i,j)>127 then
Q(i,j)=1
else
Q(i,j)=0
end
error=255*Q(i,j)-P(i,j)
End

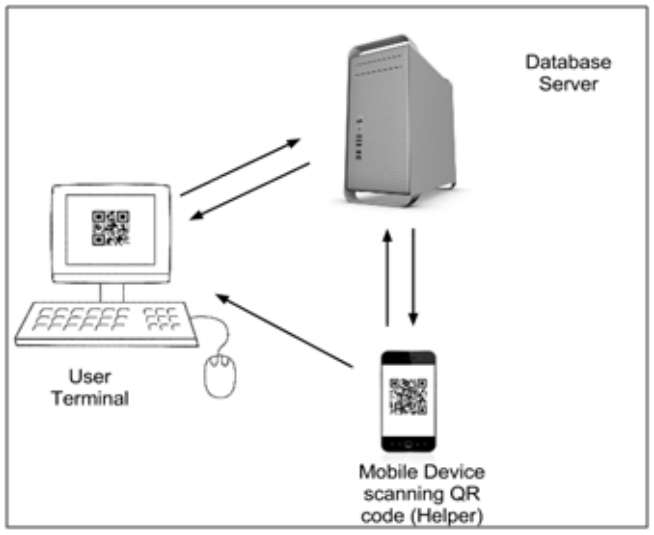
Formats	Mean Square Error	PSNR
.tif	9442.49	8.41
.jpg	2250.22	14.64
.png	1079.32	17.83

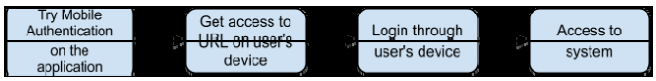
"Table" for Vernam Chiper method

You can generate an image of a mathematical formula using the TeX language (pronounced "tek" or "tech"). This is useful for displaying complex formulas on your web page. Here are some examples of formulas rendered on the fly:

Not URL-Encoded	URL-Encoded
cht=tx&chl=a^2+b^2=c^2	cht=tx&chl=a^2%2Bb^2=c^2

III. FIGURE AND TABLE





To ensure a high-quality product, diagrams and lettering MUST be either computer-drafted or drawn using India ink.

Figure captions appear below the figure, are flush left, and are in lower case letters. When referring to a figure in the body of the text, the abbreviation "Fig." is used. Figures should be numbered in the order they appear in the text.

Table captions appear centered above the table in upper and lower case letters. When referring to a table in the text, no abbreviation is used and "Table" is capitalized.

III. 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.

ACKNOWLEDGEMENT

This research paper cannot be considered complete without mentioning Prof. P. V. Mahadik We wish to express true sense of gratitude towards her valuable contribution .We are grateful to her for his constant encouragement and guidance in the fulfillment of this activity.

REFRENCES

[1] David Pintor Maestre Universitat Oberta de Catalunya 08018, "QRP:
An improved secure authentication method using QR codes", Barcelona, June 8, 2012
[2] David Muñoz-Mejías, Ivan Gonzalez Diaz, Student Member, IEEE,
and Fernando Diaz-de-Maria , Member, IEEE ,"A Low-Complexity
Pre-Processing System for Restoring Low-Quality QR Code Images", 2011.
[3] Majdi Al- qdah & Lin Yi Hui, Faculty of Information Technology
Multimedia University Cyberjaya, 63100, Malaysia "Simple Encryption/Decryption Application ".
[4] Henryk Blasinski, *Student Member, IEEE,* Orhan Bulan, and Gaurav
Sharma, *Fellow, IEEE,*" Per-Colorant-Channel Color Barcodes for
Mobile Applications: An Interference Cancellation Framework",
2013.
[5] Yu-Hsun Lin, Student Member, IEEE, Yu-Pei Chang and Ja-Ling
Wu, Fellow, IEEE, "Appearance-based QR Code Beautifier",2013.
[6] The QR algorithm, white paper, 2010.
[7] Akanksha Mathur, "A Research paper: An ASCII value based data
encryption algorithm and its comparison with other symmetric data
encryption algorithms", Jodhpur, India
[8] Kevin Berisso, Ph.D. "Designer QR Codes; Ensuring the "beep",
Automatic Identification and Data Capture Lab" spring 2013.
[9] Vinod Shokeen, Niranjan Yadav "Encryption and Decryption
Technique for Message Communication", 2011.
[10] Professor Greenstein, "QR Codes", Friday, March 11, 2011.
[6] K.Sasirekha,P.Baby,"Agglomerative Hierarchical Clustering Algorithm- A Review". Proceedings of the eleventh international conference on Information and knowledge management 2002
[7] Tapas Kanungo, David M. Mount, Nathan S. Netanyahu, Christine D. Piatko, Ruth Silverman, and Angela Y. Wu, "An Efficient kMeans Clustering Algorithm: Analysis and Implementation". IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 24, NO. 7, JULY 2002
[8] B. S. Everitt, S. Landau, and M. Leese, Cluster Analysis. London, U.K.: Arnold, 2001.
[9] A. K. Jain and R. C. Dubes, Algorithms for Clustering Data. Englewood Cliffs, NJ: Prentice-Hall, 1988.
[10] Osama Abu Samu computer science department yarmouk university,"comparison between data clustering algorithm", may 2 2007
[11] paresh chandra barman,Md. Sipon Miah, Bikash Chndra Singth,"Feature extraction clustering in text miningusing NMF basis probability", Ulab journal of science and engineering ,november 2,2011.

