QR Sharing: A New Approach in Security Using Visual Cryptography and Quick Response Codes

Rahul M. Shivalkar
P.V.G.'s COET, PUNE
rahulshivalkar@rediffmail.com

Parag T. Thorve
P.V.G.'s COET, PUNE
paragthorve@gmail.com

Prasanna A. Renushe
P.V.G.'s COET, PUNE
prasanna.renushe@gmail.com

ABSTRACT

Nowadays online transactions have become very common but there are various attacks present behind this. Thus, the security in these cases needs to be very high and should not be easily vulnerable for outside attacks. Our work proposes a scheme that attempt to collaborate Quick Response (QR) and Visual Cryptography (VC) together to improve the transmission of secret messages i.e. OTP via different medium as a means of authentication which may have more practicality in terms of real world usage. QR codes are basically two dimensional barcodes embedded with data that can be decoded quickly for information. In this work, we show that QR codes can be used for secret communication using VC. An interesting feature of our work is that we present a technique to convert QR codes into carriers for secret messages using VC. VC provides a way of sharing secrets between a numbers of participants. The secrets are in the form of an image that is encoded into multiple pieces known as shares. When these shares are superimposed, the secret can be instantly observed. Communicating secret messages in plain sight creates a credible threat to our national security. We hope that our work brings this issue to light and enhances counter-terrorism education.

KEYWORDS

OTP, Visual Cryptography, Quick Response (QR) Code, Shares, Online Transaction.

1 PAPER PREPARATION

In online transactions various types of attacks can take place, phishing is identified as a major security threat, and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective. Today, most of the applications are only as secure as their parent system. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet is completely secure or not. Phishing has also become a problem for online transactions.

The one-time password (OTP), a passcode valid for a single system login or online transaction and then discarded. OTP is used to perform authentication. In the case of a transaction an OTP is sent to the mobile phone of the user, for an authentication. Our proposed work is to improve the security in one time password (OTP). Presently password is sent by single medium, no authentication takes place regarding the merchant, whether it is fake or genuine. Our proposed system will make sure that the complete transaction takes place in a secured environment confirming about the originality of the merchant.

2 CURRENT SYSTEM

Some banks generate and dispatch OTPs to the customer's mobile phone via SMS or mobile Transaction Authorization Numbers (mTANs), as they are referred to in Europe and some countries in

South America. In some countries, banks still use hard copy methods to deliver OTPs, usually on paper or in the form of a plastic scratch card. All OTP systems share the same flaws and vulnerabilities. First, they are all symmetric because the bank has access to the same secrets as its customer (and the mobile carrier does too, in the case of SMS transmission). Secondly, OTP systems all remain reliant on browser-based communications back to the bank. This means that if a phishing site mimics the bank's online banking or the browser is otherwise compromised, the customer's credentials and the OTP can be harvested by fraudsters and immediately used to gain access to accounts and authenticate fraudulent transactions.

A hacker intercepts communications between a bank and its customer. The legitimate parties are unaware of the hacker's presence, enabling the fraudster to act as a proxy – the "man in the middle." In phishing, an unauthorized user copies the user's ID, password and OTP, and immediately uses them.

Flow on the next page shows one of the current systems in online transactions.

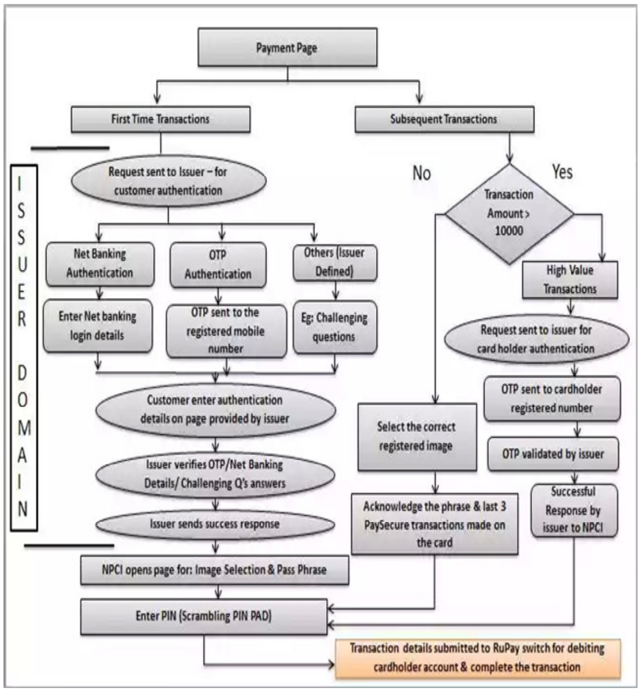
Payment Page
First Time Transactions
Subsequent Transactions
ISSUER DOMAIN
Request sent to Issuer – for customer authentication
Net Banking Authentication
OTP Authentication
Others (Issuer Defined)
Enter Net banking login details
OTP sent to the registered mobile number
Eg: Challenging questions
Customer enter authentication details on page provided by issuer
Issuer verifies OTP/Net Banking Details/ Challenging Q's answers
Issuer sends success response
NPCI opens page for: Image Selection & Pass Phrase
Enter PIN (Scrambling PIN PAD)
Transaction details submitted to RuPay switch for debiting cardholder account & complete the transaction
No
Yes
Transaction Amount > 10000
High Value Transactions
Request sent to issuer for card holder authentication
OTP sent to cardholder registered number
OTP validated by issuer
Successful Response by issuer to NPCI
Select the correct registered image
Acknowledge the phrase & last 3 PaySecure transactions made on the card

Fig.1 Present online transaction system

3 PROPOSED METHODOLOGY

Our proposed work is to improve the security in one time password (OTP). Presently password is sent by single medium, no authentication takes place regarding the merchant, whether it is fake or genuine. Our proposed system will make sure that the complete transaction takes place in a secured environment confirming about the originality of the merchant.

Our system will send the password via different medium to improve the efficiency of security. The detail system will be as follows.

The complete flow is as shown in the following figure.

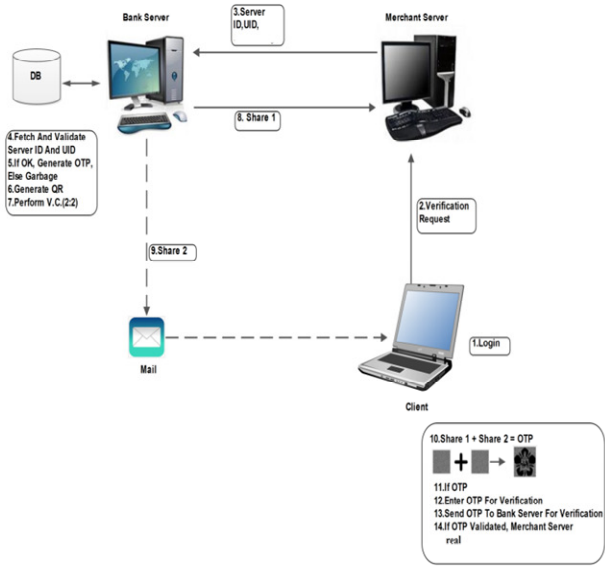
Bank Server
3.Server ID,UID,
Merchant Server
DB
8. Share 1
4.Fetch And Validate Server ID And UID
5.If OK, Generate OTP, Else Garbage
6.Generate QR
7.Perform V.C.(2:2)
2.Verification Request
9.Share 2
Mail
1.Login
Client
10.Share 1 + Share 2 = OTP
11.If OTP
12.Enter OTP For Verification
13.Send OTP To Bank Server For Verification
14.If OTP Validated, Merchant Server real

Fig.2 Proposed online transaction system

Our system is a hybrid system. It consists of client, server and merchant server. When client requests for the OTP first time, the request is sent to the merchant server. Merchant server sends UID and server ID to bank server. Bank server fetches and validates server ID and UID referring database. If OK, Generates the OTP, Else garbage. Then it generates Quick response (QR) code for OTP. We perform Visual Cryptography (VC) on QR and make 2 shares. These 2 shares are then transferred to client via different medium. One share will be transferred through the network and the other one via mail. When client gets both shares it will give QR code. On decoding QR, client will get the OTP. Then client sends this OTP for verification to bank server. If the OTP is valid, the merchant server is real and all further transaction will be secured.

4 IMPLEMENTATION &ANALYSIS

In our proposed methodology system is implemented using Application Servers, Java, Net Beans etc. technology. Detailed implementation of the proposed system can be as shown below: Hence, we will implement the anti-phishing system as described in below figure. So that online transaction fraud will reduce.

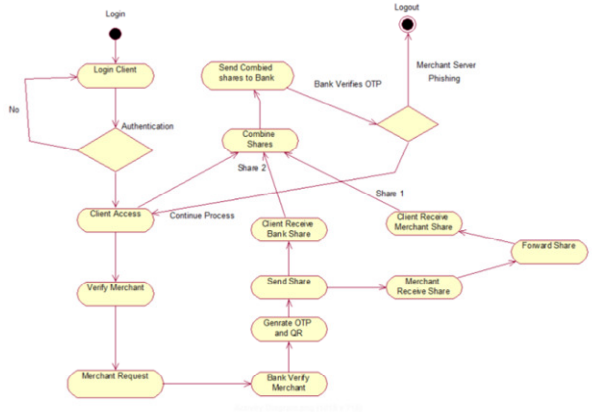

Fig.3 Flow of system to be implemented

5 RESULT & DISSCUTION

- Chances of fraud will be reduced at high level than the current system available for online transactions.
- Customer/ User will feel free or secured to do online transactions without any fear in their mind regarding insecurity of his/her transaction.
- Confidential data will be avoided being stolen or hacked by unauthorized or illegal sites for their welfare.

6 CONCLUSION

Currently, phishing attack is very common as it can attack globally and capture and store the users' confidential data. This data is used by an unauthorized user which is indirectly involved in the phishing process. Phishing websites can be easily identified using our proposed " QR Sharing: A New Approach in Security Using VC and QR" work. The system will make sure that the complete transaction takes place in a secured environment confirming about the originality of the merchant.

Merging the concept of QR (Quick Response) and VC (Visual Cryptography) together, our system will lead to a complete secured environment for online transactions.

7 ACKNOWLEDGEMENT

We gratefully acknowledge the contributions of M.Naor and A.Shamir for their work in the field of Visual Cryptography (VC).

REFERENCES

[1].Ollmann G., The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.

[2].M. Naor and A. Shamir, "Visual cryptography," in Proc.EUROCRYPT,1994, pp. 1–12.

[3].W.-G. Tzeng and C.-M. Hu, "Anewapproach for visual cryptography, "Designs, Codes, Cryptog. vol. 27, no. 3, pp. 207– 227, 2002

[4].A. Shamir, .How to Share a Secret,.Communication ACM, vol. 22,1979, pp. 612-613.

[5].http://searchengineland.com/what-is-a-qr-code-and-why-do-you-need-one- 27588

[6].http://www.datagenetics.com/blog/november32013/

[7].https://www.duosecurity.com/blog/the-current-state-of-online-and-mobile- banking-security

[8].https://www.staysmartonline.gov.au/business/online_transactions_and_ban king

[9].W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography for Print and Scan Applications,. IEEE Transactions, ISCAS-2004, pp.572-575.

[10].http://www.circleid.com/posts/how_do_you_do_secure_bank_transactions_ on_the_internet/