QR Code based secure OTP distribution scheme for Authentication in Net-Banking

Abhas Tandon[1],Rahul Sharma[2], Sankalp Sodhiya[3],P.M.Durai Raj Vincent [4]
[1,2,3]IIIrd B.Tech(IT),SITE, VIT University
[4] Assistant Professor(Senior), SITE, VIT University.
abhastandon007@gmail.com, rahulsharma3493@gmail.com, sankalp28011992@gmail.com

***Abstract*— Authentication is the process of verifying the identity of a user. One time passwords (OTP) play a vital role for authentication in net-banking to make it more secure. OTP are used to provide higher layer of security over static passwords that are prone to replay attacks. Distribution of OTPs to concerned user is a major issue. Short message service that is available for mobile phones is the most common methodology for OTP distribution. Quick Response code (QR code) is actually two dimensional bar codes and can store information in both length and breath. QR codes are widely being used to convey short information such as website address, mobile numbers etc. In this paper we are presenting a new authentication scheme for secure OTP distribution in net banking through QR codes and email.**

Keyword- QR code, OTP, authentication, net banking

I. INTRODUCTION

Net Banking is one of the most critical systems which the online users use in their daily life. This system has been witnessing increase in the number of users on a steep percentage. Although most of the banks claim that net banking is provided with 100% online security but there are still many customers who are reluctant and plead for higher security requirements [1].

In order to protect from illegal access to user information, remote authentication of users is essential service in this system [2]. In 1981, Lamport [3] first introduced the one-time password authentication scheme with usage of one-way hash chain. Hence to generate series of passwords the set of hash values are restricted. But in recent times there have been many techniques used for authentication during net banking. Most of them involve the usage of one time passwords and they differ only in the means of delivering them to users.

One Time Passwords (OTP) is passwords which are valid only for a session to validate the user within a specified amount of time. Hence for each session the user will be validated using new OTP. They are also helpful in preventing replay attacks, phishing attacks and other attacks on basic static passwords [4]. Also they offer other characteristics like anonymity, portability, extensity and enables to keep the information from being leaked [5].Some of them OTP transmission techniques are text messages by gateway, propriety tokens, web based methods, Secure Code devices and Grid file. The most recent Grid file maintains a hash type file to verify the user's authentication request also increases the risk of tampering. But all of them deal with text based methods which could be identified in infinite time.

QR codes [6] are used to store textual information in the form of images that can be read by any smart device including most mobile phones. QR codes can be considered as two-dimensional bar codes. Recently much research has been done that focus on application of QR code and advancement of the technology for providing better user experience. In [7] authors have suggested a method of contextual QR code recognition that can be used to provide information related to particular subject through QR codes. QR codes have also been used in the field of cryptography for data security. In [8], Hsiang-Cheh Huang et.al have proposed a data hiding scheme through application of QR codes. Authors have analysed QR codes embedded in images have shown implementation of proposed system. QR codes have range of applications. Algorithms have been proposed and implemented that can allow use of QR code for electronic ticket system [9].

AES is a well-known encryption algorithm that is symmetric in nature. It has been applied in various applications other than data security. In [10] authors have suggested an algorithm that utilizes power of AES scheme for implementation of an anti-theft system.

II. PROPOSED AUTHENTICATION SCHEME

System consists of a web service that will generate alpha-numerical OTPs using pseudo-random numbers and current timestamp. Use of timestamp further assures security and uniqueness of OTP. The alpha-numerical password string is then encrypted using Advanced Encryption Standard (AES).The key for the algorithm will be ATM pin of the user since it is unique for every user and can be obtained by Bank Server in every login session through account number. The AES algorithm is used here since not only it provides higher security but also it improves performance in such critical systems. The encrypted string is then converted to QR image by the Bank Server. It is then sent to the concerned user using email as transmission medium via SMTP. User then

downloads the QR code image and uploads it in standard application that is made available to him by net-banking provider. The application provides space for QR image to be uploaded and user then enters his ATM pin which is used to decrypt the string read from QR code. The validation of the pin is carried out by sending request to the bank server. If the ATM pin is entered correctly, application displays the OTP that was generated for the session. User then enters the OTP for net-banking and completes authentication. Then any type of transaction can be carried out online on the service provider website.

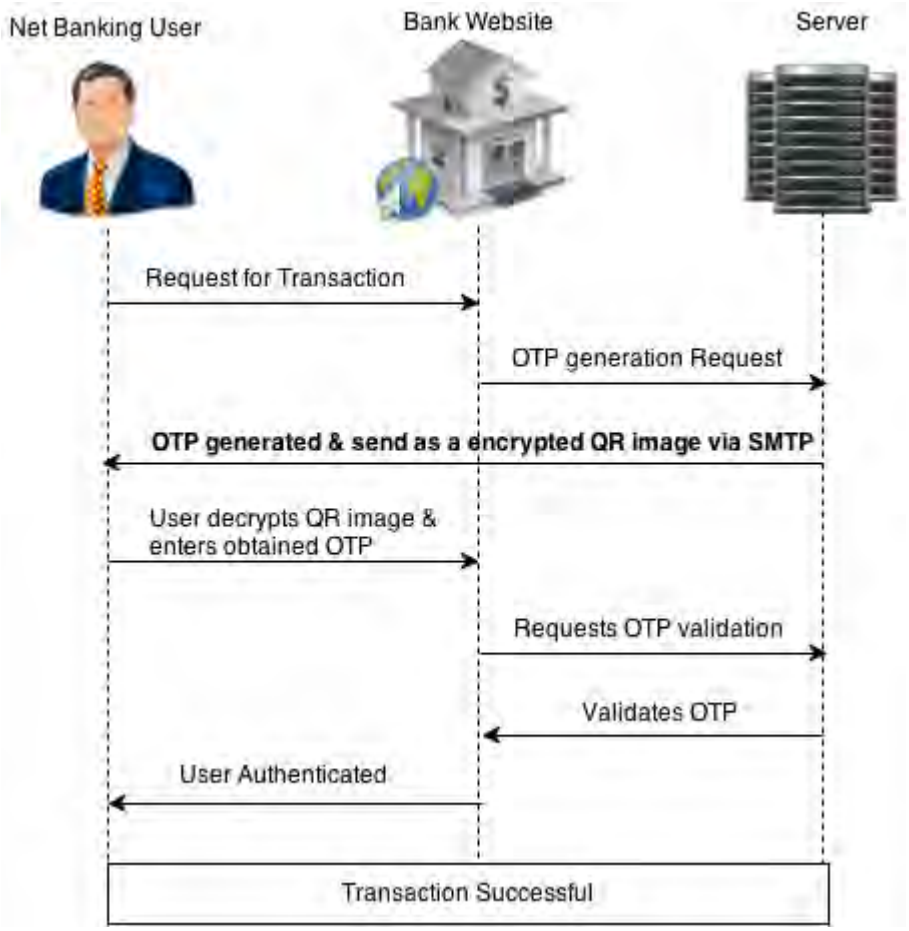

Fig. 1 Sequence diagram for proposed authentication scheme

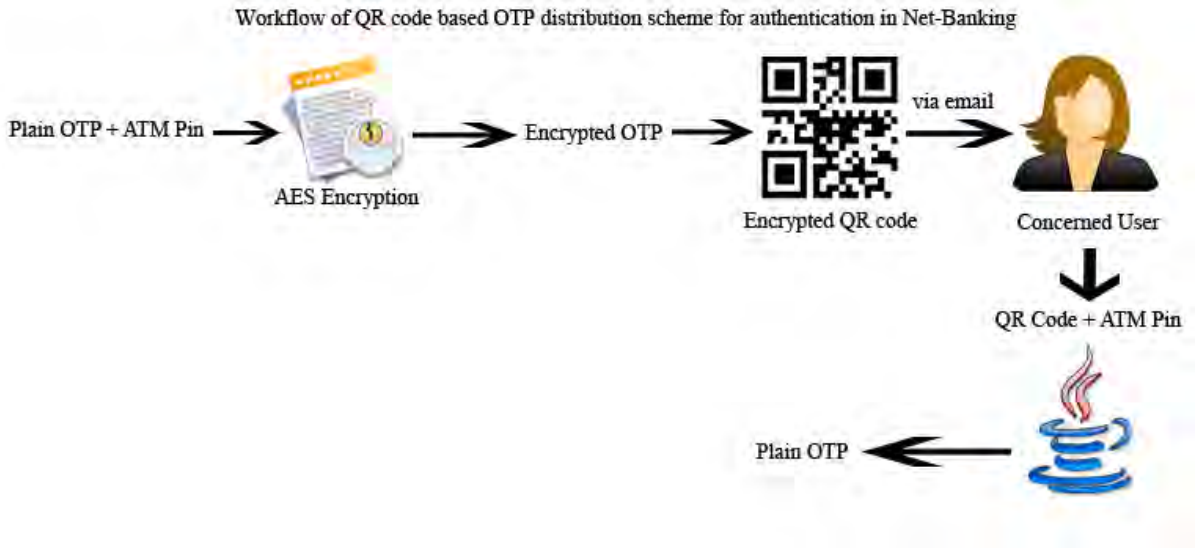

Fig. 2 Workflow of proposed authentication scheme

III. IMPLEMENTATION

Fig. 3 OTP in the form of an AES encrypted QR code.

Fig. 4 Java implementation for decrypting encrypted QR code using AES and QR code reader java library.

IV. SECURITY ANALYSIS

OTPs are transmitted in the form of an image which makes it complex for intruder to detect the presence of secured information. OTP is send to the concerned user through an email message. Net-banking users can conveniently access their email accounts and obtain the QR code containing the encrypted OTP. Hence under a secure transmission of the QR code it can only be interpreted by application software deployed by the bank with the QR image. Usage of AES algorithm for encrypting one time password further enhances the security of the system. Proposed scheme has higher degree of complexity than all existing systems and clearly the time required to crack the scheme will be more than the useful lifetime of OTPs. OTPs are generated for a session and have a short lifetime. It's not possible to use the OTP after their expiry. Popularity of QR codes makes the method user friendly. Even a trivial user having basic understanding of using a computer system can adapt to it.

V. FUTURE ENHANCEMENTS

Visual cryptography is the method through which an image is converted into two or more images. Original image can be obtained by overlaying all these images over one another physically. Act of overlaying an image over another can also be performed through software programs. Visual cryptography can be applied to convert the qr code into two images and both these images can then be transmitted separately. Even if intruder manages to get one of the images, he won't be able to crack the scheme without the knowledge of the other corresponding part of the image. Thus visual cryptography can be applied to further enhance the security of the entire system. Further, java application to decrypt the qr code image can be deployed as a cloud application and can be made available to intended audience easily.

VI. CONCLUSION

In this paper we have proposed a novel authentication scheme for net-banking through QR code based OTPs. In recent years there has been a steep increase in the number of net-banking users. Hence the proposed system satisfies the high security requirements of the online users and protects them against various security attacks. Also the system does not require any technical pre-requisite and this makes it very user-friendly. Hence QR code proves to be versatile at the same time beneficial for both the customers in terms of security and vendors in terms of increasing their efficiency. Hence it is most widely used to advertise and market the products by most businesses.

REFERENCES

[1] 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.
[2] L.Lamport, "Password authentication with insecure communication, "Communications of ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[3] Kuan-Chieh Liao, Wei-Hsun Lee, Min-Hsuan Sung, Ting-Ching Lin, “A One-Time Password Scheme with QR-Code Based on Mobile Phone”, Fifth International Joint Conference on INC, IMS and IDC, 2009, pp 2069-2071
[4] Kuan-Chieh Liao, Wei-Hsun Lee, A Novel User Authentication Scheme Based on QR-Code, JOURNAL OF NETWORKS, VOL. 5, NO. 8, AUGUST 2010, pp 937
[5] Sang-Il Cho, HoonJae Lee, Hyo-Taek Lim, Sang-Gon Lee, “OTP Authentication Protocol Using Stream Cipher with Clock-Counter”, October, 2009.
[6] J. S. Tan, “QR code,” Synthesis Journal, Section 3, pp. 59-78, 2008.
[7] Jose Rouillard, “Contextual QR Codes”, Proceedidngs of the Third International Multi-Conference on Computing in the Global Information Technology (ICCCGI2008), Athens, Greece, July 27-Augst 1, 2008.
[8] Hsiang-Cheh Huang; Feng-Cheng Chang; Wai-Chi Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," Consumer Electronics, IEEE Transactions on , vol.57, no.2, pp.779,787, May 2011
[9] Conde-Lagoa, D.; Costa-Montenegro, E.; Gonzalez-Castao, F.J.; Gil-Castiñeira, F., "Secure eTickets based on QR-Codes with user-encrypted content," Consumer Electronics (ICCE), 2010 Digest of Technical Papers International Conference on , vol., no., pp.257,258, 9-13 Jan. 2010
[10] Qiu-xia Wang; Tie Xu; Pei-zhou Wu, "Application research of the AES encryption algorithm on the engine anti-theft system," Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on , vol., no., pp.25,29, 10-12 July 2011