ISSN:0975-9646

Advanced Online Banking Authentication System Using One Time Passwords Embedded in Q-R Code

Abhishek Gandhi, Bhagwat Salunke, Snehal Ithape, Varsha Gawade, Prof.Swapnil Chaudhari.

Department of Information Technology
Marathwada Mitra Mandal's Institute of Technology,
Lohgaon, Pune-411043, India

***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. 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 we are going to use concept of QR-code with android application. QR-code which would be scanned by user mobile device which overcome the weakness of traditional password based system. We improve more security by using one time password (OTP) which hides inside QR-code.**

***Keywords*— One Time Password (OTP) , Quick Response Code(QR Code)**

I. INTRODUCTION

The Internet is an integral part of our daily life, and the proportion of peoples who expect to be able to manage their bank accounts anywhere, anytime is constantly increased. As such, Internet banking has come as a crucial component of any financial institutions.

Online banking is one of the most sensitive tasks performed by general internet user. Security of a customer's financial information is very important, without which online banking couldn't be successful. Financial institutions have set up various security processes to reduce the risk of unauthorized online access to a customer's records, but there is not a single one method that fulfills all the requirements. Most of the attacks on online banking used today are based on steal user login data and valid TANs. A well known example is phishing attack. Phishing is the act which acquires personal information such as credit card details, passwords, user name etc.

Cyber –security is very important because of gradually increased in information technology. The Online financial transaction in the past was required to apply a security card and public key certificate which were the methods to conforming a user, and in recent decade OTP was introduced. One-Time Pass-word is a password system where passwords can only be used once and the user has to be authenticated with a new password 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 leaked.

Previous banking service uses security card which does not suite modern Mobile environment because we do not know when and where online banking will be used. In very emergency situation online banking cannot be done without security cards. The current online banking system send OTP on user's mobile which can be hack during transmission .In order to overcome such weaknesses and inconvenience of security card, our proposed authentication system uses two dimensional barcodes (2D Barcode) called QR code instead of security cards. QR code stands for "Quick Response" code. From QR code data can be retrieved very fast with greater accuracy even if some part of data is corrupted.

II. RELATED WORK

1.One Time Password :

One-time passwords are a mechanism for logging on to a network or service using a unique password which can be used only once .This prevents various forms of identity theft by ensuring that a user name or password combination cannot be used a second time. Usually the user's login name remains the same, and the one-time password changes with each login. Hence for each session the user will be validated using new OTP. They are also useful in preventing replay attacks, phishing attacks and other attacks on basic traditional passwords. Also they offer other characteristics like anonymity, portability, and extensibility and enable to keep the information from being leaked. Some of the OTP transmission techniques are text messages by gateway, propriety tokens, web-based methods Secure Code devices and Grid file. The most recent Grid file handles a hash type file to verify 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. One-time passwords are a form of strong authentication, and offer more effective security to corporate networks, on-line bank accounts and other systems containing sensitive data.

OTPs avoid a number of shortcomings that are associated with traditional passwords. The very important shortcoming that is addressed by one time passwords is that, in contrast to traditional passwords, they are not vulnerable to replay attacks, phishing attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since OTP will be no longer valid. On the downside, OTPs are hard for human beings to memorize. Therefore they need additional technology to work.

There are two approaches to generate an OTPs:

1. Time based OTP – the OTP changes at frequent intervals.
2. Event-based OTP – the OTP is generated by pressing a button on the OTP device or token.

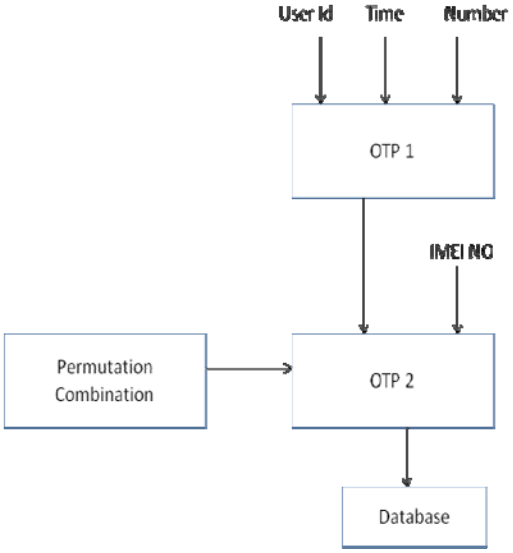

Fig.1. One time Password Generation

By using combination of 3 parameters- customer id ,current system time and Random number OTP1 is generated that is hide inside QR code image.

Permutation combination logic is applied on 2 parameters- OTP1+IMEI NO and from that OTP2 is generated. So OTP1 is 4 digit number that is embedded in QR code and OTP2 is 8 digit number that is calculated from OTP1.

The above process will done successfully only if customer uses our given QR code scanner.

If customer uses QR code scanner which is available on internet then wrong OTP is generated and authentication process will failed.

2.QR Code :

QR Code is a two-dimensional barcode introduced by the Japanese company Denso-Wave in 1994. This kind of barcode was initially used for tracking inventory in vehicle parts manufacturing and is now used in a variety of industries. QR stands for "Quick Response" because its contents are decoded at high speed.

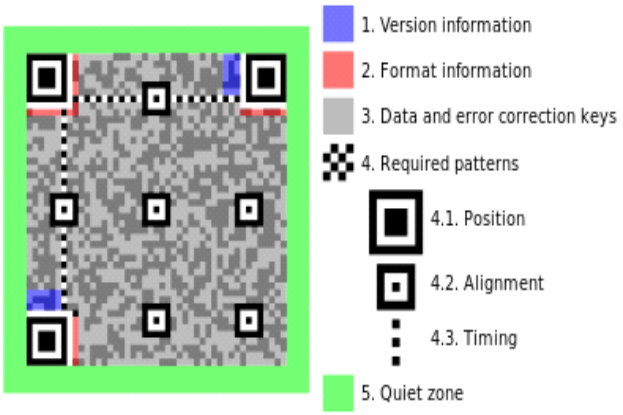

Fig.2. QR Code Structure

A. Technology

A QR Code is a matrix code developed and released primarily to be a symbol that is easily interpreted by scanner equipment. It contains information in both vertical and horizontal directions, whereas a 1D barcode has only one direction of data (usually the vertical one). QR Code also has error correction capability. Data can be restored even when some parts of the code are distorted or damaged. Compared to a 1D Barcode, a QR Code can hold greater volume of information: 7,089 characters for numeric only, 4,296 characters for alphanumeric data, 2, 953 bytes of binary (8 bits) And 1,817 characters of Japanese Kanji/Kana symbols.

B. Usage

Without a machine, it's impossible for a human to manually decode QR Codes but they are easily processed by scanning equipment. Nowdays QR code scanner app is available on many app stores at free cost. Users can scan the QR Codes and the software integrated into their phones Decodes the messages and display the information on their mobile devices. Depending on the type of data hide inside QR code and the nature of the application, alternative actions can be taken the at decoding stage: a phone number can be automatically dialed, a SMS can be sent, a web page to the URL can be displayed in a mobile , or a definite application can be executed.

3.Android :

Android is a Linux-based operating system designed primarily for touch screen mobile devices such as smart phones and tablet computers. Android was Initially developed by Android Incorporation, which Google financially supported and later purchased in 2005.At beginning android works on Linux kernel version 2.6 ,and from android 4.0 OS version (Ice Cream Sandwich) onwards, it works on version 3.x with libraries and APIs. . Android uses the Dalvik virtual machine compiler to run Dalvik 'dex-code' (Dalvik Executable) which is usually translated from Java byte code.

Our QR code scanner application is developed in the Java language using the Android software development kit (SDK). The SDK includes a comprehensive set of development tools, including a debugger, software libraries, a handset emulator, documentation, sample code, and tutorials. The supported IDE is Eclipse using the Android Development Tools plug in.

3.1 User Interface Overview

All user interface elements in an Android app are built using View and View Group objects. A View is an object that draws something on the screen that the user can interact with. A View Group is an object that holds other View (and View Group) objects in order to define the layout of the interface.

Android provides a collection of both View and View Group subclasses that offer you common input controls (such as buttons and text fields) and various layout models (such as a linear or relative layout).

III. PROPOSED SYSTEM

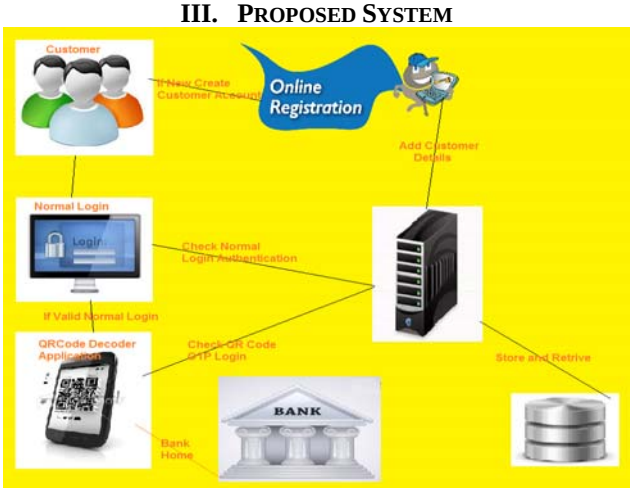

Fig.3. Proposed Authentication System

In our proposed system , we are going to develop two softwares for online banking system which provides more security to bank customer. First one is android based mobile software which will scan the QR code generated by bank server. We are developing another software that provides E-banking facility.

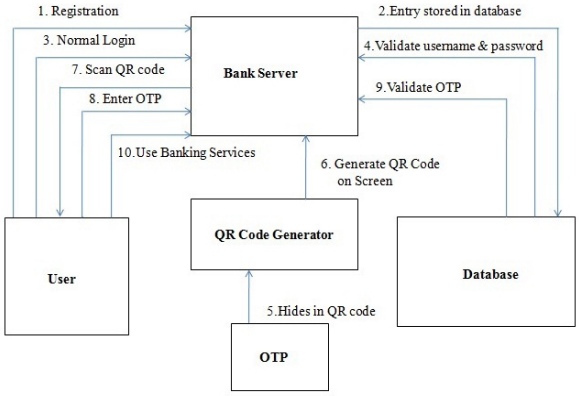

Fig.4. Working of Authentication System

1. At first ,Bank customer have to do registration and create his account.
2. Next step is normal login step in that customer have to provide username and password for login process.
3. Based on customer id ,current system time and Random number(3 parameters) OTP1 is generated that is hide inside QR code image.
4. QR code image is generated by three parameters OTP1,image size and image format.
5. QR code image is displayed on computer screen(bank server).
   a) Permutation combination logic is applied on OTP1 + IMEI number(of customer's mobile).
   b) After that new OTP2 is generated that is stored in bank database.
6. Customer will scan the QR code by android QR code scanner application.
7. OTP1 is extracted from QR code and again same permutation combination logic is applied on OTP1 + IMEI number.
8. In this process OTP2 is generated which is displayed on customer's mobile. Customer have to enter that OTP2 in login process.
9. If newly generated OTP2 matches with the one which is store in database then Customer will get successfully login into banking system.

Customer can use the banking services. Such as –
- Viewing account balances
- Viewing recent transactions
- Ordering cheque books
- Funds transfers between different customer accounts
- Pay electricity bill facility

IV. CONCLUSION

The use of online banking services is increased gradually in daily life and existing online banking requires the usage of one time password which is send to customer's mobile. As mobile is a gateway , one can hack the OTP in between SMS transmission. In our project we does not use this technique instead of that we scan the QR code from mobile that will decode OTP and display it on the customer's mobile directly.

In this project, we propose new authentication system for online banking which can provide greater security and convenience by using mobile OTP with the QR-code .The importance of security and ease of use is like two side of a coin. It cannot be provided considering that show up on one side. Therefore, we should always seek for safety devices to meet all ease and security of electronic financial services.

REFERENCES

[1] Online Banking Authentication System using Mobile-OTP with QR-code Young SilLee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee june , 2010sec01/fu/fuhtml:Secureinternetb

[2] J. Bringer, H. Chabanne, and E. Dottax, HB++: A Lightweight Authentication Pro-tocol Secure against Some Attacks, Proc. Second Intl Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006.

[3] K. Fu et al., Dos and Donts of Client Authentication on the Web, Proc. 2001 Usenix Secu- rity Forum, Usenix Assoc., 2001, pp. 251268; www.usenix.org/events/ sec01/fu/fuhtml:Secureinternetb

[4] 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.

[5] ISO/IEC 16022:2000 – Information Technology – Automatic Identification and Data Capture Techniques – BarCode Symbology – QR Code, 2000.

[6] 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.

[7] Sang-Il Cho, HoonJae Lee, Hyo-Taek Lim, Sang-Gon Lee, "OTP Authentication Protocol Using Stream Cipher with Clock-Counter", October, 2009

[8] Ohbuchi, E., Hanaizumi., H., Hock, L.A, "Barcode Readers using the Camera Device in Mobile Phones", in Proc. of 2004 International Conference on Cyberworlds, pp.260-265, 2004.

[9] Jean-Daniel Aussel, "Smart Cards and Digital Identity", Telektronikk 3/4. 2007. ISSN 0085-7130.

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