Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Online Banking Security System Using OTP Encoded in QR-Code

D. R. Anekar, Binay Rana, Vishal Jhangiani, Aziz Kagzi, Mohammed Kagalwala

Department of Information Technology, Sinhgad Academy of Engineering,
Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract— Technology is advancing at a rapid pace and with this advancement making our systems secure from threats and attacks becomes an issue of major importance. The authors of this paper are implementing a security system for online internet banking using a QR (quick response) based approach to authenticate users and also to eliminate the threat of phishing. The user after requesting an online transaction will scan the QR code from the computer screen using his/her mobile phone whose IMEI number is registered with the bank to generate an OTP (one time password) on his/her phone for the transaction. The OTP is encoded in the QR code which in turn is encoded using the user's phone's IMEI which will serve as a shared private key between the bank and the user in a sense that only the user's phone is able to scan the QR code meant for him/her and generate the correct and valid OTP for the transaction. Use of conventional methods to deliver the OTP to the user will not be made; instead, the user is deciphering the OTP by making use of a device of which he/she is required to necessarily have physical possession.

Keywords— online internet banking, QR, OTP, IMEI, shared private key, physical possession.

I. INTRODUCTION

Online banking is one of the most sensitive tasks performed by a general internet user. Most traditional banks now offer online banking with a high degree of security. Although the banks heavily advertise an apparent `100% online security guarantee', typically the fine print makes some conditions that can compensate security lapses. The number of users of online banking systems has increased rapidly from 2009 to 2014 and continues to increase as people have greater knowledge about the internet and the services accessible from it. Also, regular access to the internet among a large number of people has led to an increase in the use of several online services, online banking included. The average amount of worldwide dealings online per day is beyond USD 26 trillion. Earlier banks used to offer fraud protection for users of their online banking services as such frauds were rare and they wanted to increase the number of customers using online banking services. However, recently banks are becoming increasingly reluctant to reimburse users who fall prey to online scams such as phishing or identity theft. As incidents of frauds became common banks and other financial institutions began studying and using several counter measures.

One of the counter measures that drew a high amount of attention from the financial agencies is the use of an OTP (One Time Password) for user authentication. 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 guarantees the safety even if an attacker is tapping passwords in a network or a user loses it. Besides, OTP features anonymity, portability, and extensity, and enables to keep the information from being leaked. Currently the services of delivering the OTP to the user from the bank's servers or password generators are being performed by third party cellular network providers or other network dependant applications. Such methods however are susceptible to interception and can lead to an attack amounting to identity theft. The purpose of the project proposed in this paper is to uniquely encrypt the OTP such that only the targeted recipient (i.e. a valid user) can decrypt it using a shared private key. Also, another major purpose is to eliminate the use of external networks in delivering the OTP from the bank's servers to the user. The proposed system is nearing completion in terms of its development.

II. LITERATURE SURVEY

A. One Time Password:

An OTP is a generated (and not user selected) password which is valid only once and that too for a pre-determined short time interval. The OTP is generated on the server side using an algorithm and cryptographic keys and delivered to the user via a network other than the one on which the services that have to be made secure are running. The user receives the OTP and enters it into a client application meant for end users. On the server side, an authentication server can check the validity of the password by sharing the same algorithm and keys. OTPs generated by a server can be used only once and are valid for only a short period of time, OTPs used by banking portals in India are by and large valid for only 5 minutes, so if an OTP has been used for attempting a transaction or was delivered to the user at a time earlier than in the last 5 minutes then the user must request for a new OTP or he/she cannot attempt a transaction.

There are two approaches to generate an OTP:

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

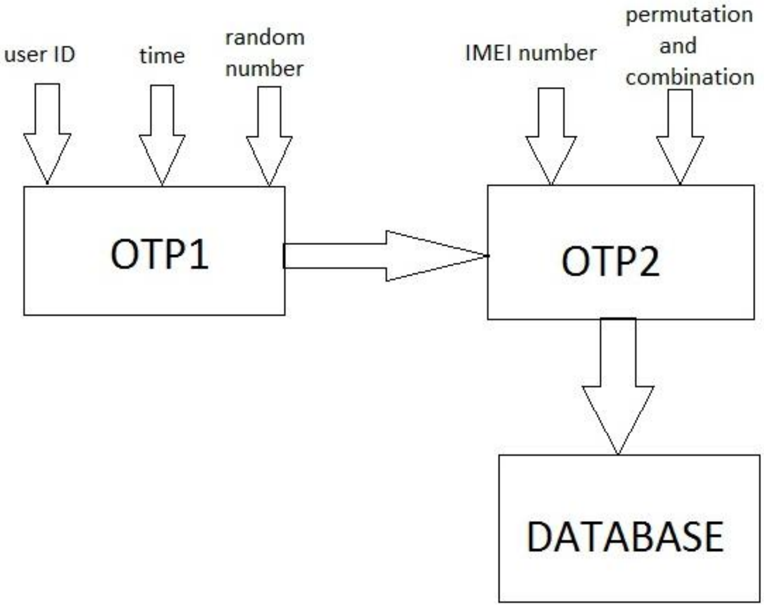

Fig.1. Proposed OTP Generation

In our proposed system we are generating 2 OTPs (of which only the second one is delivered to the end user for use) as illustrated in Figure 1 by using a combination of 3 parameters: customer id, current system time and a random number. OTP1 is generated and hidden inside the QR code image. OTP1 is an intermediate result and is not delivered to the user.
A permutation and combination logic is applied on 2 parameters: OTP1+IMEI NO to generate OTP2 from them. So OTP1 is a four digit number that is embedded in the QR code and OTP2 is an eight digit number that is calculated from OTP1.The above authentication process involving OTP will complete successfully only if the customer uses the bank's QR code scanner application and has previously registered his/her mobile device's IMEI number with the banking portal.
OTP based authentication has advantages over PKI (Public Key Infrastructure) as it does not require the deployment of smart card readers, drivers and PC software. However in terms of features, OTP only provides identification and authentication, whereas PKI provides addition encryption a signature. OTP being a password based authentication is also vulnerable to man-in-the-middle attacks, such as phishing scams. Since there is no mutual authentication of the PC and the internet service provider server, an attacker can intercept an OTP using a mock-up site, and impersonate the user to the real internet web site. The system that we have developed aims to eliminate such attacks, how that is to be achieved is discussed in detail in section IV i.e. "proposed system".

B. QR (Quick Response) Code:

"QR" is short for "Quick Response" and is so called because its contents are decoded at a high speed. A QR Code is a matrix code (or a two-dimensional bar code). A QR code carries meaningful information in the vertical as well as the horizontal direction, hence the term two-dimensional. Conventional barcodes carry meaningful information in only one direction i.e. the horizontal direction.
A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed until the image can be appropriately interpreted. The required data is then extracted from patterns present in both horizontal and vertical components of the image.
A QR Code also has error correction capabilities. It enables data restoration even when some parts of the code are distorted or damaged. Compared to a 1D Barcode, a QR Code can hold a greater volume of information: 7,089 characters for numeric only and 4,296 characters for alphanumeric data.

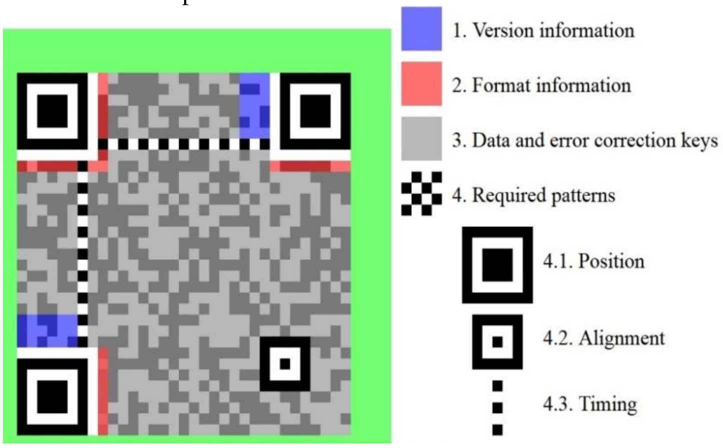

Fig 2. Structure of QR code

Decoding a QR code manually is impossible, but it can easily be processed by using some scanning equipment. Using any of the QR code scanning apps that are available free of cost users can scan a QR code and the integrated software will decode the messages and display the information on their mobile devices. Depending on the type of data encoded inside the QR code and the nature of the application, alternative actions can be taken at the 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.

QR codes have come a long way since their creation, having first been developed to help track parts in the manufacturing process of vehicles. Today they have a number of purposes, including transport ticketing, entertainment, location tracking, and product labeling/marketing, just to name a few. You can find QR codes being used to send audiences to a website for browsing, to bookmark a webpage, to initiate phone calls, send short messages, send emails, produce links to web URL's, start chats with other messaging service users, connect to WI-FI networks, access information, get coupons, view videos, purchase items, process orders, advertise products, etc. In our system we are using the two dimensional QR code as a medium to encode and store the OTP, the encoding is done in such a manner that only the intended recipient can decode it.

C. IMEI number

The International Mobile Station Equipment Identity (or IMEI) is a unique number, used to identify 3GPP (i.e., GSM, UMTS and LTE) and iDEN mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dialpad, or alongside other system information in the settings menu on smartphone operating systems.

The IMEI number is used by a GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network. For example, if a mobile phone is stolen, the owner can call his or her network provider and instruct them to "blacklist" the phone using its IMEI number. This renders the phone useless on that network and sometimes on other networks too, whether or not the phone's SIM is changed.

The IMEI is only used for identifying the device and has no permanent or semi-permanent relation to the subscriber. Instead, the subscriber is identified by transmission of an IMSI number, which is stored on a SIM card that can (in theory) be transferred to any handset. However, many network and security features are enabled by knowing the current device being used by a subscriber. The IMEI number in the proposed system is being used to identify whether a user who is using a device to decode the QR code and obtain the OTP has registered the device with the bank as the QR code will be encoded by the bank using the user's mobile device's IMEI number in such a manner that only the phone having that particular IMEI (i.e. a registered phone) will be able to decode the QR code correctly and decipher the correct OTP. So the IMEI number is basically being used to ensure that a user has physical possession of the device he has registered with the bank.

III. COMPARISON WITH OTHER EXISTING SYSTEMS

The system proposed in [1] by Mete Eminağaoğlu, Ece Çini, Gizem Sert and Derya Zor is making use of a two factor identity authentication system where the first factor is the type 1 credentials such as user ID, password, pin, etc. and the second factor is a pseudo-randomly generated alphanumerical QR code which is used as the one time password (OTP) token sent to the user via email or MMS.

While in the case of our system we have added an additional security feature that is IMEI number specific encoding and decoding which means that the IMEI number is a shared private key between the user and the bank. IMEI adds more security to our system as every mobile phone device has a unique IMEI no. and using this feature we can assure that only an authorized person is allowed to conduct transactions using the system. Also, we are not making use of networks to send OTP to the user as in the case of E-mail or MMS but are generating the QR code image that has the encoded OTP encrypted using the user's IMEI number as the private key such that the QR code (containing OTP) is never delivered to the user's phone over a network but in fact he will scan it from the computer screen using his phone to generate the OTP. The QR code will be visible to the user on the banking portal and one must keep in mind that only the user's phone whose IMEI number he/she has registered with the bank will be able to decode the QR code and obtain the OTP. Attempts to scan the QR code from devices whose IMEI number has not been registered with the bank will either yield a wrong OTP or will result in a complete failure to decode any information.

IV. PROPOSED SYSTEM

The use of online banking services is increasing gradually in daily life and existing online banking requires the usage of OTP which is sent to customer's mobile. As mobile services are provided by third parties, the OTP can be intercepted by anyone in between the SMS transmission. In our project instead of this technique we scan the QR code from mobile, decoding the OTP and displaying it on the customer's mobile directly, we propose a new authentication system for online banking which will provide greater security and convenience by using mobile OTP with the QR-code.

In our proposed system, we are going to develop two softwares for the online banking system:

1. An android based mobile software which will scan the QR code generated by bank server and decipher the OTP.
2. An online portal (website) that provides E-banking facility.

Working of our proposed system is as follows:

1. A customer of the bank must initially register with the bank for using online banking services so that the bank can store the customer's particulars in their databases, a customer is ideally required to register only once unless he/she misplaces his/her phone and starts using another mobile device or purchases a new device, in such cases the customer must register the IMEI of his/her new handset with the bank.
2. The customer then logs onto the banking portal using the provided conventional username and password.
3. The customer either browses the portal or initiates an online transaction. In case the user initiates an online transaction then the process of generating an encoded OTP is started on the server side by the bank's servers.
4. Based on the customer id, current system time and a random number (3 parameters) OTP1 is generated, this is an internal result of system processes and is not visible to the user
5. OTP2 is generated on the bank server using OTP1 + the user's IMEI number and a certain permutation and combination logic. OTP2 is stored on the bank server and is then encoded in a QR code. This QR code image is the final result of the encoding process. The QR code is then made visible to the customer on his/her computer screen.
6. The customer is then required to scan the QR code by using the bank's android QR code scanner application and obtain the OTP.
7. The customer then enters the OTP in the banking portal.
8. The OTP entered by the user on the portal and the OTP saved on the bank's server are compared, if they match then transaction proceeds to completion and the bank's databases are adequately updated otherwise if the two OTPs do not match then the transaction fails.
9. Each OTP may be used only once and must be used within a period of 5 minutes from being delivered to the user, failing to use the OTP within the specified time interval renders it invalid and in such a case a user must request a new OTP in order to proceed with the transaction.

A customer can use the banking system for following services:

1. Viewing account balances, viewing recent transactions, ordering cheque books
2. Online fund transfers between different customer accounts
3. Pay bills online

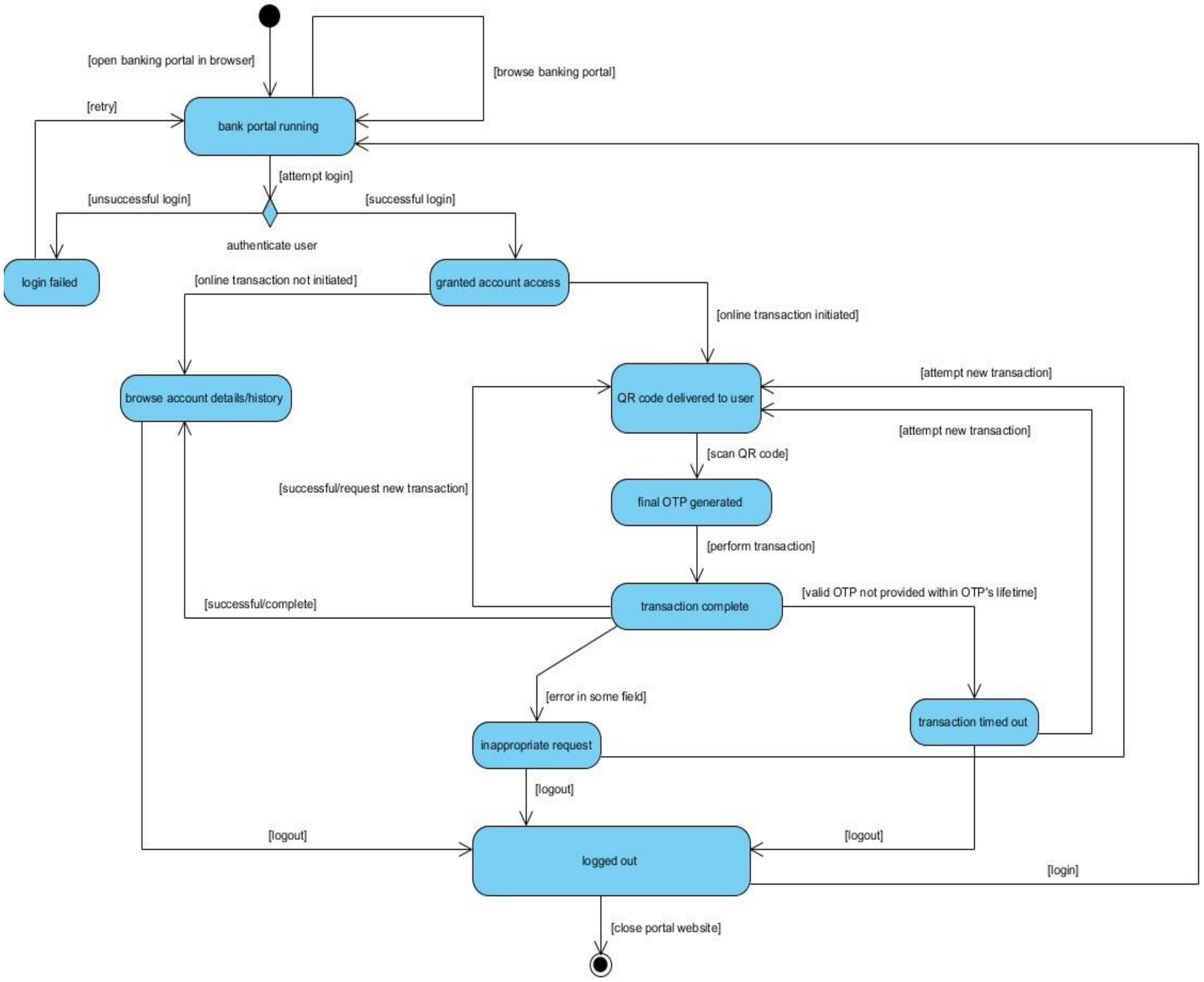

Fig.3 Activity diagram of the proposed system

V. CONCLUSIONS

We have proposed a new authentication system for online banking using existing technologies like QR scanning and OTP but combining their functionalities to build a security system with unique features like QR code encoding using IMEI number and registered device specific decoding of QR to obtain OTP. Since there is no exchange of OTP over networks the proposed system currently appears to be quite secure. Furthermore, an OTP has a lifetime of only 5 minutes which means that even in the rare case that a sophisticated hacker obtains the transaction OTP the transaction is either likely to have been completed or the OTP is likely to have expired. What will be interesting to see is where such two factor authentication systems will be used in the future, such systems are still in their infancy and are being developed and worked upon with great interest keeping in mind the growing audiences of both online monetary transactions and scanning capable smartphone users.

REFERENCES

[1] Mete Eminağaoğlu, Ece Çini, Gizem Sert and Derya Zor **“**A two-factor authentication system with QR codes for web and mobile applications” IEEE 2014.

[2] Raed M. Bani-Hani, Yarub A. Wahsheh and Mohammad B. Al-Sarhan. “Secure QR Code System” IEEE 2014.

[3] Somdip Dey, Asoke Nath and Shalabh Agarwal "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System" 2013 International Conference on Communication Systems and Network Technologies IEEE 2013.

[4] Wikipedia, Retrieved March, 5, 2015, from http://en.wikipedia.org/wiki/QR_code.

[5] Wikipedia, Retrieved March, 5, 2015, from http://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity