IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Online Banking System using Mobile-OTP with QR-code

Amandeep Choudhary[1], Shweta Rajak[2], Akshata Shinde[3], Siddeshwar Warkhade[4], Prof. F.S. Ghodichor[5]

Student, Information Technology, Sinhgad Institute of Technology, Lonavala, Pune, India [1]

Professor, Information Technology, Sinhgad Institute of Technology, Lonavala, Pune, India [5]

Abstract: As a high-speed internet infrastructure is being developed and people are information zed, the financial tasks are also engaged in internet field. However, the existing internet banking system was exposed to the danger of hacking method such as Phishing or Pharming beyond snatching a user's ID and Password. Several techniques have been developed that help to protect transactions performed over insecure channel. Like which provides security by generating passwords. However, this technique is not that much beneficial for user. To provide more secure channel, we are implementing security on Banking transaction by using OTP with QR code. QR Code is a 2D matrix Bar Code where the information is stored both in horizontal and vertical dimensions. QR Code can hold a larger amount of data in a compact space and can perform error-correction at higher speed and has faster response time. QR Code is versatile and is used in various fields such as online banking, managing attendance, help visually impaired people, security applications such as different kinds of cryptography and steganography as well. Secure authentication, is achieved using data-hiding algorithms with the embedded QR Code.

Keywords: Privacy Preserving, QR Code, Encryption, OTP Generation, Integrity.

I. INTRODUCTION

In traditional signature mechanisms, the user who applies a signature has full control over the signature method. However, within the case of electronic signatures the user depends on a shopper that always can't be trusty. Notwithstanding a secure revolving credit is employed, the user is commonly unable to claim that the knowledge displayed on the screen is truly up to the knowledge signed by the revolving credit. This drawback is gift altogether kinds of electronic transactions that need some style of signature by the user .Examples embrace on-line banking and electronic signatures for contracts. The most drawback is that data on the shopper may be haphazardly changed by malicious code. One among the countermeasures that draw high attention of the money agencies is OTP (One Time Password), one among the user confirmation strategies is introduces, and Joint Confirmation Canter of OTP is established .The Online money dealing within the gift is apply a security card and public key certificate that are the strategies confirming a user, and recently OTP was new introduced.. Besides, OTP options namelessness, movableness, and extensity, and allows to stay the knowledge from being leaked.

II. MOTIVATION

Meanwhile, the utilization of electronic banking services is inflated gradually in lifestyle and presently on-line banking needed the utilization of security card from every banks. But this service victimization security card doesn't suite trendy Mobile surroundings as a result of we tend to don't grasp once and wherever on-line banking and can be used. If there's emergency state of affairs to try and do on-line banking, the web baking can't be kept away from the protection card. So as to beat such a weaknesses and inconvenient of security card, our propose authentication
System use two-dimensional barcodes (2D Barcode) rather than security card. Barcode is quick, easy, correct and automatic information assortment methodology. Barcode allows product to be half-tracked expeditiously and accurately at speeds web attainable victimization manual information entry system. During this paper, we tend to propose authentication system for on-line banking which might offer bigger security and convenience by mobile OTP with the QR-code, one among the 2nd barcode adopted by current international and national standards. . Afterward use to a portable generates the OTP code with the input of transfer data and hashed user's mobile serial variety. Then user enters the generated OTP code, to complete the transfer method.

III.LITERATURE REVIEW

1. Modern Applications of QR-Code for Security

With the large growth of technology, QR Code has a large vary of applications.

DOI10.17148/IJARCCE.2017.64125

QR Code may be a 2nd matrix Universal Product Code wherever the data is keep each in horizontal and vertical dimensions. QR Code will hold a bigger quantity of information during a smaller area, performs reliable error-correction at higher speed and has quicker latency. Increasing use of sensible phones among all age teams created accessing QR Code easier by providing end-user content, together with net links, personal details etc. QR Code is flexible and is employed in various analysis fields like on-line banking, group action management, health care, facilitate visually impaired folks, security applications like totally different styles of cryptography and steganography still. Secure authentication, is achieved victimization data-hiding algorithms with the embedded QR Code. This paper highlights security aspects handled by QR Code in several applications and more directs to secured transportation of the info victimization SQRC that has its real time applications like vehicle and identity verifications.

2. "A Secure Mobile Payment System using QR Code:

Mobile phones became an indivisible companion for several users, serving way more than simply communication tools. In developing countries, the amount of mobile users exceeds the amount of these having bank accounts. Besides, the low banking service penetration and therefore the massive migrant communities are another issue to utilize mobile phones for payment functions. Therefore, mobile payment might realize the success it's targeting simply and far quicker than in developed countries. There are lots of variables concerned associated with Mobile Payments. During this paper, the varied models used for Mobile payments are initial mentioned. Then, the paper can propose a state of affairs for mobile payment that tackles each considerations of the method, namely: speed of group action and security, while not complicating the method or creating it undesirable to users

3. "QR-TAN: Secure Mobile Transaction Authentication

This paper contributes with the QR-TAN authentication technique. QR-tans area unit a dealing authentication technique supported two-dimensional barcodes. Compared to different established techniques, QR-tans show 3 advantages: initial, QR-tans enable the user to directly validate

The content of a dealing among a sure device. Second,validation is secure notwithstanding associate offender manages to achieve full management over a user's laptop. Finally, QR-tans together with sensible cards may also be utilised for offline transactions that don't need any server

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

This paper explains implementation details of on-line banking authentication system. Security is associate vital issue for on-line banking application which might be enforced by varied web technologies. Whereas implementing on-line banking system, secure information transfer want is consummated by exploitation https information transfer and info encryption techniques for secure storage of sensitive info. To eliminate threat of phishing and to substantiate user identity we have a tendency to ar aiming to use conception of QR-code with robot application. QR-code which might be scanned by user mobile device that overcome the weakness of ancient countersign based mostly system. We have a tendency to improvemore security by exploitation only once countersign (OTP) that hides within QR- code

.

5. "OTP-Based Two-Factor Authentication Using Mobile Phones:"

Two-factor authentication (2FA) provides improved protection, since users are prompted to supply one thing they understand and one thing they need. This methodology delivers a higher-level of authentication assurance, that is important for on-line banking security. Several banking systems have happy the2fa needs by causation a one Time password (OTP), one thing possessed, through AN SMS to the user's phone device. Unfortunately, international roaming and SMS prices and delays place restrictions on this technique reliableness. This paper presents a unique two-factor authentication theme whereby a user's device produces multiples otps from AN initial seed mistreatment the planned production theme. The initial seed is created by the communications partners' distinctive parameters. Applying the numerous from one operate to an exact seed removes the necessity of causation SMS-based otps to users, and reduces the restrictions caused by the SMS system.

IV. PROPOSED SYSTEM

Traditionally, for banking transaction people use to go bank to do transaction's procedure, this become hectic to customer. Then NFC card ,which is nearest field communication came into picture which is a 1D security card .But user has to carry that card whenever transaction is required .If user fails to bring NFC card during transaction or user lost the card, then no transaction will be done which is again drawback of NFC card. To overcome from this problem we are implementing online banking transaction by using OTP which is hidden inside a QR code. In this, there no need to remember password or there no need to keep card all the time for doing transaction.

One Time Password is a 1D password system which is validate only one time for a valid user within a specific time. Hence each time user will be authenticated with a new passwords .It helps in preventing various types of attack like

DOI10.17148/IJARCCE.2017.64125

replay attack , phishing attack and many more which is using static passwords[1].It provides security by ensuring that user cannot use same password again and again. It also offers other characteristics like anonymity, portability, extensibility and enable to keep information safe or from being leak [2].There are two approaches for generating an otps:

1. Time based OTP- In these OTP changes at frequent interval of time.
2. Event based OTP- In these OTP will be generated by pressing a button on the OTP device or token.

On the other hand, QR –code[3]is a Quick Response 2D barcode which is used to store information into an image forms.It provides more security ,more storage for storing information.These are proven by ISO standards that contain information in both horizontal and vertical directions, whereas 1-D barcode contains information only in one direction either horizontally or vertically. It also provides error correction capability. Data can be recovered easily even the some part of the image is damage or distorted. There will be no loss of data. Users can decide what action should be taken or what information are needed to store inside a QR code. QR-CODE can store 7089 characters as compare to bar code which store only 20 digits [4]. We can store URL, text, images , geolocations, and other forms of data.

V. IMPLEMENTATION

During online transaction. The reliable security solution is very important. Even if a secure smart card is used, the user is often not able to assert that the information displayed on the screen is actually equal to the information signed by the smart card. The main problem is that information on the client can be arbitrarily modified by malicious software. In Secure Input for Web Applications .the three phases of an attack against a user's computer redescribed. In the first phase, executable malware is installed on the computer. In the second phase, the malware monitors the user's interaction with the Web based system. If the malware detects a security critical operation, it modifies or captures the transmitted information in the final phase.

In our proposed system we are going to use OTP and Qr-code. A Qr-code consisting a private key will be generated between client and server. Along with this an OTP will be hidden inside this QR-code which will be used later on for providing authentication to the authorized user only. The basic architecture of our system.

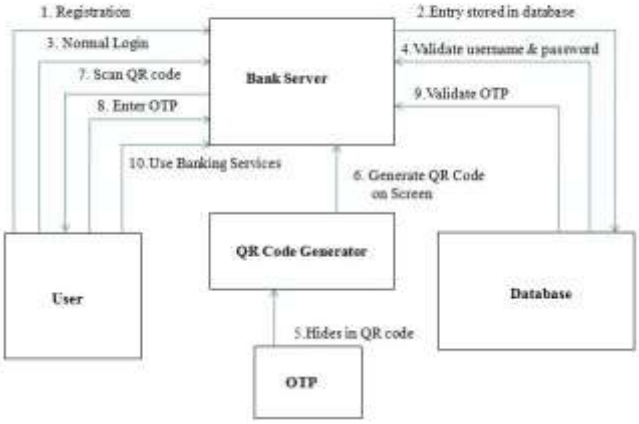

Fig1: Architecture Design

- How system works

Our system comprises of mainly four steps:

1. Setup Phase
2. Phase OTP Generation Phase

DOI10.17148/IJARCCE.2017.64125

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

3. QR code Scanning Phase
4. Payment Complete Phase

- Setup Phase: The setup algorithm takes no input other than the implicit security parameter. It stores the user's information into the database.
- QR Code Generation PHASE:- When the user selects the QR code, they can scan it with their mobile phone with the help of QR-code reader. The QR code reader decrypts the code and the mobile phone show the hidden OTP. Every QR code contains OTP but the OTP is different for all the user. This parameter is used to help the detection script to determine the type of scanned code.
- OTP Generation Phase:-One-time passwords is a unique password generated for a specific timestamp .This ensures that a username or password combination cannot be used second time. Usually the user's login name remains unchanged, and the OTP changes for each login. Hence for each session the user will be validated with the new OTP. One-time passwords are a form for providing strong authentication, and offer more effective security to corporate networks, online bank accounts and other systems containing confidential data. The very important parameter that is addressed by one time passwords in contrast to the traditional passwords is that , they are not vulnerable to replay and phishing attacks.
- Payment Complete Phase : 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.

VI. SECURITY ANALYSIS

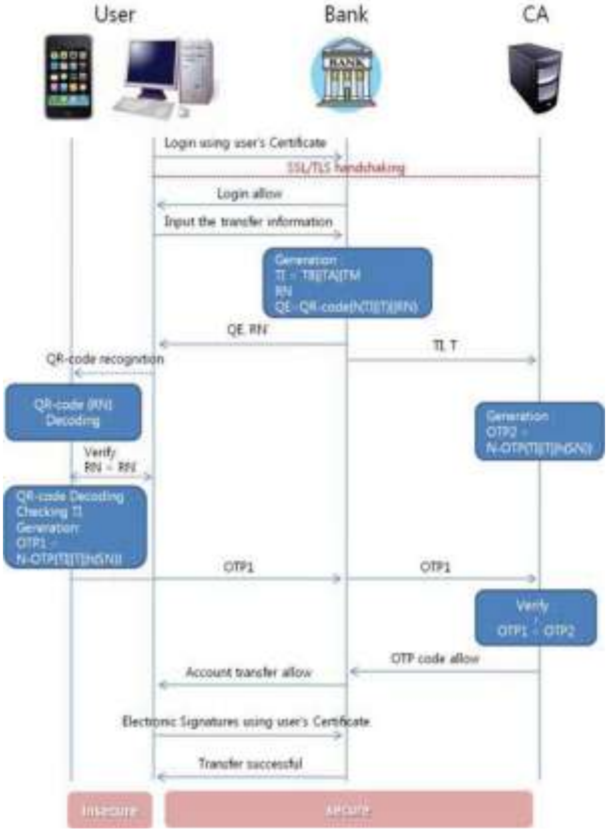

Fig.2 Authentication System

Assume the secure communication through SSL/TLS tunnel between user (PC) and certification authority (CA) and repair suppliers (Bank). Therefore a malicious user cannot analyze the content of communications as our projected system use the camera of mobile device to acknowledge of QR-code, doesn't separate to communicate between the user's computer and mobile devices. Conjointly the user and certification authority (CA) has been shared the hashed the serial variety (SN) of user's mobile device through a secure method within the initial registration section. If a counterfeit or altered the PIN, the OTP worth is modification. In our projected system, the user to forestall Phishing attacks by distinctive the worth of random number (RN) before to verify the knowledge of dealing once the conversion of QR-code. When confirming a legitimate service supplier ,information of dealing is born-again. If a counterfeit or

DOI10.17148/IJARCCE.2017.64125

altered the random number (RN) and also the info of dealing, the generation of OTP are often stopped by discretion of the user. Meanwhile, our projected system need a necessity input of dealing info exploitation QR-code and approved authentication by the general public certificate for the generation of OTP. Through this method, known as legitimate users and may block the utilization of malicious user. Conjointly the continuance accustomed generate the OTP code isn't attainable to vary randomly as a result of we have a tendency to used the user's requested time of transfer.

VII. CONCLUSION

This paper concludes that there are so many possibilities for QR Code's use in different areas for authentication and to provide security and lot more are yet to be explored. In many countries, QR codes are used in most of the commercial market items. Essentially, QR codes are a convenient way to add the virtual to the physical to provide useful content, often at the time of need. QR codes are a low threshold technology, easy to use and implement and its cheap. QR Code has various applications in numerous fields. Online banking which involves high security transactions are made even more highly protected using QR codes .OTP distribution is made accessible by authenticated users with the help of QR codes.

ACKNOWLEDGMENT

The heading of the Acknowledgment section and also the References section should not be numbered. It offers us nice pleasure in presenting the preliminary project report on 'ONLINE BANKING SYSTEM USING MOBILE-OTP WITH QR-CODE' . I might wish to take this chance to impart my internal guide for giving me all the assistance and steering I required. I'm very grateful to them for his or her kind support. Their valuable suggestions were very useful. I am additionally grateful to Head of COMPUTER ENGINEERING Department ,SITCOE for his indispensable support, suggestions. In the finish our special due to different Person Name for providing numerous resources like laboratory with all required software system platforms, continuous internet association, for Our Project.

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] antiphishinggroup, "Phishing Activity Trends Report",from: http://www.antiphishing.org, Dec. 2008.
[3] Sang-Il Cho, hoonjae Lee, Hyo-Taek Lim, Sang-Gon Lee, "OTP Authentication Protocol Using Stream Cipher with Clock-Counter", October, 2009.
[4] Jean-Daniel Aussel, "Smart Cards and Digital Identity", Telektronikk 3/4. 2007. ISSN 0085-7130.
[5] 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.
[6] IETF RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm, Dec. 2005,
[7] ISO/IEC 16022:2000 – Information Technology – International Symbology Specification – Data Matrix, 2000.
[8] ISO/IEC 18004:2000 – Information Technology – Automatic Identification and Data Capture Techniques – BarCode Symbology – QR Code, 2000.
[9] 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.
[10] Reilly, D., Smolyn, G. and Chen, H., "Toward fluid, mobile and ubiquitous interaction with paper using recursive 2D barcodes", Pervasive Mobile Interaction Devices 2007 (PerMID2007), workshop at Pervasive 2007, Toronto, Canada, 2007.

DOI10.17148/IJARCCE.2017.64125