A Survey on Secure OTP With QRCode Mobi Shopping

Mrs. Kavitha Bai A S[1], Assistant Professor

Madhu R Muchandi[2], Vidhya Bushan M N[3], Sindhu Shree B N [4]

[1,2,3,4] Department of CSE, [1,2,3,4]Vemana Institute of Technology
Bengaluru -34 India.

Abstract— *online shopping has a huge scope because of busy life. Major security issues arises with online shopping i.e., third party attackers may hack data. Secure OTP codes with Quick Response mechanism is proposed to overcome security issues. Fast QR filtering technique is developed to get information quickly which is hidden inside QRcode for the security purpose. To make payment for selected products, first credit card information has to be given. Credit card details are validated, QRcode image is generated. Generated OTP is hidden in QRcode image and sent to credit card linked user mail-id. If scanned OTP is validated then payment is made successfully.*

Keywords — *QR Code, Fast QR filtering technique, Security*

I. INTRODUCTION

Recent advancement of smartphones and tablet computing devices has witnessed the increasing popularity of short-range wireless-communication in many mobile applications and services, such as mobile advertisement, contactless mobile payment and device pairing, etc. For instance, Near Field Communication (NFC)[2] enables the devices to have low-power radio communication between them by a simple touch. Although Near Field Communication (NFC) allows two NFC-enabled devices to communicate with each other, it is possible that a third device could intercept the data. Three major concerns related to data interception are data corruption, data modification, and data insertion. Data corruption involves transmitting valid frequencies at well-timed intervals. NFC is higher cost than QR-codes. With the rapid increase and growth of inexpensive cameras such as in cell phones or webcams, the consumer use of barcodes is becoming popular. A consumer can take an image of the back of a product with the barcode printed on it with his cell phone camera or webcam. A computer vision algorithm localizes and segments the barcode, and the bits extracted are passed to the appropriate decoder, and once the product is identified, the information pertaining to the product can be retrieved. The QR code system was invented in 1994 by Denso Wave and its ambition was to track vehicles during manufacturing; it was designed to allow high-speed component scanning. QR codes shown in fig1 are now used in a much broader ambience, including both commercial tracking applications and convenience-oriented applications aimed at mobile-phone users. QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode. A barcode is a optical label that a machine can read which contains information about the item to which it is attached. QR Code is capable of handling several dozen to several hundred times more information than conventional barcodes which are capable of storing maximum of 20 digits approximately. QR Codes also have error correction capability. Though the symbol is partially dirty or damaged data can be restored and to maximum of 30% of code words can be restored. In our paper, we investigate secure barcode-based communication for smartphones. QR-TAN [4] was proposed to use QR codes as a VLC channel for transaction authentication. A new system is designed that can stream QR codes between smartphones at a throughput comparable to that of state-of-art NFC systems. Because of the inherent directionality, the (VLC) visible light communication channel of barcode exchanges yields some interesting security properties.

We present secure barcode-based visible light communication (SBVLC)—a novel secure ad-hoc wireless communication system for smartphones. Unlike NFC, SBVLC can be widely adopted by most off-the-shelf smartphones. It works across various smartphone platforms equipped with a colour screen and a front-facing camera. Our system can also be easily extended to support other mobile and portable devices such as laptops and tablets. To quickly remove the non-QR and duplicate QR frame images- Fig.1.1 we developed a fast QR filtering technique.

Fig.1.1 QR Code

A system architecture as shown in Fig.1.2 is a conceptual model that defines the structure, behavior, and more views of a system. A system architecture can encompasses system components that will work together to implement the overall system. Wireless Application

Protocol (WAP) a technical standard is used for accessing information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones that uses the protocol. Web server contains database to store admin details for server-side authentication. Webserver provides product details to the users on client-side and accepts credit card details. If valid, generates QRcode in which the OTP is hidden through encryption, sends this encrypted OTP to mail. On client side, smart phones with QRcode scanner scans the QRcode and decrypted OTP is obtained. If OTP is valid, then it begins the payment process.

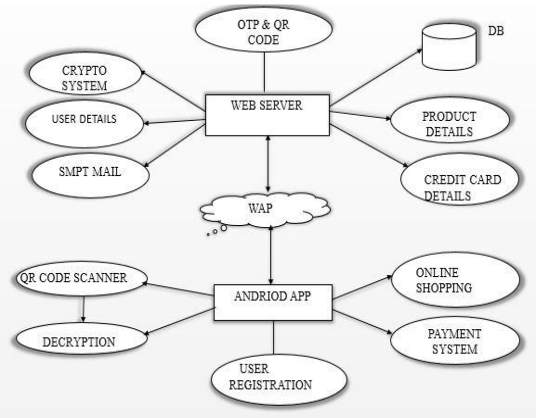

Fig.1.2 System Architecture

II. LITERATURE SURVEY

Near Field Communication (NFC)[1] a short-range RFID technology intended to equip mobile devices with a contactless communication channel companionable with present contactless technology. NFC-enabled mobile devices are prone to Relay attacks. In [2] We contemporary a real-world application of an NFC-enabled relay attack, demanding only appropriate mobile software applications. To perform a relay attack, the opponent wants two devices, which act as a token and a reader respectively. These devices are linked via a correct communication channel in order to transmit data over a greater distance. The proxy-reader is used to communicate with the real token, while the proxy-token is located near the real reader. Any data transmitted by the reader is acknowledged by the proxy-token and relayed to the proxy-reader, which will transfer the data to the token. The token assumes that it is communicating with the reader and answers accordingly. The token's reply is then dispatched back to the proxy-token, which will transmit the information to the reader. The goal of the attacker is to certify that the reader is unable to distinguish between the real token and the proxy. Our relay attack establishes a compact complexity of attack as it did not require special hardware. The attack implementation required no unlocking of devices or secure elements, no hardware or software modification to the phone platform, and minimal knowledge of the data that was to be relayed. Neither was there any necessity to entrance the mobile network or any related services, and we utilised devices of a form factor accepted by merchants. The attack implementation was application independent so would work against a number of conventional contactless systems.

Priwhisper[2] a keyless secure acoustic short-range communication organization for smartphones. It adopts the emerging friendly jamming technique from radio communication for data privacy. The plan prototype is implemented and evaluated on several Android smartphone stages for efficient and usability. Firstly, transmission of acoustic signal does not require line-of-sight, which bids Priwhisper much higher usability than the barcode based communication system. Secondly, the computational power of most smartphones are sufficient to modulate/demodulate acoustic signals using a software acoustic modem. Hence such acoustic communication system can be deployed on most off-the-shelf smartphone platforms. Acoustic channel is a full-duplex channel that supports android smart phone platforms, but is not well-suited with the major smart phone OS's such as iOS.

Quick Response-Transaction Authentication Numbers (QR-TAN) [4] use a method based on transaction-signing that has been adapted to fit the skills of commonly used Web-based applications. QR-TANs are based on two-dimensional QR barcodes QR-TANs authenticate transactions by consuming a trusted device. This device can be a mobile phone with a display and a camera with a modest resolution. QRTANs use QR codes for the transmission of information. QR-TAN method only requires the user to authenticate the transaction on her trusted device and to approve the transaction by entering a short number into her computer. Advantages of QR-TANs are they allow the user to openly authorize the content of a transaction within a trusted device. Secondly, validation is secure even if an attacker achieves to gain full control over a user's computer. Finally, QR-TANs in blend with smart cards can also be used for offline transactions that do not require any server. Limitations of QR-TANs are they do not address the refuge the barcode-based VLC channels, it is based on half duplex communication mechanism.

III.PROBLEM STATEMENT

Design ideologies of 2D barcode makes it difficult to add security features and include private information sharing. Hacking of OTP is possible which is misused in money transfer.

IV.EXISTING SYSTEM

2d barcodes have been increasingly used for security sensitive mobile applications including mobile payment and personal identification. The study of barcode safety in applications of mobiles has not been systematically studied. Difficult to add security and eavesdropping in 2D barcodes.

V. PROPOSED SYSTEM

We are proposing Secure Barcode-Based Visible Light Communication for Smart phones, Quick response (QR) codes are scanned using smart phones as shown in Fig.5.1. We advanced a fast QR filtering method to rapidly to get information which is hided inside the QR code for the security persistence. Security contactless payment and security exposures such as eavesdropping and jamming.

Fig.5.1 QR code scanning

VI.DESIGN PHASE

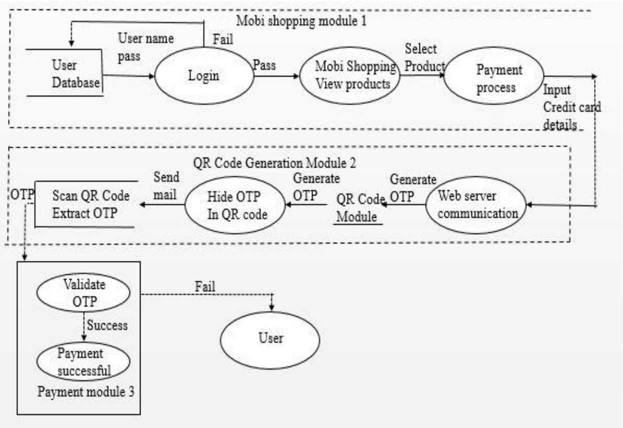

Fig.6.1 Data Flow diagram

A data flow diagram (DFD) is a graphical depiction of the movement of data, through an information system, and sculpting its process phases. Fig 6.1 shows dataflow diagram with three different modules: Mobi Shopping module, QRcode generation module, Payment module. Mobi Shopping module represents the process of shopping in which the user signs into the app and starts viewing the products, once the product is selected the payment must be done through the input of credit card details. The second module represents the web server communication and the generation of OTP which is hidden in QR code. The mail will be received by the user and the user scans the QR code with the help of mobile device and extracts the OTP. The third module is all about Payment process in which the OTP is validated and payment is done successfully.

.

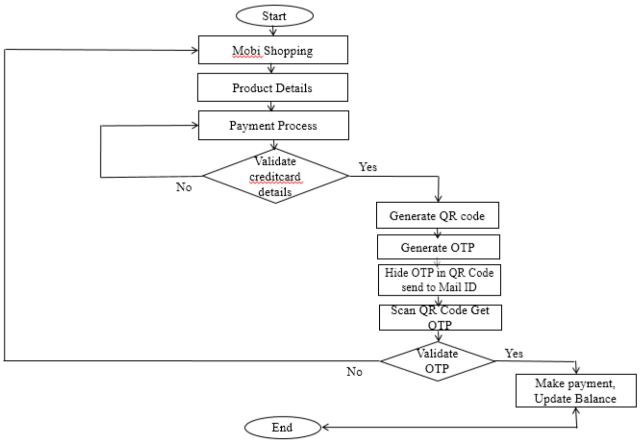

Fig.6.2 Flow chart of QR code generation

A flow chart is the step by step process to solve a given problem in a systematic way as shown in Fig.6.2 once the details and payment process is done, credit card details validation takes place, if no problem occurs, QR code and OTP will be generated and OTP will be hidden in QR code which is sent to mail-id. OTP will be retrieved after scanning and validated. Payment process takes place once the OTP validation is successful.

VII. METHODOLOGY

i. Web Server Module (J2EE)

In this web server module product details and credit/debit card details is added and maintained in the database.

ii.Login and Registration Module

After the registration phase user has to enter his username and password for the login phase, after the validation of the username and password it will redirect to home page.

.

iii.QR Code generation module(Android) and mail sending process

In this module user can purchase the products by giving credit card details, first credit card will be verified for primary account number. If valid it will check for current balance to buy the product and if the balance is less than the product price, popup alert message will be given to user informing account balance is low. If balance is satisfied QR code with a encrypted OTP will be sent to mail-id through SMTP protocol.

iv.OTP Validation and Bill Paying Process

After the validation of OTP , bill is paid and remaining amount is updated to credit card.

III.CONCLUSION

One time password (OTP) can be hacked and misused in money transfer. To overcome this problem we develop a innovative OTP transfer with encryption technique and also which is hidden in QR code that double protection in money transfer.This system has two sides, one is web server and another is client android application. We tested with experimental data and all the result shows system meets the functional specification of the system.

.

REFERENCES

[1] B. Zhang, K. Ren, G. log Xing, X. Fu, and C. Wang, "SBVLC:Secure barcode-based visible light communication for smartphones," in Proc. IEEE Conf. Comput. Commun., 2014, pp. 2661–2669

[2] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using NFC mobile phones," Cryptology ePrint Archive, Tech. Rep. 2011/618, 2011.

[3] G. Starnberger, L. Froihofer, and K. M. Goeschka, "QR-TAN: Secure mobile transaction authentication," in Proc. Availability, Rel. Security, Mar. 2009, pp. 578–583.

[4] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[5] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/