Scientific Journal Impact Factor (SJIF): 1.711

IJMTER

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

2D Barcode Based Mobile Payment System With Biometric Security

Pragyan A Masalkar (Be Comp)[1], Udayraj Singh (Be Comp)[2], Sayali Shinde (Be Comp)[3]

[1,2,3] G H Raisoni Institute of Engineering & Technology.

Abstract— Currently Indian market doesn't use 2-D based Barcode Mobile. In market or malls 1d barcode system is used and queue line system is used thus it is time consuming. In market most of mobiles don't have barcode detection system in them; only phones like iPhone have it. Money transaction system in market is also slow and credit cards and other money payment system are used. Mobile payment is very important and critical solution for mobile commerce. A user-friendly mobile payment solution is strongly needed to support mobile users to conduct secure and reliable payment transactions using mobile devices. We will present an innovative mobile payment system based on 2-Dimentional (2D) barcodes for mobile users to improve mobile user experience in mobile payment. Comparatively our system is time saving. A user-friendly mobile payment solution is strongly needed to support mobile users to conduct secure and reliable transactions using mobile devices.

Keywords— Mobile Payment, POS, Payment System-Commerce, 2D-barcode

I. INTRODUCTION

Currently Indian market doesn't use 2-D based Barcode Mobile. In market or malls 1d barcode system is used and queue line system is used thus it is time consuming. In market most of mobiles don't have barcode detection system in them; only phones like iPhone have it. Money transaction system in market is also slow and credit cards and other money payment system are used. Mobile payment is very important and critical solution for mobile commerce. We will present an innovative mobile payment system based on 2-Dimentional (2D) barcodes for mobile users to improve mobile user experience in mobile payment. Comparatively our system is time saving. A user-friendly mobile payment solution is strongly needed to support mobile users to conduct secure and reliable transactions using mobile devices. This project is about to implement an innovative mobile payment

System based on 2-Dimentional (2D) barcodes for mobile users to improve mobile user experience in Services based on 2D Barcodes. We will present an mobile payment which will support buy-and-sale products and innovative mobile payment system based on 2-Dimentional (2D) barcodes for mobile users to improve mobile user experience in mobile payment. Unlike other existing mobile payment systems, the proposed payment solution provides distinct advantages to support buy-and-sale products and services based on 2D Barcodes. This system uses one standard 2D Barcode (Data Matrix) as an example to demonstrate how to deal with underlying mobile business workflow, mobile transactions and security issues.

A. Types of 2D Barcodes

Traditional barcodes stored data in the form of parallel lines in different widths, and they are known as 1D barcodes (or linear barcodes). A linear barcode refers a way of encoding numbers and letters in a sequence of varying width bars and spaces so that it can be read, retrieved, processed, and validated using a computer. Linear barcodes have been used for 30 years since they were firstly used in railway transportation for tracking of the goods in USA. Today, as machine-readable representation of information in a visual format, linear barcodes have been used almost everywhere, such as manufacturing, postal, transportation, health care, retail business, and automotive business. Since barcodes can be easily stored, transferred, processed, and validated in a digital form, Barcode identification provides a simple and inexpensive way of encoding text information that is easily read using electronic readers. Hence, using barcodes provides a fast and accurate tool to enter data without keyboard data entry.

There are two types of 2D-barcodes: 1) stacked 2D- barcodes, such as PDF417, and 2) Matrix 2D-barcodes, such as Data Matrix and QR Code. Figure12 illustrates different types of these barcodes namely, Code 49, QR Code, PDF417, and Data Matrix.

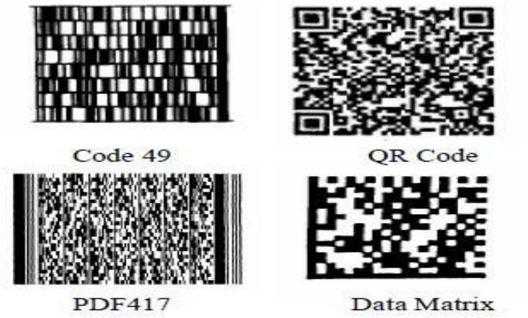


Figure12. Different kinds of 2D-Barcodes

Table1. 2D-Barcoes Comparison

	QR Code	**PDF 147**	**Data Matrix**	**Maxi Code**
Developer	DENSO (Japan)	Symbol Technologies	RVSI Acuity CiMatrix	UPS (USA)
Numeric	7,089	2,710	3,116	138
Alphanumeric	4,296	1,850	2,355	93
Binary	2,953	1,018	1,556	
Kanji	1,817	554	778	
Major features	Large capacity Small printout High speed	Large capacity	Small printout size	High speed scan
Standards	AIM International ISO JIS	AIM International ISO	AIM International ISO	AIM International ISO

Compared with 1D barcodes which hold vary limited information data, 2D barcodes have a much larger capacity to hold more information data. As shown in Table 1, a QR code can holds up to 7,089 digits, 4296 letters, and 2953 binary data. Selecting and using 2D barcodes must consider the following factors: a) the application usage, b) standard, c) implementation, d) the data to be encoded in barcodes, and d) barcode printing format. Recently, 2D barcodes gain its popularity in many business applications due to the advantages of holding more data information and presenting in a smaller area. However, 2D barcodes require sophisticated devices for decoding, which was a challenge until recently. Today, with the advance of the image processing and multimedia capabilities of mobile devices, they can be used as portable barcode encoding and decoding devices.

II. PROPOSED SYSTEM

The proposed system has a broader scope in the future because this application can be used in malls for purchasing of items. New customer will register to system through admin and that information of customer will be stored into database along with his/her fingerprint and face image for authentication through biometric equipment.

The proposed application is installed in Wi-Fi enabled mobile having more than 2 megapixel camera of registered customer. A mall contain local server connected with database of product and customer. So customer has to connect their mobile to local server via Wi-Fi and need to login with registered ID and password.

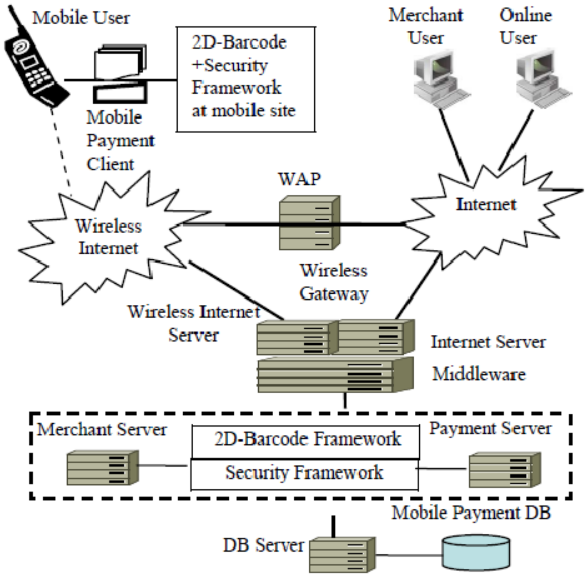


Fig 11. The 2D Barcode-Based Payment System Infrastructure

A customer has to capture 2D barcode which will be decoded by proposed application. This decoded barcode data will be sent to local server. Given data will be compared with database and corresponding detail of given product like product id, name, price, quantity, expiry date, packing date, manufacturer on mobile screen will be displayed. Customer has to choose option as ‘add to cart’ or ‘remove from cart’. So finally customer will purchase the cart which contain list of items to be purchased. After that he/she will select the payment option. Payment can be done in three ways: SBI account, prepaid account and PayPal. Customer gets notification about payment transaction and he/she can able to view his/her balance. Customer can share scans with his/her friends via social Medias like Facebook, twitter.

All the details of purchased products and amount will be transferred to admin database. Admin can view details of transactions of customer through web based module. Admin can update customer’s profile and also he will be able enter information of new product, update stock and analysis of sell to smoothen the business. If there are any new schemes (like discount etc.) going on in mall then customer will be notified with the help of SMS messages. Customer will be authenticated at gatekeeper through biometric equipment and gatekeeper will generate the bill receipt

A) Customer

User can get registered to the application easily. Here user have to fill the information like User Name, Address, Mobile Number, Password Etc. & click on Register Button. User get registered by server & information entered by the user is saved in database. Customer has to register with all his details like name, mobile no., email_id, address, and most importantly his/her Finger Print which will be store in java media framework tool.

B) Admin

Admin has the right to monitor all the transaction of the user and he can add the product in the list and can alter all the data about the product. The sub module Gatekeeper is use to check whether customer is valid or not and also to check correct count of product and payment customer has made. Gatekeeper also sends paperless bill with all details to the customer

C) Merchant Server

The merchant server will save the details of the product and the details of the registered user. While the product registration the server will generate the 2D barcode of the product which will add all the details of the product. In Customer Database All information with fingerprint of the customer is store. In Product Database All Product details with barcode is store with their prices. In Daily/Weekly Stock Database Daily or Weekly details regarding products, Customer etc are store for further usage. And In Mobile Payment Database All Payment details are store in this database sub-module. The Techniques that are going to be used are wireless internet server (Tomcat server) and other Java related middleware, such as Java 2 (J2SE), Bouncy Castle Crypto Library, JSON utility, Java DB connectivity and Java Servlet technology. Tomcat server are used for database maintenance purpose. Java DB connectivity to be done with java web module for connectivity purpose. Java Servlet technology is use for server side programming purpose through which dynamic data is access with servlet.

D) Payment system

Wireless-based (or mobile) payment systems could be classified into the following types.

(A1) Account-Based Payment Systems

In account-based payment systems, each customer is associated with a specific account maintained by the Trusted Third Party (TTP) like a bank (or a Telco). In pre-paid transactions, this account will be directly linked to the consumer’s savings account. The consumer maintains a positive balance of this account which is debited when a pre-paid transaction is processed. If post-paid transactions are supported, the charges from a transaction are accrued in the consumer’s account. The consumer is then periodically billed and pays for the balance of the account to the TTP. Account-based payment systems can be classified into FOUR categories:

- ***Mobile Phone-Based Payment Systems*** – They enables customers to purchase and pay for goods or services via mobile phones. Here, each mobile phone is used as the personal payment tool in connection with the remote sales. A phone card-based payment system has the advantage over the traditional card-based payment in that the mobile phone replaces both the physical card and the card terminal as well. Payments can take place anywhere far away from both the recipient and the bank.

- ***Smart Card Payment Systems*** – They use a smart card, an embedded microcircuit, which contains memory and a microprocessor together with an operating system for memory control. These smart cards can be used for electronic identification, electronic signature, encryption, payment, and data storage.

- ***Credit-Card Mobile Payment Systems*** – This type of mobile payment systems allow customers to make payments on mobile devices using their credit cards. These payment systems are developed based on the existing credit card-based financial infrastructure by adding wireless payment capability for consumers on mobile devices. The existing SET secure protocol, developed by Visa and MasterCard for secure transfer of credit card transactions, has been extended and known as 3D SET to support mobile payment for mobile device users.

- **Mobile POS (Point-Of-Sale)-** Payment-Mobile POS payment system enables customers to purchase products on vending machines (or in retail stores) with mobile phones.

Two popular types of mobile POS systems are:

a) Automated point-of-sale payments, and

b) Attended point-of-sale payments.

The first type is frequently used over ATM machines, retail vending machines, parking meters or toll collectors, and ticket machines to allow mobile users to purchase goods (such as snacks, parking permits, and movie tickets) through mobile devices. The other type of Mobile POS systems is useful for shop counters and taxis. They allow mobile users to make payments using mobile devices with the assistance from a service party, such as a taxi driver, or a counter clerk. A P2P mobile payment system to allow mobile users to use mobile devices as a point-of-sale device to issue and deliver secure mobile payment transactions between them at anywhere and anytime.

(B1) Mobile Wallets

Mobile wallets are the most popular type of mobile payment option for transactions. Like e-wallets, they allow a user to store the billing and shopping information that the user can recall with one-click while shopping using a mobile device. The primary types of mobile wallet schemes in the market are client wallet and hosted wallet. ***Client wallets*** are stored on a user's device in the form of a SIM Application Toolkit card that resides in a mobile phone. Since the wallet is based on hardware, it is difficult to update, and potentially the user's sensitive financial information is compromised if the device is lost or stolen. ***Hosted wallets*** refer to digital wallets hosted on a server. This gives the service provider much greater control over the functionality it delivers and the security of the data and transactions. Hosted wallets can be self-hosted wallets or third party hosted wallets. In addition, server based mobile e-wallets using SET technology are already being used, providing secure transaction capability for merchants and cardholders.

III. BARCODE FRAMEWORK

Here first we capture the image of barcode. Then it will convert to bitmap. Then it will convert to Histogram. Then it will convert to byte array. After that we can decode it by using Zxing Google API. We use packages like utility. Finger, utility.fingercheck. Utility finger is used to scan the fingerprint and utility finger check is used to compare the fingerprint.

***Advantages*:**

- Free Advertisements of products.
- High Level Security is provided for mobile payment system.
- In Mall, Lot of Time is consumed in big queues for payment purpose which will be reduce through this system.

- Biometric Security is included for checking valid user which increases security of overall system.
- The application is platform independent since it is developed in JAVA.
- The behavior of the application is user friendly since the GUI is compatible with all operating environment.

IV. RELATED WORK

Mobile payment system was developed for the user to pay bill for their purchase. The user has to pay online using their debit/credit card or the can use the PayPal account for the payment. In Authentication module, Requesting customer is authenticated by using all his credentials for accessing his account to pay the purchase item through mobile. Transaction will be done through this module with checking all other credentials and transferring amount into merchant account. The algorithm that are going to be used in this module

A .Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization .

B. Elliptic Curve Digital Signature Algorithm

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.

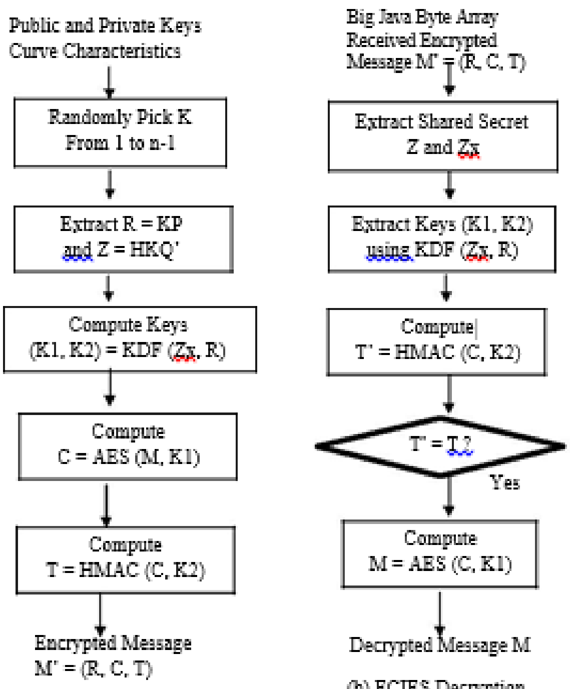
C. Advance Encryption Scheme

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

VI. SYSTEM USED TECHNOLOGY AND APPLICATIONS

Since 2006, a number of master projects are designed to build the proposed payment system in the Computer Engineering Department of San Jose State University. This section reports the mobile enable technologies used for the recent system release.

Mobile Client Technologies: the proposed payment system is developed using a number of mobile enable technologies. **J2ME & Net beans IDE** is used as the mobile development platform due to its research nature of this project. The Java ME File Connection API (JSR 75) is used to store user certificates and related mobile data on the client emulators. Net beans (Version 5.5), as an open source tool, is used as the integrated development environment. Its extension known as Mobility Pack provides an intuitive drag and drop user interface to support building a mobile interface. The mobile client software is implemented based on MIDP 2.1 and CLDC 1.1.


Public and Private Keys
Curve Characteristics
Randomly Pick K From 1 to n-1
Extract R = KP and Z = HKQ'
Compute Keys (K1, K2) = KDF (Zx, R)
Compute C = AES (M, K1)
Compute T = HMAC (C, K2)
Encrypted Message M' = (R, C, T)
Big Java Byte Array Received Encrypted Message M' = (R, C, T)
Extract Shared Secret Z and Zx
Extract Keys (K1, K2) using KDF (Zx, R)
Compute T' = HMAC (C, K2)
T' = T ?
Yes
Compute M = AES (C, K1)
Decrypted Message M

(a) ECIES Encryption

(b) ECIES Decryption

Figure 13 the ECIES Encryption and Decryption Processes

Next, mobile client software also uses **Bouncy Castle Crypto APIs,** which provides a light-weight API in J2ME and a complete open source library for encryption and decryption. In addition, **JSON utility (JavaScript Object Notation)** is used to represent JavaScript objects and format the exchanged mobile data in a structural manner like XML. These data records are exchanged and communicated between mobile client software and the payment server as well as the merchant server.

Middle-Tier Technologies:

To support online user interface, Java Servlet technology and Java server pages are used to work with Apache Tomcat Web Server to support the mobile payment server and merchant server. In addition, Java Database Connectivity (JDBC) is used to provide a seamless integration of middle layer servers with the mobile payment database. Furthermore, **Bouncy Castle Crypto APIs** is used at the server side to support implementation of X.509 V3 certificate authority, generation, and validation as well as Java Cryptography extension.

Application-Tier Technologies:

(A) The 2D barcode library

Figure 14 shows the basic steps in encoding and decoding of a 2D barcode at both client and server sides. As indicated in a 2D barcode are divided into a number of segments (say four smaller barcodes). Each segment is a smaller barcode, which includes a specific type of information, such as product advertisement, merchant information, and security or transaction data. Using 2D barcodes in a payment system not only supports mobile payment transactions, but also enables post-sale activities, product delivery and pick-up. In addition, a cost-efficient barcode technology can enhance mobile security.

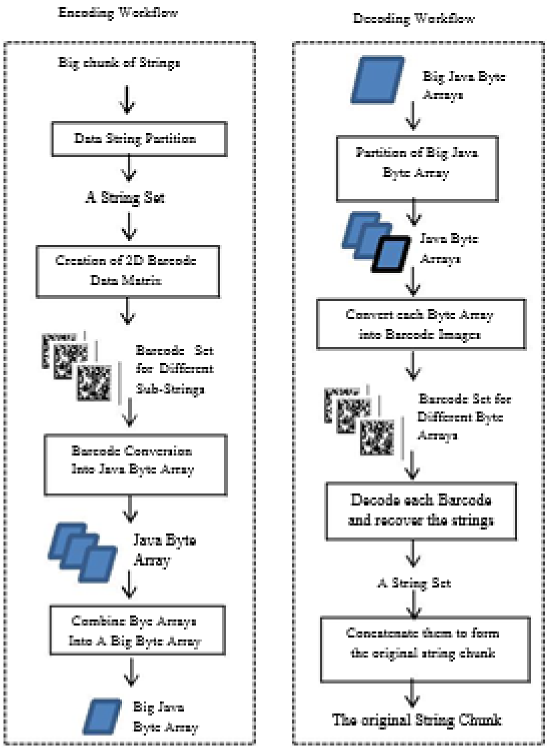

Encoding Workflow
Big chunk of Strings
Data String Partition
A String Set
Creation of 2D Barcode Data Matrix
Barcode Set for Different Sub-Strings
Barcode Conversion Into Java Byte Array
Java Byte Array
Combine Byte Arrays Into A Big Byte Array
Big Java Byte Array
Decoding Workflow
Big Java Byte Arrays
Partition of Big Java Byte Array
Java Byte Arrays
Convert each Byte Array into Barcode Images
Barcode Set for Different Byte Arrays
Decode each Barcode and recover the strings
A String Set
Concatenate them to form the original string chunk
The original String Chunk

Figure 14 Encoding and Decoding for 2D Barcodes

(B) E-Wallet

The system provides a server-based digital purse (wallet) for each user to store his (or her) financial information. The user can enter a fixed amount of money that must be transferred from his/her credit card account or a bank ATM card. Using an e-wallet for a mobile user provides two major benefits. Mobile client software provides a simple interface to support user accesses to e-wallets.

(C) Mobile Payment Server

The payment server supports the following functions:

- Certification generation, management and validation for mobile client and merchant server.
- Mobile user registration for merchant users, end-users.
- Use the barcode-based framework to process and generate 2D barcode-based messages between mobile clients and the payment server.

- Mobile client authentication and e-wallet management.
- Secure session creation, management, and validation

Mobile payment processing based on secured message validation (using the ECC-based key pair) and data integrity checking with digital signatures.

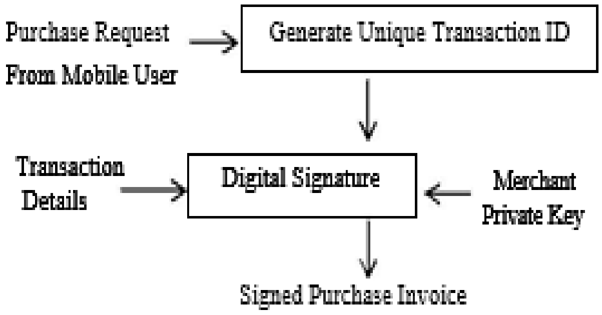
Figure 15(b) shows the basic procedure to generate a signed payment request, and Figure 15(c) displays the basic steps in validating a signed purchase Invoice.

(D) Merchant Server

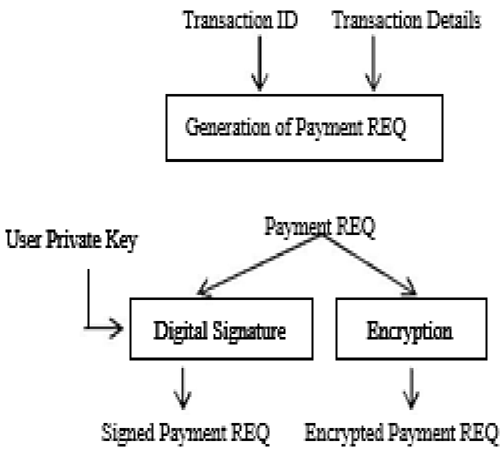
The merchant server supports the following functions:

- Maintains a record of products for sale.
- Supports product purchasing function.
- Use the barcode-based framework to process and generate 2D barcode-based messages between mobile clients and the Merchant server.
- Provide required security functions, such as secured transaction IDs, digital signature generation and validation,

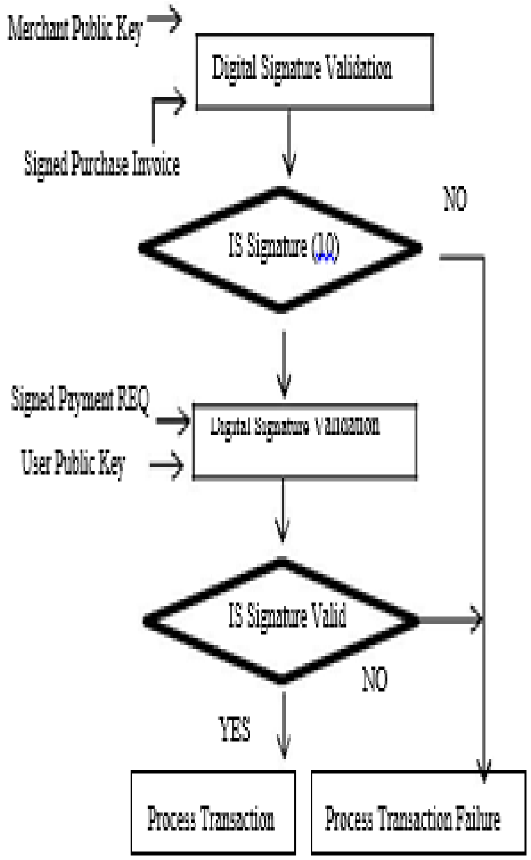
Data integrity checking. Figure 15(a) shows the basic procedure to generate a signed purchase invoice, and Figure15(c) displays the basic steps in validating a signed purchase Request from a mobile client.



a) Generation of Signed Purchase Invoice



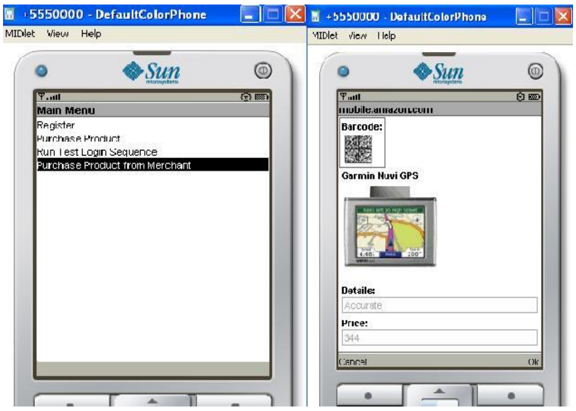
b) Generation of Signed Payment



c) Validation of Signed Purchase REQ and Signed Purchase Invoice

Figure 15 Generating Purchase/Payment Invoice and REQ

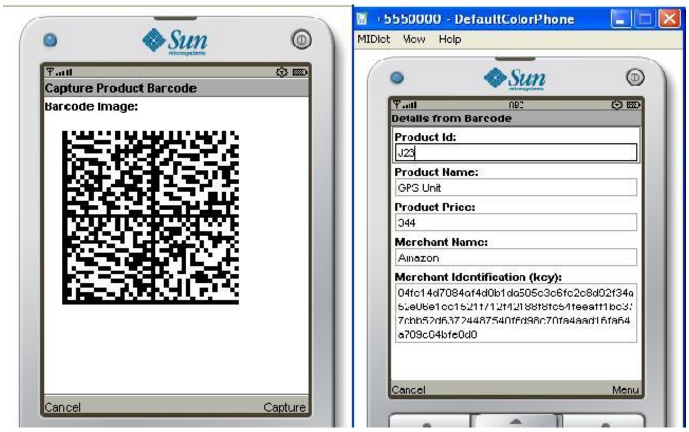
Since April 2008, we have completed the first prototype of a 2D barcode-based mobile payment system to support mobile users to perform electronic payment transactions for products identified with 2D barcodes at anywhere and anytime. We have done some application case study and performance evaluation on a wireless internet using a mobile emulator. Students have recorded the details design Figure 16 shows a simple scenario involving the steps for mobile purchasing and payment operations on the mobile site.



Main Menu
Register
Purchase Product
Run Test Login Sequence
Purchase Product from Merchant

mobile.amazon.com
Barcode:
Garmin Nuvi GPS
Details: Accurate
Price: 344

(a)First Mobile Screen After login (b) A receive AD with a Barcode



Capture Product Barcode

Barcode Image:

Details from Barcode

Product Id: J23

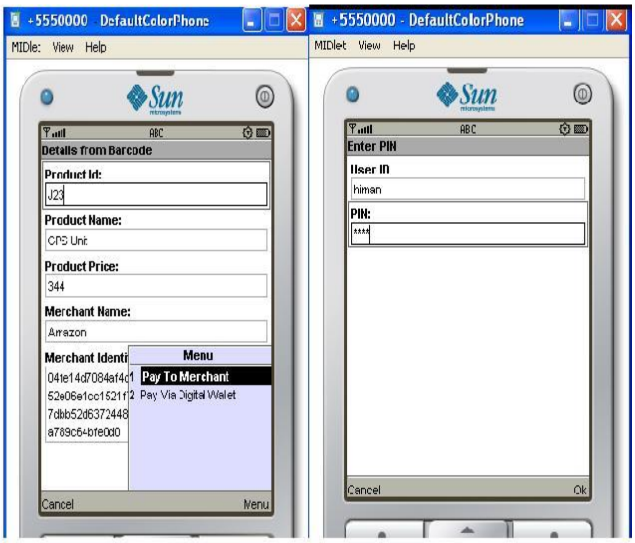
Product Name: GPS Unit

Product Price: 344

Merchant Name: Amazon

Merchant Identification (key): 04fc14d7084af4d0b1da505c3c6fc2c8d02f34a 52e06e1cc1521f712f4218818fc54feeaff1bc37 7cbb52d6372448754f0fd98c70fa4aad16fa64 a709c04bfe0d0

c) Captured 2D Barcode d) Displayed Barcode Information



Details from Barcode

Product Id: J23

Product Name: GPS Unit

Product Price: 344

Merchant Name: Amazon

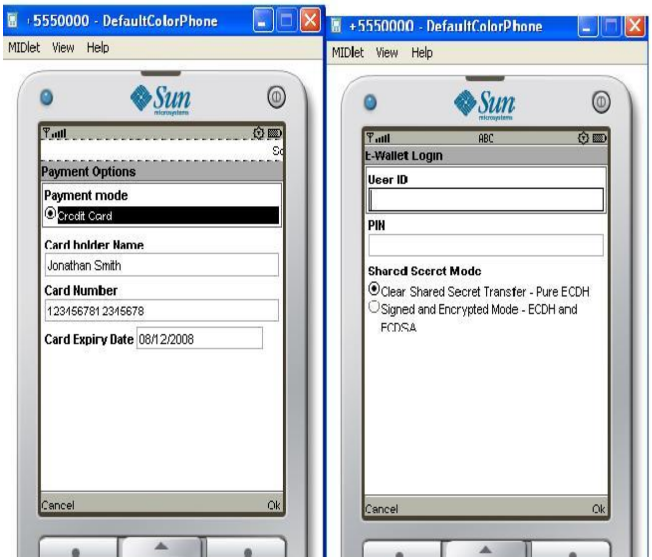
Merchant Identi 041e14d7084af4d 52e06e1cc1521f 7dbb52d6372448 a789c64bfe0d0

Enter PIN

User ID: himan

PIN: ****

e) Initate Mobile Payment to Merchant f) Mobile user enter secret PIN



Payment Options

Payment mode

● Credit Card

Card holder Name: Jonathan Smith

Card Number: 123456781 2345678

Card Expiry Date: 08/12/2008

E-Wallet Login

User ID

PIN

Shared Secret Mode

● Clear Shared Secret Transfer - Pure ECDH

○ Signed and Encrypted Mode - ECDH and ECDSA

g) Select credit card payment) Display Payment Confirmation

VI. SECURITY ISSUES

There are three data channel types between partners in the model. Every channel faces its own security issues. You can see the channels in Figure3. The three channels and their properties are shown in Table2:

Security issue of the SMS channel is clear, commitment is sent through GPRS or by SMS while it is enciphered by the shared key that is shared between customer and the broker in the registration time. Because the channel considered as an unsecure one (SMS channel), both the commitment and the acknowledgment must be enciphered. The acknowledgment is hash of deciphered commitment that enciphered by the shared key. If a customer is not authorized to create a new chain, the broker sends a meaningful enciphered message to inform him/her. Customers can not submit a new hash-chain when there is another active valid chain or when there is not enough money in their accounts.

Channel Type	**Sender**	**Receiver**	**Sent data**	**Transferred data**
SMS	Custom	Broker	Commitme	Acknowledge
2D-	Custom	Mercha	PP	Verification
SSL	Mercha	Broker	PP	Verification

Table2. Data Channels

The 2D-barcode channel is a secure channel because it is proximity communication. Barcode must be placed in the sight of scanner and in very near distance. It is so hard for eavesdropper to listen to this channel because of proximity communication. So, no cryptography or other security technics has been taken into account. 2D-Barcode technology makes this channel secure.

But the SSL channel may have different circumstances with respect to who is the broker and which network and infrastructure is installed for data transformation. It is a range from secure network to unsecure one. For example if the merchant itself is the TTP too, then there is no such a communication because customer gives the barcode directly to the TTP. On the other hand if broker and merchant are separated entities then the network should become a secure one.

A.Attacks

1) Skimming

There are 3 channels as listed in table2. The 2D-barcode channel is assumed to be a secure channel against skimming because it is so hard to conceal in the middle especially in stadiums or metro station where CCTV and officers are present; barcode must be taken in front of the scanner in the near distance maybe under 10cm so this attack is an unexpected one. The SMS and SSL channels are also protected by encryption; hence skimming attack can be ignored unless a shared key is stolen.

2) Double spending

The verification system is online, so double spending is not probable because every payment is checked before completion.

3) Replay Attack

Online checking prevents this attack to effect.

4) Masquerading

Until every user can protect his/her key, Masquerading is out of range. Unless one can access customers' cellphones and use the software on it (in which the key is placed). So, customers must protect their cell phones as the key holder.

5) Merchant Fraud

Merchants can fake PPs instead of customers. Then they can send the faked PPs to broker in order to receive the credit. In order to prevent merchant fraud, we use hash-chain. When customers use inversed hash elements, merchants cannot
Produce the correct elements in order to make valid PPs.

B.Privcy

There are three sides that interact directly or indirectly with the customers. Every side has different access level to the customers' information. Merchant is aware of what every customer has bought and when and where they have been spending their money. Broker also is able to access the information that shows when and where the customers have spent their money. However bank is just aware of when the customers have spent nothing more.

VII. BASIC FLOW OF 2D

This paper proposes a 2D barcode-based payment system using the second approach. Figure 2 displays its underlying payment process, which consists of the following steps:

- **Step #0:** A registered mobile user uses his/her user account and PIN to login the mobile payment system by sending a login request to the mobile payment server. The mobile server processes mobile client authentication and sends a login response with the server certificate ID, and secured session ID,
As well as a public key for the communications.

- **Step #1:** The mobile client authenticates the mobile server with received public and server's certificate.
- **Step #2:** The mobile client captures or receives a 2D barcode for an interested product from its advertisement. There are two scenarios in which a mobile user can get a 2D barcode. In the first case, a mobile user may use a mobile camera on the mobile device to capture the image of a 2D barcode from a posted product. In the second case, a mobile user may receive a mobile ad on a mobile device from a merchant. Meanwhile, the mobile client decodes the received 2D barcode, which includes product and maker's information, marketing data, merchant's mobile URL information.
- **Step #3:** The mobile use clicks the given 2D barcode to switch the target merchant's mobile site using the provided URL in the received 2D barcode.
- **Step #4:** The mobile use prepares and submits a purchasing request with a digital signature as a 2D barcode to the merchant server.
- **Step #5:** The merchant server authenticates the mobile client based on the provided the secured session ID from the mobile client, as well as the public key. Meanwhile, the received signed request is validated by the merchant using the private key.
- **Step #6:** The merchant server generates and sends a signed purchase invoice with a transaction ID to the mobile client.
- **Step #7:** The mobile client prepares and sends a payment request with the same transaction ID and a digital signature to initiate a payment request. The digital signature is made using the client private key. The entire message is encoded as a 2D barcode.
- **Step #8:** A secure session is established between the payment server and the mobile client. In this step, the payment server validates the given security information, including the certificate from mobile client, session ID, public key, and received digital signature. The mobile payment server processes the payment transaction.
- **Step #9:** The payment server prepares and sends a payment confirmation with a 2d barcode receipt to the mobile client. The mobile client displays the received confirmed message to the mobile user.

-**Step #10:** The mobile server also sends a payment transaction completion notice with a 2D barcode to the merchant server. This barcode will be useful for the merchant to carry out the post-sale operations, such as pick-up validation or product delivery.

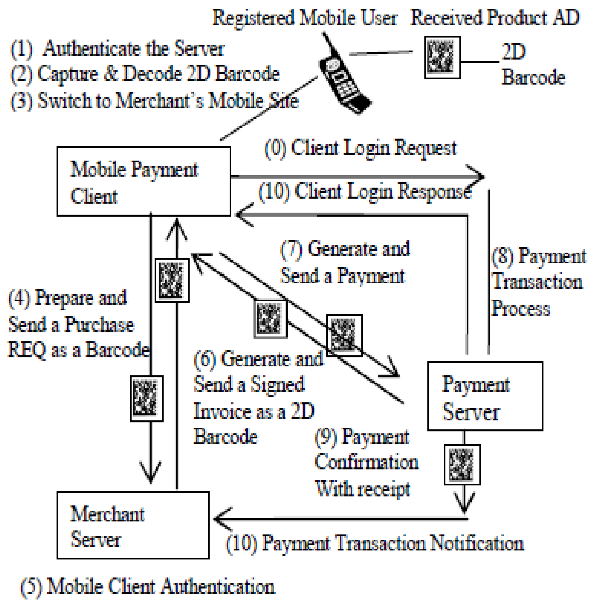

Registered Mobile User
Received Product AD
2D Barcode
(1) Authenticate the Server
(2) Capture & Decode 2D Barcode
(3) Switch to Merchant's Mobile Site
Mobile Payment Client
(0) Client Login Request
(10) Client Login Response
(7) Generate and Send a Payment
(8) Payment Transaction Process
(4) Prepare and Send a Purchase REQ as a Barcode
(6) Generate and Send a Signed Invoice as a 2D Barcode
Payment Server
(9) Payment Confirmation With receipt
Merchant Server
(10) Payment Transaction Notification
(5) Mobile Client Authentication

Figure 2 The 2D Barcode-Based Payment Process

VIII. FUTURE WORK

Here we discuss some extensions can that be adopted in order to add new capabilities to the model

A. Offline solution:

Chains can become vendor specific. In order to satisfy this, the customer specifies the specific vendor (merchant). The broker will pass the customer a commitment to the specified merchant (the commitment is enciphered by the shared key between broker and the merchant). Thus, the merchant itself can verify the elements sent by the customer. It lessens cost by omitting broker verification and also slims the waiting time. Any communication between broker and merchant is secured by using security protocols like SSL connection.

B. Independent merchant:

The broker and a merchant can integrate as a united entity. In this situation, merchant also plays broker's role. It speeds up the model but reduces customer's trust to the model, unless merchant is a trustful one. Indeed it

IX. CONCLUSION

As more and more products and goods are identified using 2D barcodes in commerce, there is a clear need to build new mobile payment systems for mobile users to support mobile transactions based on 2D barcodes. To address this need, this paper introduces an innovate mobile payment system, which supports and delivers secure and easy operating mobile payment transactions based on 2D barcodes. Unlike other mobile payment systems and solutions, the proposed system has several distinct features. □Enable mobile payment transactions for all goods and products identified by 2D barcodes at anywhere and anytime. □Support 2D barcode-based security solutions for mobile payment □Improve mobile user experience by reducing user inputs in mobile payment.

This paper presents the basic business process and workflow, and the proposed system architecture and design, as well as the underlying 2D barcode-based security solution. For future research directions, we are studying and developing more mobile solutions for buying and selling goods and products identified by 2D barcodes. One of them is how to enhance the current payment solution by adding customer and product verification capability using 2D barcodes. The other is how to build 2D barcode enabled mobile solutions for advertising and marketing.

REFERENCES

[1] Jerry Zeyu Gao, Lakshmi Prakash, and Rajini Jagatesan, "Understanding 2D-BarCode Technology and Applications in M-Commerce – Design and Implementation of A 2D Barcode Processing Solution" stated in IEEE conference, 2007.

[2] Hiroko Kato, Keng T. an, "Pervasive 2D Barcodes for Camera Phone Applications" stated in IEEE conference, 2007.

[3] Jerry Gao, Vijay Kulkarni, Himanshu Ranavat, Lee Chang, "2D Barcode- Based Mobile Payment System" stated in IEEE conference, 2009.

[4] Vibha Kaw Raina, U.S Pandey, Munish Makkad," Barcode Payment System in Trusted Mobile Devices" stated in IEEE conference, 2012.

[5] N. Jobanputra, V. Kulkarni, D. Rao, and Jerry Gao, "Emerging Security Technologies for Mobile User Accesses", Accepted by The electronic Journal on E-Commerce Tools and Applications (eJETA), 2008.

[6] Vijayendra Kulkarni, and Himanshu Ranavat, "A 2D Barcode-based Mobile Payment System", the master project, SanJose State University, May, 2008.