A 2D Barcode-Based Mobile Payment System

Jerry Gao, Vijay Kulkarni, Himanshu Ranavat, Lee Chang
San Jose State University, San Jose, USA

Hsing Mei
Fu Jen Catholic University, Taiwan

Abstract

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. This paper presents an 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 (DataMatrix) as an example to demonstrate how to deal with underlying mobile business workflow, mobile transactions and security issues. The paper discusses system architecture, design and implementation of the proposed mobile payment solution, as well as 2D barcode based security solutions. In addition, this paper also presents some application examples of the system.

Keywords: mobile payment, mobile payment system, mobile commerce, electronic commerce, 2D barcodes.

1. Introduction

Mobile payment is one of the important and hot subjects in mobile commerce and wireless application. According to the survey on mobile-commerce [1], it is estimated the global revenue expected from m-commerce and related services is about $88 billion in 2009. According to the Mobile Payments 2002 report, published by Wireless World Forum, the size of the mobile internet based mobile payment market will grow from around 5 bullion Euros in 2002 to nearly 55 billion Euros in 2006 in the key 13 markets. As more businesses and merchants are paying their attention to mobile users for product and service sales, there is a strong demand to for vendors to provide reliable and user-friendly mobile payment services to delivery secured and efficient payment transactions at anytime and anywhere.

In the recent years, there have been a number of published papers [2][3][4][5][6], which address different perspectives of mobile payment, including mobile payment market, business models, schemes and processes, as well as needs and challenges. Meanwhile, there are a number of mobile payment players, which provide mobile users with mobile payment systems, solutions and services. As more and more products are identified using 2D Barcodes, it is reasonable for merchants and business vendors to expect a mobile payment system to support the buy-and-sale products using standard 2D barcodes on mobile devices. Meanwhile, current mobile users have encountered their input limitation by interacting with mobile commerce due to the limited keyboards and display screens of mobile devices. As the fast increase of mobile phones with the touch-screen feature and digital camera function, mobile users are looking for mobile solutions to provide rich mobile experience and simple operations for mobile commerce. Mobile payment systems supporting 2D Barcodes are definitely needed by mobile users and merchants.

This paper proposes an innovative mobile payment system based on 2D barcodes for mobile users to improve mobile experience in conducting mobile payment transactions. Unlike other existing mobile payment systems, the proposed payment solution provides distinct advantages to support buy-and-sale products and services with 2D Barcodes. This system uses one standard 2D Barcode (DataMatrix) as an example to demonstrate how to deal with underlying 2D barcode-based mobile payment workflow, mobile transactions and involved security mechanisms. The paper discusses the architecture, design, and implementation of this mobile payment solution, which ensures the easy delivery of secure mobile transactions at anytime and anywhere. In addition, this paper also presents some application examples of the developed prototype system.

The paper is structured as follows. Section 2 provides the basic background about mobile payment and 2D barcodes, and reviews the related work on mobile payment systems and 2D barcode-based mobile applications. Section 3 presents mobile commerce workflows and mobile payment processes for buying products with 2D barcodes. Section 4 discusses the architecture, functions, and high-level design for the proposed mobile payment system for products with identified 2D barcodes. Section 5 shows some applications of the mobile payment system. Finally, Section 6 discusses the conclusion remarks and future research directions.

2. Background and Related Work

This section provides the basics about mobile payment and 2D barcodes. Meanwhile, it also reviews the existing related work on mobile payment systems and 2D barcode-based mobile applications.

2.1. Basics and Related Work of Mobile Payment and Systems

What is ***wireless payment***? According to [2], it refers to mobile-commerce payment (or m-payment) which supports "any transaction with a monetary value that is conducted via a mobile telecommunications network". A wireless payment system (also known as a mobile payment system) refers to an electronic payment system that provides wireless-based electronic payment solutions to support point-of-sale and/or point-of-service payment transactions over wireless and/or wireless internet through diverse mobile user devices, such as cellular telephones, smart phones or PDAs, and mobile terminals. The detailed requirements, business processes, and major players have been discussed in [2][3][4]. As discussed in [2], wireless-based (or mobile) payment systems could be classified into the following types.

(A) 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 three 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. Y. Lin et al. [8] discuss the basics and Zheng Huang and Kefei Chen in [10] presents an example of phone-based payment systems.
- ***Smart Card Payment Systems*** [2][3]– 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. Some detailed discussion and examples can be found in [13]. Ashutosh Saxena et al. [12] report a sample system.
- ***Credit-Card Mobile Payment System***s [2][3][13] – 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 [15]. 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 [17]. An example system is presented in [9].
- **Mobile POS (Point-Of-Sale) [2][3]** - 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. Gao et al. [11] presents 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.

(B) Mobile Wallets *[2][3]*

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. The authors in [14] present an approach to building e-wallets. G. Me and Strangio, M.A.[16] discuss a sample system using e-wallet for mobile payment.

2.2. Related Work of 2D Barcode-Based Mobile Applications

This section reviews the basics of 2D barcodes and related mobile applications.

(A) Basics of 2D Barcodes

According to [19], 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.

QR Code PDF417
Data Matrix

Figure 1 2D Barcode Samples

Since the earlier forms of linear barcodes were not capable of encoding letters, 2-D barcodes were invented to meet the needs of encoding alphanumeric data, including letters, numbers, and punctuation marks. At the end of 1980s, two-dimensional (2D) barcodes appeared. With a much larger data capacity, 2D barcodes become popularly used in different areas. There are two types of 2D barcodes: a) stacked 2D barcodes, such as PDF417, and b) Matrix 2D barcodes, such as Data Matrix and QR Code. Some common 2D barcode standards are listed below.

Table 1 Capacity, Features, and Standards for Major 2D Barcodes

	QR Code	PDF417	DataMatrix	Maxi Code
Developer (country)	DENSO (Japan)	Symbol Technologies (USA)	RVSI Acuity CiMatrix (USA)	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 size High speed scan	Large capacity	Small printout size	High speed scan
Standards	AIM International JIS ISO	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 2, 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 [18]. 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.

(B) Related 2D Barcode Mobile Applications

In M-Commerce systems, 2D barcodes can be used to support pre-sale, buy-and-sell, post-sale operations in mobile commerce transactions [22]. For example, 2D barcodes can be used to present advertisements, coupons, and receipts, which can be captured and decoded by mobile client software on mobile devices. Moreover, 2D barcodes enable mobile devices to become a point-of-sale device that reads the barcode and facilitates payment transactions. After a payment transaction, 2D barcodes can be used to present a purchase receipt to gain access to the information about the purchased goods and services. Until recently, people are gradually realized the importance of 2D barcodes and its great application value in M-Commerce because of the followings [22]:

• 2D barcode-based input and interaction provides a new effective approach for mobile customers when their mobile devices with inbuilt digital cameras.

• 2D barcode-based presentation is becoming a popular approach to present semantic mobile data with standard formats.

• 2D barcodes support a new interactive and efficient approach between mobile customers and wireless application systems.

As the fast advance of 2D barcode enabling technology, people have found its great value and diverse applications in M-commerce.

- *Wireless trading (pre-sale/sale-and-buy/ post-sale)* – Using 2D Barcodes on products and goods, merchants and manufactures allow mobile customers to find more detailed product information. For example, NTT DoCoMo, in Japan, is developing a system using 2D barcodes for food consumers. Using mobile camera phones, consumers can easily input a 2D barcode of a product by scanning product barcodes in the store, and found more detailed information about each product, including producers, harvest date, shipping date, and agricultural chemicals. In addition, 2D barcodes are also very useful in post-sale, including product tracking, shipping, and delivery.
- *Product information tracking and checking* for mobile users - For example, K. Seino at al. [25] describes an application used to track the fishery products using QR codes. Another example is CyberCodes, developed by Sony Computer Science Lab. [20].
- *Mobile security* – One good example is the system, known as Seeing-Is-Believing, developed by Carnegie Mellon University [23]. The system utilizes 2D barcodes and camera-phones to implement a visual channel for authentication and demonstrative identification of devices. The paper uses 2D barcodes as a visual channel to deal with several problems in computer security. These include: a) authenticated key exchanges between devices that share no prior context, b) the establishment of a trusted path for configurations of a TCG-compliant computing platform, and c) secure device configuration in the context of a smart home.
- *Mobile customer and product verification* - Using 2D barcodes merchants (or a delivery man) can easily perform the verification with a mobile scanner device (or mobile device) to check 2D barcodes on a product, such as an e-ticket, a digital coupon, and an invoice [18][21][24].

3. 2D Barcode-Based Business Scenarios in Mobile Payment

There are two ways to build 2D barcodes in mobile payment systems. The ***first*** approach is to build 2D barcode-based Position-Of-Sale (POS) systems to support mobile payment transactions between mobile users and mobile terminals at anytime and anywhere. This type of POS-based payment systems can be used in Parking lots, TAXI, airport and railroad stations. 2D barcodes are useful to support product information retrievals, secured payment transactions, customer and product verification, and mobile security checking.

The ***other*** approach is to build 2D barcode-based systems to allow mobile users to issue mobile payment transactions using their digital wallets based on mobile payment accounts in a mobile payment server. Comparing with the existing account-based mobile payment systems, this approach has *five distinct advantages:*

- It provides the buy-and-sale payment services for goods identified using 2D barcodes.
- Mobile users can easily retrieve all related product information from 2D barcodes.
- It easily supports product and customer verification for post-sale services, such as delivery and pick-up.
- It increases the mobile security for payment transactions.
- It improves mobile user experience by reducing user inputs. A typical example is given in [22]. When a mobile customer wants to access a wireless internet site (http://yahoo.com) using a mobile phone, he must enter the address through 33 clicks using the device keyboards. However, using a 2D barcode to present a URL for a mobile site, a customer only needs to 2 clicks to enter the URL (http://yahoo.com).

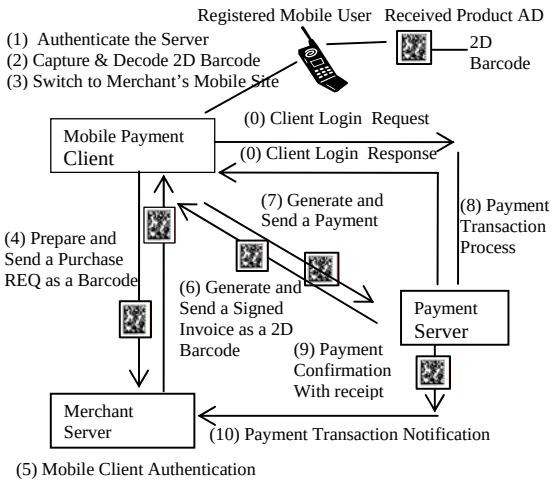


Figure 2 The 2D Barcode-Based Payment Process

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.

4. A 2D Barcode Mobile Payment System

Since January, 2007, we have started the research project to create an innovative 2D barcode-based payment system for mobile users using the second approach. It supports mobile users to buy-and-sale as well as pick-up goods identified with 2D barcodes at anytime and anywhere. This section provides an overview of system functions, architectures, and security solution.

4.1. System Infrastructure and Framework Architectures

Figure 3 shows the system infrastructure, which consists of four layers:

- *Client Layer* – This layer includes mobile user interface and online client interface. The online client interface is designed support end customers and merchants to perform user account and membership management. The mobile payment client software supports mobile user interactions for mobile payment. As shown in Figure 4(a), the mobile payment client is supported by J2ME (with Netbeans IDE, CLDC 1.1. MIDP 2.1), Bouncy Castle Light Weight Crypto APIs, JSON utility, and the 2D barcode framework [22].
- *Middle Layer* – Figure 4(b) shows the components in the middle layer. They include 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.
- *Application Layer* – This is the mobile payment server, which supports the 2D barcode-based mobile payment process and related transactions (see Figure 5).
- *Data Store Layer* – This includes a database server, which stores, maintains, and processes the customer account and membership data, transaction data, and user digital wallet as well as necessary security data, such as PIN and session records.

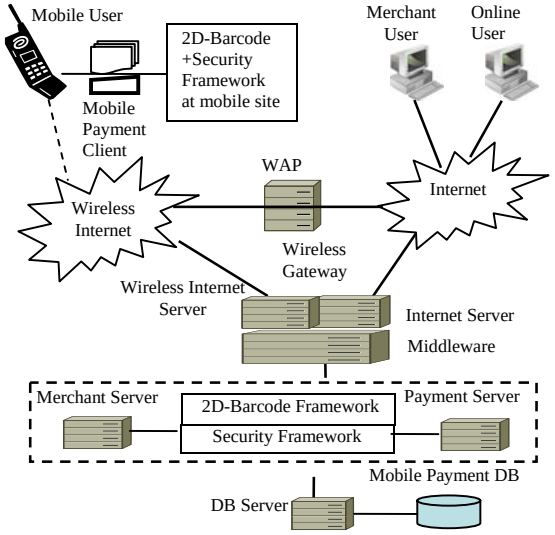
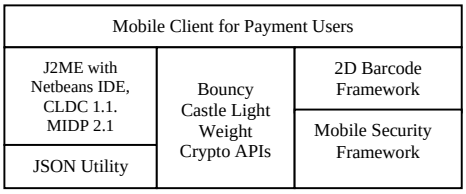
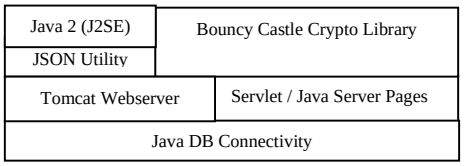


Figure 3 The 2D Barcode-Based Payment System Infrastructure



(a) Mobile Client Layer for Mobile Payment Users



(b) Middle Layer for Components

Figure 4 Mobile Client Structures for Different System Users

As shown in Figure 5, the ***mobile payment server*** includes a number of function components, which are operated based on two supporting frameworks. These functional components can be classified into three groups. The ***first*** group is related to service management, including user service management, membership management, and user payment account management. The ***second*** group includes the following two components:

a) The transaction management component - it creates stores, tracks, merges dynamic mobile payment transactions.
b) The digital wallet management component – it creates, updates, maintains, and deletes server-based digital wallets for mobile users. These digital wallets can be accessed through mobile payment clients.

c) The interface agent provides a simulation interface for the mobile payment server to interact with a financial bank system.

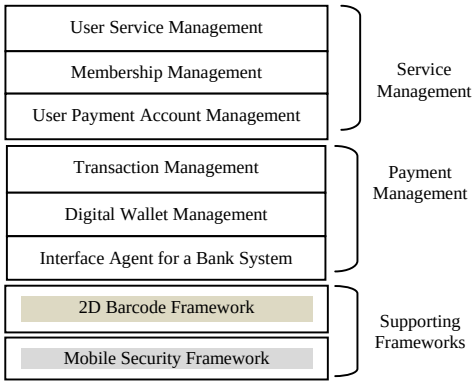


Figure 5 Functional Components in the Payment Server

The ***last*** group contains a) a 2D barcode framework, which supports decoding and encoding 2D barcodes based on the DataMatrix standard. The detailed discussions about this framework has been discussed in [22], and b) a mobile security framework.

4.2. Mobile Enabled Security and 2D Barcode Frameworks

In a mobile payment system, a reliable mobile enabled security solution is critical in mobile payment systems. To achieve the essential security requirements for mobile payment, we must address different security issues in authentication, certification, payment session, data integrity, and end-to-end communications.

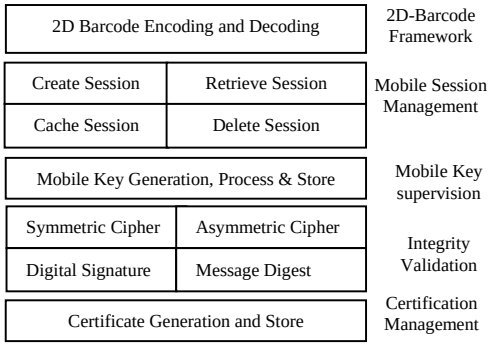


Figure 6 2D Barcode and Security Frameworks

To address these security issues, we build a mobile enabled security framework in the 2D barcode payment system. As shown in Figure 6, this security framework includes the following components.

- *Authentication management* – This component is built to support the required authentication functions for each party, including mobile client, merchant, and the payment server. In this system each party must be authenticated before any payment transaction.
- *Mobile session management* - This function component is designed to assure the security of a payment session between involved parties.
- *Certification management* - This component is designed here to support the payment-oriented certification generation, validation, and management.
- *Mobile key management* – This component is built to generate, distribute, check public and private key based on the Elliptic Curve Cryptography (ECC) technique [26-29].
- *Message and data integrity validation* – This component is useful to check the message and data integrity for the communications between mobile client and the payment server using encryption and decryption methods.

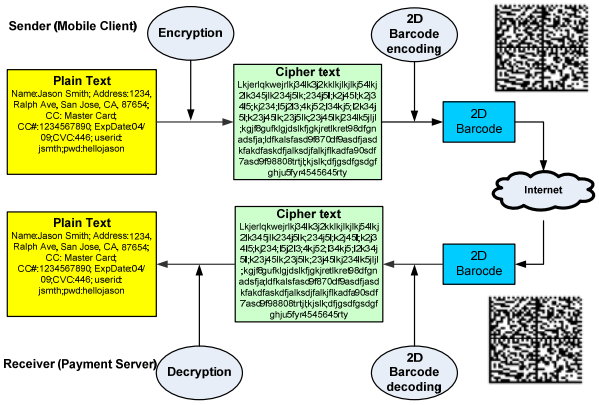


Figure 7 2D Barcode-Based Security Workflow

In addition, a 2D barcode framework is used to support 2D DataMatrix barcode generation, encoding, and decoding at both client and server sides. The detailed discussion about the framework design and implementation can be found in [22]. The detailed DataMatrix barcode algorithms and standards can be found in [22]. Figure 7 shows the basic security workflow for 2d barcodes in the payment system.

In the proposed payment system, 2D barcodes are used for the following purposes:

- In a product ad, a barcode is used to hold product related information. Typical examples are product tracking data, maker, marketing, merchant information. In addition, some security information is also embedded, including a certificate ID for the merchant and public key.
- In a payment invoice, a barcode is used to carry mobile user's selected purchasing information as well as security data, including secured session ID, client ID, PIN and private key, mobile client for authentication by the merchant.
- In a payment transaction, a barcode is used to contain the detailed payment information for a mobile user, including the credit card, PIN, private key, and secured session ID for mobile client.
- In a payment confirmation, a barcode is used to hold the secured transaction ID and conformation code as well as validation ID.

4.3. Mobile Enabled Security Solution in Mobile Payment

The mobile enabled security solution consists of three parts, which supports the security functions and needs in mobile client software, the mobile payment server, and the merchant server. Unlike other existing electronic payment systems, the major security solutions in the proposed payment system used the Elliptic Curve Cryptography technique to deal with different security issues due its advantages in processing time, key lengths and key generation, and energy consumption in mobile computing over other cryptography techniques [30].

User Registration:

All users of mobile payment system must registered first before they access the payment services. Since the system provides online website to support all of its user membership and accounts management, so its users (both customers and merchants) can access the provided mobile user interface (or online interface) to

register, access, and update their profiles and account information. During user registration, each user will be assigned to a unique user ID. In addition, a pair of public and private keys will be generated for the user based on the user's unique International mobile Equipment ID (IMEI) or the Element Serial Number (ESN) and current timestamp. At the end of user registration, a user certificate is issued to the mobile client.

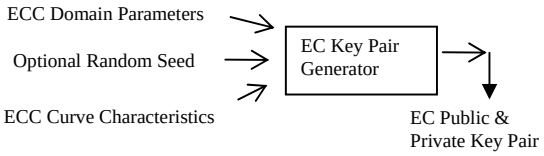


Figure 8 ECC Key Pair Generation

Public and Private Key Generation:
As shown in Figure 8, each mobile user with a unique user ID will be assigned a generated public and private key pair based on the *Elliptic Curve Cryptography* (ECC) technique, which provides the public key infrastructure using 256 bit keys to provide confidentiality, integrity, and authenticity. The optional random seed is used to ensure that the public key generated for the user will be unique in the system. It must be derived from some unique characteristics of the handset such as network host name of the mobile device, the IMEI number or the ESN number. This key pair is used in generating secret session keys and digital signatures to achieve secured sessions and data integrity checking.

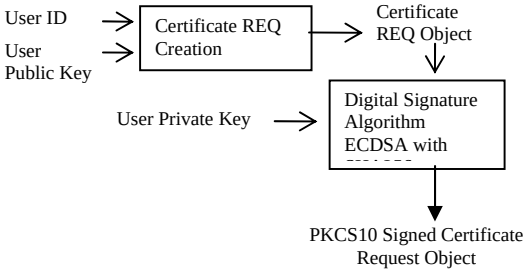


Figure 9 Certificate Request Creation

User and Merchant Certification:
A certificate request is generated for each user (including merchant user and customer user) during user registration based on a generated key pair. As shown in Figure 9, a certificate request for a user is implemented using the *Elliptic Curve Digital Signature Algorithm* (ECDSA) with the *Secure Hash Algorithm* (SHA256). Figure 11 shows the process to generate a user certificate, which is a signed X.509 V3 certificate. All user certificates are stored in the data store in the Base 64 DER encoded format and indexed against the user's ID. During the payment communications between parties, the public key is derived from the certificate. In the first release of this payment system implementation, the payment server is used as a certificate authority, the most trusted and central entity in the system. For the real practice, we can use a third party certification server to work as the certification authority agency.

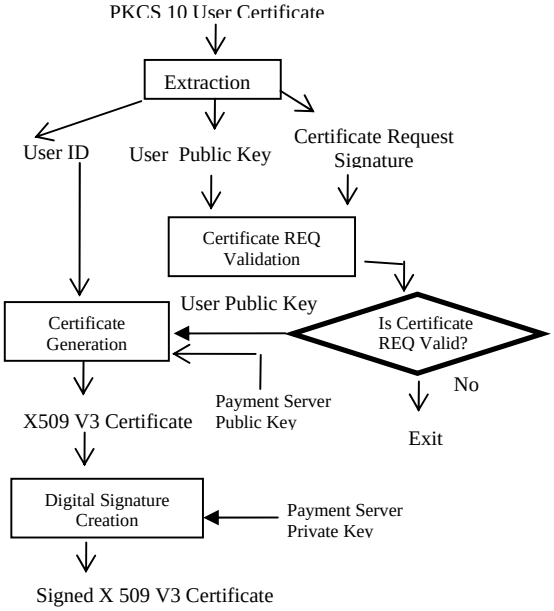


Figure 10 Certificate Generation

Private Key and Certificate Key Management:
Since each user's private key and certificate key is stored on mobile devices, it is important to protect their security. To achieve this goal, mobile client software encrypts a user's PIN and certificate key (or private key) are based on the *Advanced Encryption Scheme* (AES) and hashed using HMAC before they are stored as a file on a mobile device by the mobile client software. The basic procedure is displayed in Figure 11(a). Later, they are retrieved following a decryption procedure in Figure 11(b).

Message and Data Integrity Checking:
To ensure the data integrity of mobile payment processing, the *Elliptic Curve Digital Signature Algorithm* (ECDSA) is used for two purposes:

- To ensure the data integrity of generated certificates in the communications.
- To ensure the data integrity of signed transaction messages from mobile users and merchants to maintain non-repudiation.

Secured Session:

To assure a secured session whenever a user starts a session with the payment system, a session key agreement protocol is used in two modes:
a) Pure Elliptic Curve Diffie-Hellman (ECDH), in which shared secrets are exchanged over the wireless internet in an uncompressed manner. The technique is less time consuming and less processor intensive. This mode is useful to exchange less sensitive information.
b) Signed and Encrypted Mode using ECDH-ECDSA, in which the shared secrets are encrypted using the user PIN. In addition, the shard secrets are also digitally signed to ensure protection against tampering and providing data origin authentication.

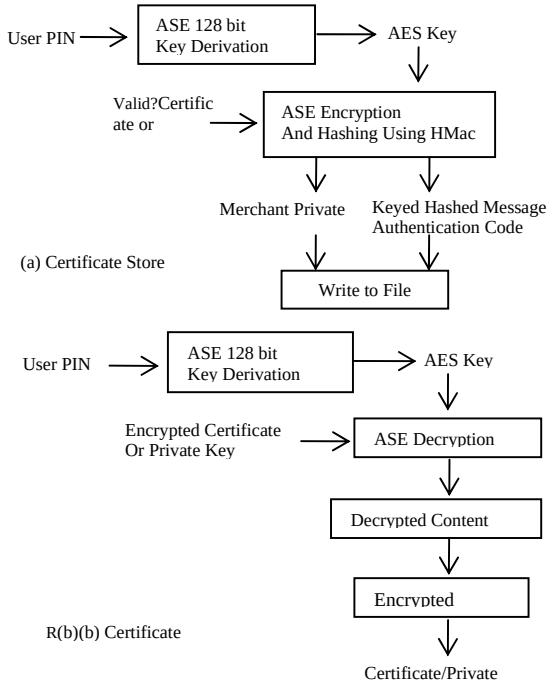


Figure 11 User Certificate Key and Private Key Management

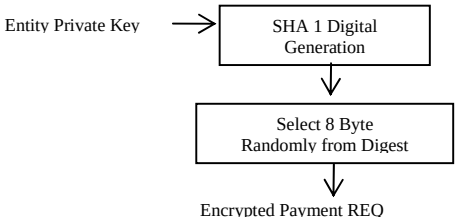


Figure 12 Generation of Pre-Master Shared Secret

This secure session solution supports the following functions:

- Generate a secret for each involved party so that they can be used as the initial vectors to generate the pre-master shared secret and secret MAC key (see Figure 12).
- Exchange of the share secret during a session.
- Support symmetric key encryption and generation, where Advanced Encryption Scheme (AES) is used to generate 128 bit symmetric encryption and decryption for all exchanged messages between two parties (a mobile user and the payment server). Figure 13 shows the encryption and decryption of the symmetric keys.

5. 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. The detailed system design and implementation can be found in [31].

Mobile Client Technologies:

Besides the use of the 2D barcode library reported in [22], the proposed payment system is developed using a number of mobile enable technologies. **J2ME & Netbeans IDE** is used as the mobile development platform due to its research nature of this project. The Java ME FileConnection API (JSR 75) is used to store user certificates and related mobile data on the client emulators. Netbeans (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.

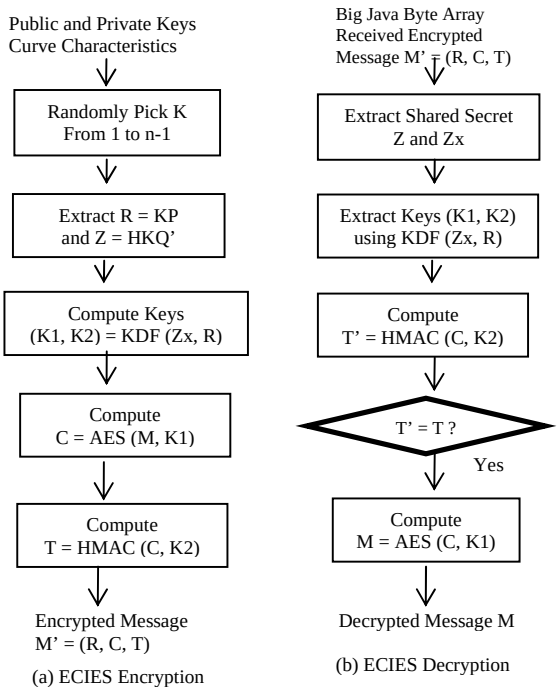


Figure 13 The ECIES Encryption and Decryption Processes

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, JavaServlet 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[22]

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.

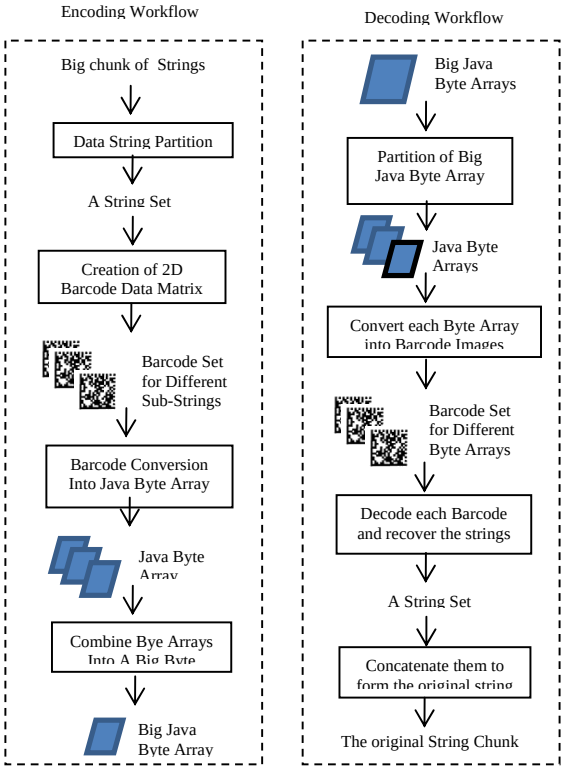


Figure 14 Encoding and Decoding for 2D Barcodes

(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

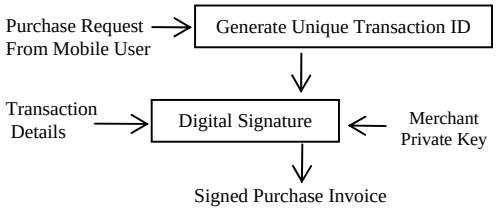
The payment server supports the following functions:

- 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.

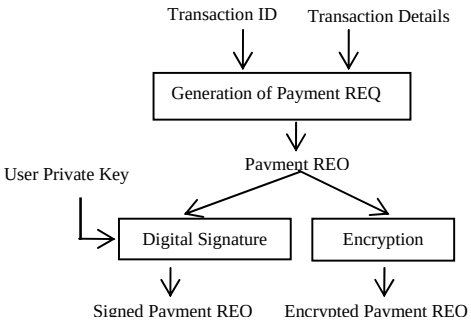
(D) Merchant Server

The merchant server supports the following functions:

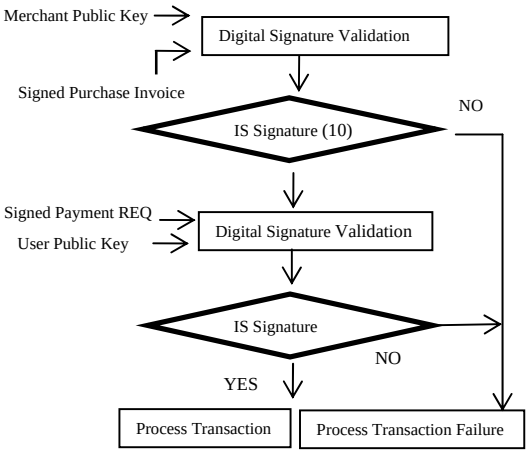
- Maintains a record of products for sale.
- Supports product purchasing function.
- Use the barcode-based framework to process and generate 2D barcode-based messages between mobile clients and the merchant server.
- Provide required security functions, such as secured transaction IDs, digital signature generation and validation, data integrity checking. Figure 15(a) shows the basic procedure to generate a signed purchase invoice, and Figure 15(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. In the master project report [31], students have recorded the details design and performance and evaluation results. Due to the limited space, we can't present the

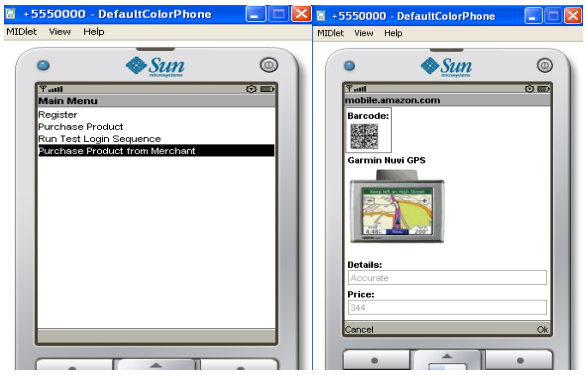
detailed evaluation results. Figure 16 shows a simple scenario involving the steps for mobile purchasing and payment operations on the mobile site.

6. Conclusion and Future Work

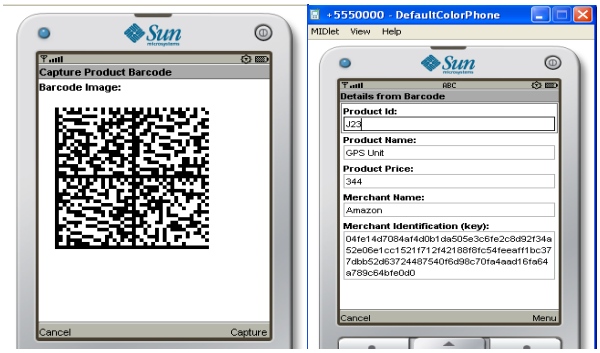
As more and more products and goods are identified using 2D barcodes in commerce, there is a clear need to build new mobile payment systems for mobile users to support mobile transactions based on 2D barcodes. To address this need, this paper introduces an innovate mobile payment system, which supports 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.

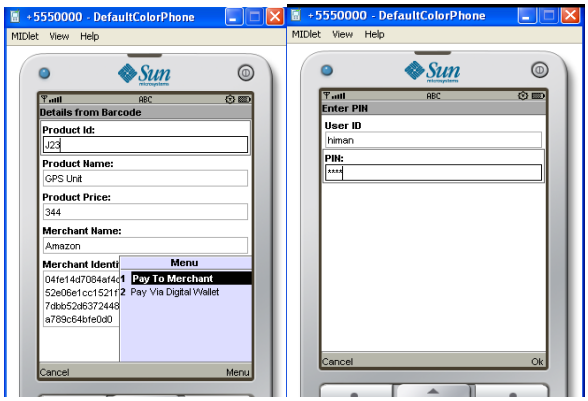
This paper presents the basic business process and workflow, and the proposed system architecture and design, as well as the underlying 2D barcode-based security solution. For future research directions, we are studying and developing more mobile solutions for buying and selling goods and products identified 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.



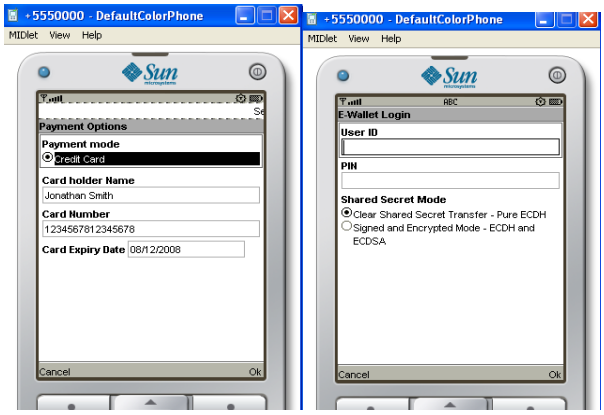
(a) First Mobile Screen After login (b) A receive AD with a Barcode



c) Captured 2D Barcode d) Displayed Barcode Information



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



g) Select credit card payment i) Display Payment Confirmation

Figure 16 A Scenario for Mobile Purchasing and Payment

7. References

[1] Trintech Group, "Statistics for Mobile Commerce", 2005, Retrieved December 4, 2007 from http://www.epaynews.

[2] Jerry Zeyu Gao., Jacky Cai, Min Li, and Sunitha Magadi Venkateshi, "Wireless Payment – Opportunities, Challenges, and Solutions", Published by High Technology Letters, Vol. 12, ISSN 1006-6748, 2006.

[3] Jerry Z. Gao, Simon Shim, Hsing Mei, and Xiao Su, Engineering Wireless-Based Software Systems, Artech House Publisher, August 2006.

[4] L. Antovski, and M. Gusev, "M-Payments", Proceedings of the 25th International Conference Information Technology Interfaces, 2003 (ITI'03).

[5] K. Pousttchi, and M. Zhenker, "Current Mobile Payment Procedures on the German Market from the View of Customer Requirements", Proceedings of the 14th International Workshop on Database and Expert Systems Application, 2003 (DEXA'03).

[6] X. Zheng, and D. Chen, "Study of Mobile Payments System", Proceedings of the IEEE International Conference on E-Commerce, 2003 (CEC'03).

[7] S. Kungpisdan, B. Srivnivasan, and P.D. Le, "A Secure Account-Based Mobile Payment Protocol", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004 (ITCC'04).

[8] Y. Lin, M. Chang, and H. Rao, "Mobile prepaid phone services", IEEE Personal Communications, 7(3): 6-14, June 2000.

[9] A. Fourati, H.K.B. Ayed, F. Kamoun, and A. Benzekri, "A SET Based Approach to Secure the Payment in Mobile Commerce", In Proceedings of 27th Annual IEEE Conference on

Local Computer Networks (LCN'02) November 06 - 08, 2002, Tampa, Florida.
[10] Z. Huang, and K. Chen, “Electronic Payment in Mobile Environment”, In Proceedings of 13th International Workshop on Database and Expert Systems Applications (DEXA'02) September 02 - 06, 2002. Aix-en-Provence, France.
[11] Jerry Gao, Jacky Cai, Kiran Patel, and Simon Shim, “A Wireless Payment System”, Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05).
[12] A. Saxena, M. L. Das, and A.Gupta, “MMPS: A Versatile Mobile-to-Mobile Payment System,” in Proceedings of the International Conference on Mobile Business, 2005, pp: 400-405, DOI: 10.1109/ICMB.2005.61.
[13] Q. Zhang, J. N. B. Moita, K. Mayes and K. Markantonakis, "The Secure and Multiple Payment System Based on the Mobile Phone Platform," Smart Card Centre, Information Security Group, Royal Holloway, University of London.
[14] Denis Hennessy (a white paper from Valista™), “The value of the mobile wallet”, Retrieved on February 10, 2004.
[15] G. Ramakrishnan, "Secure Electronic Transaction (SET) Protocol Information Systems Control Journal, vol. 6, 2000.
[16] G. Me, Strangio, M.A., " EC-PAY: an efficient and secure ECC-based wireless local payment scheme," in Information Technology and Applications Third International Conference, 2005. ICITA 2005 - Vol.2, pp: 442 – 447.
[17] Atlantic Payment, (March 2002). “Payment based on 3D SET”, Retrieved on February 10, 2004 from http://www.atlanticpayment.com/3DSET.htm.
[18] E. Ohbuchi,, H. Hanaizumi, and L. A. Hock, “Barcode Readers using the Camera Device in Mobile Phones”, Proceedings of the 2004 International Conference on Cyberworlds, pp. 260-265, November 2004.
[19] R. C. Palmer, The Bar Code book: Reading, Printing, and Specification of Bar Code Symbols (3rd ed.), Helmers Publishing, 1995.
[20] Jun Rekimoto, and Yuji Ayatsuka, “CyberCode: Designing augmented reality environments with visual tags”, Proceedings of DARE 2000 on Designing augmented reality environments, pp. 1 - 10, 2000.
[21] Adickes et al., “Test Protocol for Comparing Two-Dimensional Bar Code Hand-Held Reader Technologies”, Journal of manufacturing Systems, Volume: 17, 1998.
[22] J. Gao, P. Lekshmi, R. Jagatesan, “Understanding 2D-BarCode Technology and Applications in M-Commerce - Design and Implementation of A 2D Barcode Processing Solution,” in Computer Software and Applications Conference, 2007. COMPSAC 2007 - Vol. 2. 31st Annual International, 2007, pp: 49 – 56.
[23] Jonathan M. McCune, et al, “Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication”, Proceedings of the 2005 IEEE Symposium on Security and Privacy, pp. 110- 124, May 2005.
[24] D. Borkowski, P. Das, and F. Tao, “Selection of a processor for a Portable MaxiCode Reader”, IEEE Computer, pp. 7-10, June 1994.
[25] K. Seino, et al, ”Development of the Traceability System which Secures the Safety of Fishery Products using the QR Code and a Digital Signature”, IEEE Computer, pp. 476-481, Volume: 1, August 2004.
[26] J. Krasner, Embedded Market Forecasters and American Technology International Inc, "Using Elliptic Curve Cryptography (ECC) for Enhanced Embedded Security Financial Advantages of ECC over RSA or Diffie-Hellman (DH)," White Paper Series, 2004.
[27] Certicom Research, "Standards for Efficient Cryptography - SEC 1: Elliptic Curve Cryptography", September 20, 2000.
[28] J. McCaffrey, "Encrypt It Keep Your Data Secure with the New Advanced Encryption Standard," Microsoft MSDN Magazine, November 2003.
[29] D. Hankerson, A. Menezes, and S. Vanstone, "Guide to Elliptic Curve Cryptography", New York: Springer, 2004, pp. 184 - 190.
[30] N. Jobanputra, V. Kullkarmi, 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.
[31] Vijayendra Kulkarni, and Himanshu Ranavat, “A 2D Barcode-based Mobile Payment System”, the master project, San Jose State University, May, 2008.