# Major Milestones of Modern Payment Systems

B. Tirimula Rao, Member IEEE, *M. Dileep, Student Member IEEE, **E. Vedavalli, ***K. Aditya, ****D.R.S. Bindu

Senior Assistant Professor
*4th year CSE,
**4th year CSE, vedavalli.
***3rd year CSE,
****3rd year CSE,
ANITS College of Engineering, Visakhapatnam

**SUMMARY**
A payment system is a system (including physical or electronic infrastructure and associated procedures and protocols) used to settle financial transactions in bond markets, and futures, derivatives or options markets, or to transfer funds between financial institutions. Electronic Payment is a subset of an e-commerce transaction to include electronic payment for buying and selling goods or services offered through the Internet. An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. Even though there are many electronic payment systems, a user uses the system only if he has trust in it. A system will be accepted if it supports several properties such as Atomicity, Consistency, Isolation, Durability and various security issues. In this paper we enumerate security issues of several payment systems in the form of a comparison table. Objective of this paper is to suggest the reader best electronic payment system among the existing ones.

***Keywords:***
*Payment system, Financial Institutions, E-commerce, Electronic Payment*

## 1. Introduction

Payment system consists of a paper based mechanism for handling checks and drafts and a paperless mechanism for handling electronic commerce transactions. The E-commerce represents the process of selling, buying or changing products services and information by means of computer networks. It doesn't require the simultaneous presence of the contracting parties. As the trade became more complicated new abstract representations of value are invented. The representation progressed from barter through bank notes, payment orders, checks, credit cards, and now the electric payments system. Worldwide proliferation of the internet led to the birth of the electronic commerce, a business environment allows the transfer of electronic payments as well as transactional information of the internet. The technologies discussed are Digital Payment system using Blind signatures, Multimodal biometrics using a combination of biometric techniques for authentication, RFID system used for payment through mobile; Smart cards provide secure transactions ,Biometric Finger prints payment, Comdata a card based solution where card holder need not have a bank account. Sound based e-commerce a technology where the details of the customer are transferred in the form of sound through mobile phone. iKP are the protocols used for the secured payments. These protocols are compatible with current card system.

The organization of rest of the paper is as follows: In the next sections various payment systems are discussed. Next we compare several security issues of payment systems discussed in the form of a comparison table. Section 10 concludes the paper.

## 2. Digial Payment System using ID-Based Blind Signatures

Anonymity of the participants is a major requirement in the payment systems. But in some cases this anonymity may lead to blackmailing. So a digital payment system is designed with Id based blind signatures with a trustee capable to revoke the anonymity of the users in a suspicious transaction [2] According to Chaum Blind Signature is a protocol of obtaining a valid signature for a digital coin such that signer's view of the protocol cannot be linked to the instance of signing protocol [3]. The Identity based crypto systems were introduced by Shamir in 1984. Here the user's public key is a binary sequence of the identity of the user. Trusted authorities called private key generators generate the keys from the user information [4]. Several Identity based crypto systems have been developed on the basis of bilinear parings [5].

### 2.1 Blind Signature Schemes

There are several blind signature schemes such as Blind Signature Based on Factoring and Discrete Logarithms, blind signatures based on bilinear pairings and Hess's Identity based blind signature. A Blind signature [5]

Manuscript received September 5, 2009
Manuscript revised September 20, 2009

consists of two parties (recipient and signer) and four algorithms. They are setup, Key extraction, Blind signature generation and verify. Moreover the blind signature should be correct and unforgeable.

### 2.2 Payment System

Now let us see the steps during the payment [6].

1. The customer generates digital currency containing a string of bits.
2. He takes the currency to bank and engages a blind signature protocol with the bank.
3. Bank deducts the amount in the customer's account.
4. Customer then takes this currency to shop and gives it to seller to buy some merchandise.
5. Seller verifies the signature using bank's public key. If invalid he stops the transaction.
6. Shop owner returns the currency to the Bank.
7. Bank verifies currency. If valid Bank credits the amount into seller's account.
8. Seller sends the merchandise to the customer.

### 2.3 Role of the Trustee

The trustee will be able to revoke the anonymity at any instance but should not be involved in operating accounts or producing the coins. A trustee may be involved during every with drawl phase or during opening of the accounts. A trustee may not be involved in any part of the transaction but the messages are encrypted under trustee's public key so that he can revoke whenever necessary. Table 1 shows the information available to various parties in the transactions of this payment system.

## 3. Multi Modal Biometric Payment System

Biometric identification means identifying an individual based on his distinguishing physiological or biological characteristics. But biometrics is not free from errors during extraction. Therefore to increase the reliability a combination of biometric authentication methods are used known as multi-biometrics. Multi biometrics increases the performance of biometric systems [7]. Multi-biometrics is combination of biometric algorithms either by logical or statistical methods. In this payment system we use a combination of Finger-print technology (Physiological biometrics) and Mouse dynamics (Behavioral biometrics).

### 3.1 Finger-print Biometrics

This biometric technology is best accepted and is convenient to use. Finger-prints are routinely used in forensic laboratories [8]. Fingerprints consist of ridges and furrows that twist to form a distinct pattern. The pattern is different for each and every person. Companies increasingly use fingerprint scanners to authenticate computer users. Fraud is less in this technology compared to other biometric technologies. Finger print is obtained through electronic devises and can be used to authenticate the users in case of payments.

### 3.2 Mouse Dynamics

Mouse dynamics is a behavioral biometrics that can be used in several security applications. Here based on the mouse movements the authentication is done. Mouse actions may be Move, Drag-and-Drop, Point-and-click and silence [9].The average speed of the mouse movement and the average distance travelled in all directions is calculated. These represent the signature for a specific user. Mouse
dynamics is the combination of Movement speed, Direction of movement, Action type, Distance travelled and Time Elapsed.

### 3.3 Detection

There are three components for mouse dynamics detection unit. They are Data Interception unit, Behaviour Analysis unit and Behaviour comparison unit [10]. Data Interception unit converts mouse movements into meaningful information. Behavioral Analysis unit analyses the processed data and Behaviour Comparison unit compares generated signature with the original signature of the user. In this system the problem is if the users screen resolution and detection units resolution are not same the authentication will not be correct. Also operating system of both the systems must be same. Table 2 shows the information available to various parties in the transactions of this payment system.

Table 1: Information available in Digital Payment system using ID-based Blind signatures

| Info Party | | Seller | Buyer | Date | Amt | Item |
|---|---|---|---|---|---|---|
| **Seller** | | Full | None | Full | Full | Full |
| **Buyer** | | Partial | Full | Full | Full | Partial |
| **Law Enf** | **Before Anonymity Revocation** | Partial | None | Full | None | None |
| | **After Anonymity Revocation** | Full | Full | Full | Full | Full |
| **Bank** | **Before Anonymity Revocation** | Full | None | Full | None | None |
| | **After Anonymity Revocation** | Full | Full | Full | Full | Full |
| **Physical Observer** | | Partial | None | Full | None | None |
| **Electronic Observer** | | Partial | None | Full | None | None |

Table 2: Information available in Multimodal Biometric Payment system

| Info Party | Seller | Buyer | Date | Amt | Item |
|---|---|---|---|---|---|
| **Seller** | Full | Partial | Full | Full | Full |
| **Buyer** | Partial | Full | Full | Full | Partial |
| **Law Enf** | None | None | Full | Full | None |
| **Bank** | Full | Full | Full | Full | None |
| **Physical Observer** | None | Partial | Full | None | None |
| **Electronic Observer** | Partial | Partial | Full | None | None |

## 4. Mobile Payment System Based on RFID

Mobile payment is the field where several service providers compete. RFID (Radio-Frequency Identification) is a technology for automated identification of objects and people by space Coupling. RFID systems consist of two main components: tags and readers. Tags are radio transponders attached to physical objects. Radio transceivers, or readers, query these tags for some (potentially unique) identifying information about the objects to which tags are attached. Major functions of RFID are tagging, addressing and sensing [11]. The distinct advantages of RFID are its unique identification and automation features. Mobile payment systems are embedding RFID inlays in cell phone to provide a cashless way to pay for the goods [12].

### 4.1 Structure of the payment system

GPRS Mobile Payment System based on RFID is composed of Mobile Terminals, Communication Network, Mobile Payment Platform (MPP), Banks and Certificate Authority [13].

#### 4.1.1 Mobile Terminals

Mobile terminals include RFID tag, Java payment software and RFID reader. Each user has two RFID tags. They are Master tag and slave tag. The master tag is attached to the cell phone. The slave tag is similar to a credit card and can be used where mobile cannot be used. Slave card supports micro payments only. RFID reader includes a issuing initialize and a RFID point of sale. Issuing initialize initializes the tags. RFID point of sale reads information on the tags. Java software is used to exchange information with MPP through GPRS and also to provide a friendly environment for the user.

#### 4.1.2 Communication Network

These include mobile and cable networks for data format conversion and to connect to merchants and banks.

#### 4.1.3 Mobile Payment Platform (MPP)

This is core for mobile payment and is a platform for information exchange among Mobile terminals, Bank and Certificate authority. It contains relevant client's information.

#### 4.1.4 Bank

It contains a front end for data conversion and other for accessing the account.

#### 4.1.5 Certificate Authority

It issues certificates to the clients.

### 4.2 Working

*Setup:* First the user signs an agreement for mobile payment with telecom and also with bank. Then software and the certificate is downloaded. Then the keys will be generated and the mobile payment device is achieved.
*Payment:* First the information on the tag is read and is sent to the mobile payment platform. Then mobile payment platform sends the payment information. Now the client enters the type of payment, Bank name and password. Now if bank validates the information is transferred into merchant's account [14].In this payment system the transactions are conducted online. Payment is made from bank account.
Security measures in this system are ID certification, encrypted information transportation, verification of the data integrality, confidentiality of data and anti-denial requirement.
Table 3 shows the information available to various parties in the transactions of this payment system.

Table 3: Information available in Mobile Payment system based on RFID

| Info Party | Seller | Buyer | Date | Amt | Item |
|---|---|---|---|---|---|
| **Seller** | Full | Partial | Full | Full | Full |
| **Buyer** | Partial | Full | Full | Full | Partial |
| **Law Enf** | Full | Full | Full | Full | None |
| **Bank** | Full | Full | Full | Full | None |
| **Physical Observer** | None | Partial | Full | None | None |
| **Electronic Observer** | Partial | Partial | Full | None | None |

## 5. Smart Card Payment System

A Smart Card is a credit card sized plastic card embedded with an integrated circuit chip (ICC) which provides memory storage and processing power [15] as shown in figure1. Here we introduce Wireless Smart card Payment System using KSL protocol for payments over Internet [17]. Using the Wireless Smart Card transactions can be performed over the wired network. Smart cards with Wireless KSL payment protocol provides more secure payment system compared to credit cards. The Wallet Applet not only stores the crucial data but also validates with a pin number. The use of smart cards for the payments over Internet is secure because even if the card is stolen or lost no one can use it [16].

### 5.1 Working

This payment system has three main entities client, merchant and the payment gateway as shown in figure 2.Payment gateway includes the issuer and the acquirer. A master key Y is shared between the client and the issuer. The session keys Yi are generated at the client before each transaction by using cyclic shifting techniques. Wireless smart card has two parts.

#### 5.1.1 Off-card Smart Client

Here the user enters pin number for authenticated access.

#### 5.1.2 On-card Wallet Applet

This part is accessible only if entered pin is correct. This Wallet Applet stores the master key and the session keys [18].

### 5.2 Payment

#### 5.2.1 Session key generation:

The session key is generated from the master key on the Wallet Applet.

#### 5.2.2 Request

Client sends Payment request and Value Subtraction Request to the merchant.

#### 5.2.3 Encryption

Merchant encrypts the Value Subtraction Request and the amount payable combined with necessary information to form Value Claim Request and is signed with the merchant's private key. This is sent to Payment Gateway.

#### 5.2.4 Response

If the Payment Gateway gets the response from the issuer then it encrypts the Value Claim Response with merchant's public key and signs it together with Value Subtraction Response encrypted with Yi. Merchant then forwards Value Subtraction Response to the client's Smart Card. If the status is accept then Session key Yi is updated otherwise transaction is rejected and key Yi is not updated [19].
Table 4 shows the information available to various parties in the transactions of this payment system.

Table 4: Information available in Smart card Payment system

| Info Party | Seller | Buyer | Date | Amt | Item |
|---|---|---|---|---|---|
| **Seller** | Full | Partial | Full | Full | Full |
| **Buyer** | Partial | Full | Full | Full | Partial |
| **Law Enf** | Full | Full | Full | Full | None |
| **Bank** | Full | Full | Full | Full | None |
| **Physical Observer** | Partial | Partial | Full | None | None |
| **Electronic Observer** | Partial | Partial | Full | None | None |

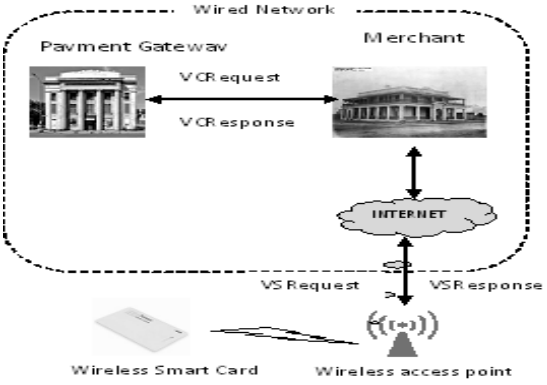


Fig 1: Payment mechanism

## 6. Biometric Fingerprint Payment System

Now-a-days the demand for enhanced security has been increasing and this lead to automated personal identification systems based on Biometrics. Biometric

systems may be used as a replacement for traditional systems.

### 6.1 Biometrics

The term biometrics is derived from the Greek words bio (life) and metric (to measure). Biometrics refers to the use of an automated system to verify personal identity through unique physiological or behavioral characteristics. Biometrics authenticates the individuals based on unique physical attributes that are difficult electronic payments [20]. Fingerprints consist of ridges and furrows that twist to form a distinct pattern. Although the manner in which the ridges flow is distinctive, other characteristics of the fingerprint called minutiae (figure 2) are most unique to the individual. These features are particular patterns consisting of terminations or bifurcations of the ridges. Fingerprints can be classified into three categories based on their major central pattern. These patterns are the arch, loop, and whorl as shown in figure 3 [21]

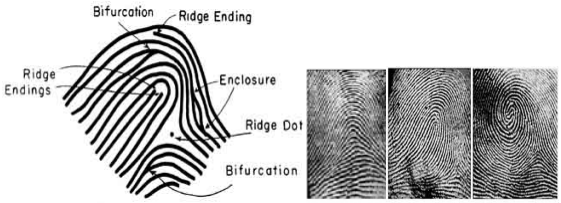


Fig 2: Minutiae Fig 3: Arch Loop Whorl

### 6.2 Working

#### 6.2.1 Account setup

Customers scan their fingerprint and enter their phone number, and then submit checking and credit card account information. Fingerprint is collected by a special sensing device. This process is called enrollment. The captured image can be stored directly as a image or as a biometric algorithm.

#### 6.2.2 Payment

The customer places his finger on a scanner at the register, enter their phone number, and choose how they want to pay (credit, debit, or checking). For added security they may enter a 4-digit pin. Software matches a fingerprint against the one scanned when the customer enrolls in the program. If matched then it sends select data from the data center to the point-of-sale terminal. Payment can be made to distributing bank [21].Table 5 shows the information available to various parties in the transactions of this payment system.

## 7. Comdata

Comdata offers a whole new way to manage purchases, payroll, security and many more. It is very simple, cost effective and works as an alternative to paper check for distributing funds to banked and unbanked employees. It is a card based solution for the business which makes it easy where there is no need to have a bank account for a card holder. The true power of comdata lies in the ability to make the multiple business functions [22]. But, the unbanked temporary, seasonal, geographically dispersed employees are not eligible for the direct deposits.

### 7.1.Working

The comdata card servers as a virtual bank account providing conveniences like a bank card. Totally the working of the comdata card is of three steps. The steps are as follows. [24]

Step1: In this step deposition takes place which means the transfer of funds takes place. (deposition into main account)
Step2: In this step transfer of the funds (deposited) takes place to the comdata cards of employee. (assigning fixed amount of money to each card)
Step3: In this step employees can use their card happily.

Comdata is solutions for many complex problems like cost and complexity in paper check, each card for each business can be used so, comdata have acquired unprecedented control over all business purchases. Comdata provides its payment processing only through the following cards all over the world-Visa, Master card, American express, Gift and loyalty cards, Discover, Comdata card for aviation fleet and fuel, Voyager, Wright express. Comdata provides many solutions for retail, aviation, construction, hospitals, restaurant to improvise them. But here retail, aviation solutions are discussed as an example.

### 7.2 Retail Solutions

It provides simple and cost effective solutions for unbanked employees. This type of paying is very flexible and convenient. It provides security for the transactions made by the employee and finally the B2B transfers are made easily. These are same advantages of comdata for hospitals and restaurants [22].

### 7.3 Aviation Solutions

Comdata is provided everywhere for FBO's(Fixed Base Operations).So, by using comdata we can manage all fuel purchases, maintenance charges etc., and smarter management of the [23]The below table illustrates the

properties of the comdata. The following table demonstrates the money is done.

Table 5: Information available in Biometric Fingerprint Payment system

| Info Party | Seller | Buyer | Date | Amt | Item |
|---|---|---|---|---|---|
| **Seller** | Full | Partial | Full | Full | Full |
| **Buyer** | Partial | Full | Full | Full | Partial |
| **Law Enf** | None | None | Full | Full | None |
| **Bank** | Full | Full | Full | Full | None |
| **Physical Observer** | Partial | Partial | Full | None | None |
| **Electronic Observer** | Partial | Partial | Full | None | None |

Table 6: Information available in Comdata Payment system

| Info Party | Seller | Buyer | Date | Amount | Item |
|---|---|---|---|---|---|
| **Seller** | Full | Partial | Full | Full | Full |
| **Buyer** | Partial | Full | Full | Full | Full |
| **Law Enf** | Full | Full | Full | Full | Full |
| **Bank** | Full | Full | Full | Full | Full |
| **Physical Observer** | Partial | Partial | Full | None | Full |
| **Electronic Observer** | Partial | Partial | Full | None | None |

## 8. Sound Based e-Commerce

The sound based system is a wireless web service. Even we can make e-commerce as m-commerce by entering the mobile number so that it checks for the authentication of the user and transaction is done only when the number is valid. In the past for performing mobile (money) transactions we need to have mobiles of sophisticated technology. This is considered as a barrier for the mobile commerce. But that barrier has been overcome by using the sound system. The basic operation is that the mobile produces sound which is converted into a number (probably credit card number) which gives the user details to the shopkeeper. Web services are network-based application components with services-oriented architecture. Customers who receive a unique sound-based file to their mobile phones through a web service are converted customer’s payment information. South Korea provides fertile ground for the growth of e-commerce as well as m-commerce. For the use of sound based m-commerce a mobile named MONETA was developed with a micro phone and chip which generate a unique signal which gives the customers identification number(credit card number).The shopkeepers has to install the necessary devices to work with moneta. This is a great barrier since the average price of high-end mobile phone using Moneta is quite high. People do not want to abandon the existing mobile phone which was not cheap either to a more expensive Moneta phone juts for the purpose of mobile commerce.[25]

A new physical m-commerce was introduced i.e. mobile bell-card solution. The Mobile Bell-Card Solution will use sound that is generated from the existing mobile phone and the sound can be recognized by the existing credit card reader of the shop with an installation of an ordinary microphone and simple software to process sound input. This system is made possible by utilizing the fact that each individual's identification information can be uniquely defined as a sound and the existing card reader with a microphone can receive the sound signal and the signal will be processed by the Point-of Sales computer that is used for card-reading, and processed information will be sent to the credit card company's main computer for authorization.

The obtained bell card is used for the transactions to buy the goods. Each transaction request is solved by the credit card company. The below data illustrates the sound based m-commerce. The following table demonstrates the information available to various parties in case of a transaction.

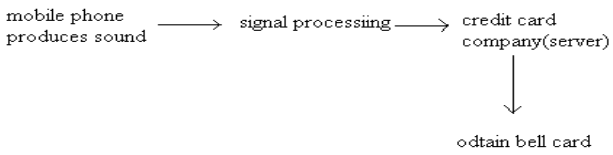


Fig4: obtaining bell card.

Table 7: Information available in Sound Based E-commerce Payment system

| Info Party | Seller | Buyer | Date | Amount | Item |
|---|---|---|---|---|---|
| **Seller** | Full | Full | Full | Partial | Partial |
| **Buyer** | Full | Full | Full | Full | Full |
| **Law Enf** | Full | Full | Full | Full | Full |
| **Bank** | Full | Full | Full | Full | Full |
| **Physical Observer** | Partial | Partial | Full | None | Partial |
| **Electronic Observer** | Partial | Partial | Full | None | Partial |

## 9. iKP Secure Electronic Payment System

iKP protocol system was developed in 1995 at IBM research labs in USA. It was incorporated in "secure electronic payment protocol (SEPP)" in the same year. It was the starting point for the "secure electronic payments". iKP is the family of the secure payment protocols. These protocols are compatible with the existing card based business model and payment system infrastructures, but it cannot be supported for systems other than credit and debit cards.[26] There exits three parties: the buyer, the merchant, the acquirer (acquirer gateway).Banks generally play the role of acquirer and credit card issuers but, this role is not considered in iKP protocols.

### 9.11KP

It is the simplest protocol which requires only the acquirer to possess a public key pair. Buyers and merchants will not have keys with them rather than they have authentic copies of the acquirer's public key. Certificates are provided for small no. of entities by minimal public key infrastructure (PKI). In the 1KP buyers are authenticated on the basis of their credit card numbers and optional secret numbers. Payments are authenticated by communicating the credit card numbers and the optional secret PIN numbers encrypted under the acquirer's public key. This prevents fraudulent merchants from collecting the credit card numbers and creating the fraudulent payments. It does not offer non repudiation for messages sent by the buyers and the merchants. It requires the minimum PKI.[29] Proof of transaction authorization by the buyer and the merchant are checked as a security requirement.

### 9.22KP

In 2KP protocol both the merchants and the acquirers hold the public key pairs and public key certificates and thus the protocol thereby provide the non repudiation messages originated by the merchants. 2KP allows the buyers to check whether they are dealing with the certified merchant or not. 1KP an 2KP allows payment orders authenticated via buyers credit card numbers and the PIN, encrypted before the transmission. Each seller in 2KP will have secret/public key which includes certificates. It requires a PKI covering all the merchants. Proof of transaction authorization by the buyer and the merchant are checked as a security requirement.[27]

### 9.33KP

3KP protocol is complex than the 1KP and 2KP protocols, but it is more secured than these protocols. In 3KP buyers have their own public key pairs and public key certificates and thus non repudiation for all the messages of all the parties. Here the authentication of the payment orders is done through credit card number, optional pin number and the digital signature. The buyer and the merchant have to take a lot of care to keep these signatures confidential because the virus called Trojan may hack the data. Necessary security measures should be implemented in the protocols to avoid different adversaries in any protocol. In 3KP unauthorized transactions are impossible. Proof of transaction authorization by the buyer and the merchant are checked as a security requirement. Receipt from the seller is also a security check in 3KP. The below table illustrates the 3KP protocol [27].

Table 8: Information available in iKP secure Electronic Payment system

| Info Party | | Seller | Buyer | Date | Amount | Item |
|---|---|---|---|---|---|---|
| **Seller** | | Full | partial | Full | Partial | Partial |
| **Buyer** | | partial | Full | Full | Full | Full |
| **Law Enf** | | Full | Full | Full | Full | Full |
| **Bank** | | Full | Full | Full | Full | Full |
| **Physical Observer** | | Partial | Partial | Full | Partial | Partial |
| **Electronic Observer** | **1kp** | Full | Full | Full | Full | full |
| | **2kp** | Partial | Partial | Full | None | None |
| | **3kp** | Partial | Partial | Full | None | None |

## 10. Conclusion

In this paper we have explored different technologies including their working and their advantages, disadvantages and enumerating security issues with respect to both the users and the bank which raises the levels of popularity of a technology. Each payment system has an edge over the other in various circumstances. It's the choice of the user to select the payment systems that suits best for his requirements. Not only businesses but governments and international organizations have a crucial role to play in shaping the future of the financial services industry. So in this paper we gave a brief analysis of present payment systems so that they can be used according to the state of affairs.

Table 9: Comparison of security issues of various Electronic Payment systems

| | Digital Payment system using Blind signatures | Multi Modal Biometric technology | Mobile Payment system on RFID | Smartcards |
|---|---|---|---|---|
| **Authenticity** | Good: Private keys containing user information is used to identify users | Best: Uses combination of mouse dynamics and finger prints. | Fair: Supports mutual authentication. | Good: Uses off-card pin verification. |
| **Privacy** | Good :Privacy holds with bank as well as shop | Good: No personal information is accessed. | Fair. No personal information is made available for unauthorized people. | Good: This can be used without revealing the client's information. |
| **Integrity** | Yes: Uses digital signatures to ensure integrity | Yes: Encrypts the data into useful information. | Good. Encrypted information is transferred. | Yes: Uses encryption and decryption techniques. |
| **Non-repudiation** | Yes: Once the message is signed information cannot be altered. | Yes: Details in the transaction cannot be altered. | Yes | Yes: Transaction details are maintained in records. |
| **Risk Management** | Good: Trustees can revoke anonymity in suspicious transactions. | Good: Risk is generally low in this payment system because it uses a combination of biometrics for authentication. | Fair | Fair |
| **Incentives** | No | No | No | No |
| **Relative feature advantage** | Good: Uses blind signatures. | Good: Uses multimodal biometric technology. | Fair: Uses RFID technology. | Good: Uses cards that do not transfer client |
| **Cross-border payment** | Yes | Yes | Yes | Yes |
| **Relative price advantage** | Fair | Fair | Poor: This system is costly. | Good |
| **Flexibility** | Fair: Can be used anywhere by people with bank accounts | Fair: The authentication systems must be present for payment. | Poor: People should have software installed in their mobile. | Fair: People need to carry these cards and should also have a bank account. |
| **Divisibility** | Fair: Digital currency should be generated for amount required every time. | Fair: Any denomination can be used in transaction. | Fair | Fair |
| **Transferability** | Good | Good | Good | Good |
| **Transparent** | Yes | Yes | Yes | Yes |
| **Auditability** | Fair: Only be done by trustee for anonymous | Good: The system records can be verified. | Good: Contains details of each and every transaction. | Good: Records are maintained for the |
| **Exitability/Reversibility** | Good: Transaction can be cancelled at any instance. | Fair: Transaction can be cancelled up to some extent. | Fair: Transaction can be cancelled. | Fair: Transaction can be cancelled up to some |
| **Interoperability** | Poor | Good | Fair | Fair |
| **Scalability** | Good | Good | Good | Good |
| **Economic viability** | Fair | Fair | Fair | Good |
| **Compatibility** | Fair | Poor: The recognizing system must be installed. | Poor | Good: Compatible with all kinds of browsers. |
| **Transaction Efficiency** | Good | Good | Fair | Good |
| **Database safeguarding** | Safeguards regular account information. | Safeguards all information in the transaction. | Safeguards all information in the transaction. | Safeguards all information in the transaction. |
| **Small payments** | Not suitable | Suitable | Not suitable | Suitable |
| **Current degree of popularity** | Popular: Will be used in coming future. | Not popular but will be used in future. | Not popular | Popular |
| **Consumers transaction risk** | No risk | No risk | No risk | No risk |
| **Party to which payment is made out** | Store | Store | Store | Distributing Bank. |
| **User Friendliness** | Fair: Easy after using once. | Fair: Easy for pc users. | Poor: understood only after using once. | Good: Easy for credit card users. |
| **Mobility** | Fair | Fair | Fair. Limited to people using mobiles with this payment system. | Good |
| **Anonymity** | Good: Blind signatures are used to provide anonymity of customers. | Good: Companies do not have any information about the user. | Fair: Data is encrypted. | Good: No information of client is used in transaction except card number. |
| **Financial risk** | Low | Low | Low | Low |
| **Value mobility** | Fair | Good | Fair | Good |

| | Biometric Fingerprint system | Comdata | Sound based e-commerce | iKP |
|---|---|---|---|---|
| **Authenticity** | Best: Uses finger prints. | Fair: Many cards are used on one account. | Good: Data is transferred through sound signals. | Very good: As the 'i' value increases authenticity will be much better. |
| **Privacy** | Good. Here companies pledge not to sell personal information or access it. | Fair: Only company knows all card details of the card holder. | Good: No company knows all the details of the user. | Very good: No company knows all the details of the bank. |
| **Integrity** | Good. There is no possibility of tampering data. Stores the finger prints in the form of digital certificates. | Good: Tampering data cannot be done but it cannot hide details from banks and companies. | Good: Tampering the data is difficult. | Very good: as the 'i' value increases. |
| **Non-repudiation** | Yes: Uses digital signatures. | Yes: For large payments. | Yes: Uses sound signals. | Yes: Uses agents in between the seller and the customers. |
| **Risk Management** | Good | Fair: Bank knows the account bal of all the card and all details about all card holders | Good: No cards are used and more over sound signals are used. | Good: Generally risk is low in iKP protocols. |
| **Incentives** | Yes | Yes | Yes | Yes |
| **Relative feature advantage** | Good: Improves security in payment transactions. | Fair: Can be improved in security aspect. | Good | Very Good |
| **Cross-border payment** | Yes | Yes | Yes | Yes |
| **Relative price advantage** | Fair | Very good: A company can make its purchases cost effectively. | Good: Cost effective when internet is provided at the cheaper cost. | Good |
| **Flexibility** | Good: Can be used anywhere without the need of any cards. | Fair: Cards should be used. | Good: No cards are used. | Fair: Cards should be used. |
| **Divisibility** | Fair | Good | Fair | Good |
| **Transferability** | Good | Good | Good | Good |
| **Transparent** | Yes | Good | Good | Good |
| **Auditability** | Good: Records can be verified. | Good: All the records of the transaction can be verified. | Good: Bank maintains the records of the card holders. | Good: Bank maintains all the records of the card holders. |
| **Exitability/Reversibility** | Fair: Up to some extent transaction can be cancelled. | Fair | Fair | Fair |
| **Interoperability** | Good | Fair | Good | Good |
| **Scalability** | Good | Good | Good | Good |
| **Economic viability** | Fair | Fair | Good | Good |
| **Compatibility** | Fair: Compatible with all kinds of browsers with identification system. | Fair | Good: Compatible with all kinds of browsers. | Good |
| **Transaction Efficiency** | Good. 70% faster than others | Good: Faster when compared to other card based transactions. | Good | Good |
| **Database safeguarding** | Safeguards all information in the transaction. | Safeguards all information in the transaction. | Safeguards all information in the transaction. | Safeguards all information in the transaction. |
| **Small payments** | Suitable | Not suitable | Suitable | Suitable |
| **Current degree of popularity** | Popular | Popular | Popular in some countries where mobile usage is high like south Korea. | Popular |
| **Consumers transaction risk** | No risk | No risk up to some extent | No risk | No risk |
| **Party to which payment is made out** | Distributing Bank. | Distributing Bank. | Distributing Bank. | Distributing Bank. |
| **User Friendliness** | Good: Easy to use. | Good | Fair | Good |
| **Mobility** | Good | Good | Good | Good |
| **Anonymity** | Good: Companies will not be able to attain personal information of the user. | Fair: The company which holds the account knows the information about the card holder. | Good: Here companies will not be able to know the info about the user. | Very good: companies will not be able to know the info about the users. |
| **Financial risk** | Low | Low | Low | Very low |
| **Value mobility** | Good | Good | Good | Good |

## References


[1] M.Dileep, E.Vedavalli, J.Sridivya. "Payment Systems and Techniques and Their Implication on E-Commerce." Proc. of International Conference on Systemics, Cybernetics and Informatics. Hyderabad: Pentagram Research Centre (P) Limited. 2009. 176-86. Print.

[2] Jan Camenisch, Ueli Maurer, Markus Stadler. "Digital Payment Systems with Passive Anonymity-Revoking Trustees." N. pag. Print.

[3] Chaum, D, 1983. Blind Signatures for Untraceable Payments, Advances in Cryptology-crypto'82 Springer- verelag, Santa Barbera, CA, USA, pp-199-203.

[4] D. Boneh and M. Franklin, "Identity-based Encryption from the WeilPairings", In Proceedings of CRYPTO 2001, Springer-Verlag, LNCS2139, 213-229, 2001.

[5] P. Barreto, H. Y. Kim, B. Lynn and M .Scott, "Efficient Algorithms for Pairing-based Cryptosystems", In Advances in Cryptology- CRYPTO 2002, Springer-Verlag, LNCS 2442, pp. 354-368, 2002.

[6] Hassan Elkamchouchi and Yasmine Abouelseoud. "Privacy Protecting Digital Payment System Using ID-Based Blind Signatures with Anonymity Revocation Trustees." N. pag. Print.

[7] School of Electronics and Information Engineering, China, Fenghua Wang, Jiuqiang Han. "ROBUST MULTIMODAL BIOMETRIC AUTHENTICATION INTEGRATING IRIS, FACE AND PALMPRINT." N. pag. Print.

[8] IBM T. J. Watson Research Center Digital Persona Inc. Dept. of Comp. Sci. and Eng., Sharath Pankanti Salil Prabhakary Anil K. Jain. "On the Individuality of Fingerprints¤." N. pag. Print.

[9] S.Benson Edwin Raj A. Thomson santhosh. "A Behavioral Biometric Approach Based on Standardized Resolution in Mouse Dynamics." N. pag. Print.

[10] S.Asha, Dr.C.Chellappan 1. "Authentication of E-Learners Using Multimodal Biometric Technology." N. pag. Print.

[11] http://www.rfidjournal.com/article/view/5021

[12] Bhuptani Manish, Moradpour Shahram, "4RFID Field Guide: Deploying Radio Frequency Identification systems", Prentice Hall PTR, 2005.

[13] Research Institute of China Mobile Crop., China Mobile Solution of Mobile Micro-payment, 2002.

[14] Beijing University of Posts and Telecommunications2Guilin University of Electronic Technology National UWB IT Research Center (UWB-ITRC), Inha University, Wei LIU, Chenglin ZHAO, Wei ZHONG, Zheng ZHOU,Feng ZHAO, Xiaoji LI, Jielin FU1'2,KyungSup Kwak. "The GPRS Mobile Payment System Based on RFID." N. pag. Print.

[15] Venkatesan Sundararajan, 1998. "Smart Cards: Enablers for Electronic Commerce." N. pag. Print.

[16] Tolga KILIÇLI. "Smart Card HOWTO." N. pag. Print.

[17] Kungpisdan, S., Srinivasan, B. and Le, P. D., Lightweight mobile credit-card payment protocol, Progress in Cryptography INDOCRYPT 2003,LNCS, Springer-Verlag, Vol. 2904/2003, pp.295-308, 2003

[18] Giorgio, R. S., Trommler, P., (1998) "Smartcards and the Open Card Framework", Java World, Available at: http://www.javasoft.com/

[19] School of Network Computing, Monash University Osama Dandash, Xianping Wu, and Phu Dung Le. "Wireless Internet Payment System Using Smart Cards." N. pag. Print.

[20] Julia Scheeres: "Will It Be Cash, Check or Finger?"

[21] Sub committee on biometrics, National Science and Technology Council (NSTC). "Myongji University, Yongin-Si, Kyonggi-Do, South Korea 449-728, Dileep Kumar, Dr.Yeonseung Ryu, Dr.Dongseop Kwon."A Survey on Biometric Fingerprints: The Card less Payment System." N. pag. Print.

[22] www.comdata.com

[23] Fleet credit card program rfp#06597. Thesis. Washington, 2008. Washington: Comdata cooperation, 2008. Print.

[24] "Comdata a perfect partner in pursuit of a paperless payroll." Rev. of Amy logan. Print.

[25] Ook lee. Sound-based mobile payment system. Thesis. Hanyang University, Seoul, Korea. Print.

[26] Internet Keyed Payments Protocol (iKP). Thesis. M. Linehan, G. Tsudik, IBM research, July, 1995. Print.

[27] Design, Implementation, and Deployment of the iKP Secure Electronic Payment System. Thesis. Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Member, IEEE, Els Van Herreweghen, and Michael Waidner, Member, IEEE. Print.

[28] www.domino.watson.ibm.com

**B. Tirimula Rao** has Masters of Technology in Computer Science and Technology from Andhra University. He is currently working as a Senior Assistant Professor in Computer Science and Engineering Department at Anil Neerukonda Institute of Technology and Sciences. His main interests lie in Image Processing, Computer Networks, Network Security, Cryptography, Neural Networks, Software Cost Estimation and Fuzzy Logic. He is a member of IEEE.

**M. Dileep** is a B. Tech final year student of Department of Computer Science Engineering, Anil Neerukonda Institute of Technology & Sciences. His interests include Electronic Payment systems, Soft Computing, Image processing Genetic Algorithms and Cyber Forensics. He is a student member of IEEE.

**E. Vedavalli** is a B. Tech final year student of Department of Computer Science Engineering, Anil Neerukonda Institute of Technology & Sciences. Her interests include Electronic Payment systems, Soft Computing, and Intrusion Detection systems.

**K. Aditya** is a B. Tech third year student of Department of Computer Science Engineering, Anil Neerukonda Institute of Technology & Sciences. His interests include Electronic Payment systems and Fuzzy logic.

**D.R.S Bindu** is a B. Tech third year student of Department of Computer Science Engineering, Anil Neerukonda Institute of Technology & Sciences. Her interests include Electronic Payment systems and Network Security.