

# Study and Analysis Issues for Mobile Payment third Party System

<sup>1</sup>Pavan P. Soni, <sup>2</sup>Ravi. S. Patel, <sup>3</sup>Jignesh A. Chauhan, <sup>4</sup>DR. V.R. Rathod  
<sup>1,2,3</sup>Asst. Prof., AMPICS, Ganpat Uni., Kherva, INDIA  
<sup>4</sup>Director, Dept. Of Comp. Sci., Marwadi Foundation, Rajkot, INDIA

## ABSTRACT

In Some Mobile payment Model, we have seen third party involvement for mobile payment transaction. In that model entities are Customer, merchant, third party payment gateway and bank. We have studied Third Party Mobile Payment System, analysis and discussed issues with this system.

## Keywords

Third Party, Pin, Mobile Operators, Mobile Payment, SMS, Bank, Transaction

## I. INTRODUCTION

M-commerce is the next generation of today's PC-based wired, e-commerce technology. The evolving success of mobile communication is transforming e-commerce (wired environment) into m-commerce (wireless environment), and as a group, users of mobile devices (PDAs, smart phones, etc.) are considered as a large potential market. It is expected that mobile and wireless systems will control the Internet industry in the future, and it will merge e-commerce and m-commerce into a singular blended entity. With the rocketing number of wireless service subscribers, the mobile phone is treated as a more convenient, immediate, and personalized means for consumer transactions. We are using m-payment for paying bills, booking tickets, and the like. We have found emerging factors for m-commerce: payment cards, networking functionalities, and infrastructures and intermediary entities with multiparty payment functionalities. M-payment establishes relationships across domains among customers and merchants by means of business and banking domains.

For m-payment, various entities are involved: consumers, merchant, mobile operators, and banks. Therefore, we are focusing on various issues in m-payments. Nevertheless, these security solutions are not sufficiently robust when new components intend to participate in the m-commerce process. The existing payment facilities have issues regarding infrastructure, service charges, and security. Consumers cannot do m-payment transactions anytime or anywhere because of high fees and lack of infrastructure. The requirements on the consumer side are any smart or debit card and an online transaction facility. It becomes an issue of security. [1]

Our survey is said that there are many entities like Banks, Mobile Operators and Third Party involvement and routes are in general Mobile Payment Model. The results are unsecure payment transaction, less confidence, fear to do transaction, so it cannot attract customer. Therefore, customer satisfaction and moral are going down. They are not accepting credit/debit card to solve this issues. There are Mchek, PayPal, Google Checkout and Amazon Payments are a few well-known third-party service providers.

## II. BACKGROUND

### A. *M-Payment:*

There are two types of payment methods; exchanging and provisioning. Exchanging is to change coin, money and banknote in terms of the price. Provisioning is to transfer money from one account to another. In this method, a third party must be involved. Credit card, debit card, money transfers, and recurring cash are all electronic payments methods. Electronic payments technologies are magnetic stripe card, smartcard, contact less card and mobile handset. Mobile handset based payments are called mobile payments.

### *Security*

An authentication is to identify or verify identity of payer for mobile payment transaction. Authentication are generally classified as under:

Something the user has (e.g., identity card, security token, software token, phone, or cell phone)

- Something the user knows (e.g., a password, or personal identification number (PIN))
- Something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier)

Two-factor authentication often a combination of methods are used, e.g., a bankcard and a PIN, in which case the term two factor authentication is used. Business networks may require users to provide a password and a random number from a security token.

Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract. Although this concept can be applied to any transmission, including Television and Radio, by far the most common application is in the verification and trust of signatures.

## III. STUDY

We have studied some third party payment model. The entities are Customer, Bank, Third Party, Operators, and Merchant in it. Mobile Payment model involved third party that relatives your credit/debit card to your mobile phone, allowing you to do payments from your mobile phone. Airline tickets, movie tickets, insurance premium, Hotel Bills and all purchases can be made securely from the convenience of a mobile phone.

We are discussing a mobile payment third party system for studies:

### *Process for Third Party Mobile payment model:*

- Install software in mobile phone

- Customers have to register their mobile number and credit/debit card information.
- Acquire PIN
- Merchant have to also make registration process in that system and have to do contract with them.
- In that, some banks also associated with them.
- One or more mobile operators also associated with them.

## IV. ANALYSIS AND ISSUE

### 1. *Limited awareness in People:*

According to RBI's statistics, With 41% of the population in India unbanked, financial inclusion could not have been top of mind when these guidelines were developed. The 41% equates to approximately 410 million people that do not have access to banking services – this is a number greater than the entire population of the US being financially excluded from mobile payment services.

### 2. *Confusion to select Third Party Payment Gateway:*

Choosing your payment gateway is a key part in the development process of your ecommerce solution, there are many different gateways in the market and all offers something different to the other. The most professional way of incorporating a gateway into your solution is to acquire a merchant account from any bank, which then gives you the flexibility to take payments through various payment gateway versions. Whether you are building a new ecommerce website or upgrading an existing website choosing the right payment gateway can have a major effect on your customer's online experience.

### 3. *Share your card details to them: They will have access to your personally identifying information:*

in order to perform their functions, but may not use the information for any other purposes. In such cases, we will have a nondisclosure agreement with the service provider to ensure your contact information is protected and is not misused.

### 4. *Limited registered entities:*

In individual third party system, there are limited registered or associated entities like customers, merchants and banks. So we cannot do all type of transactions in it.

### 5. *Compulsory remember one more account settings:*

Customers have to remember one more password/PIN to do mobile payment transactions in mind.

### 6. *Depends on Mobile operators SIM:*

Some Third party transaction is limited to operators and supported their software to SIM of Operators.

### 7. *Limited and Selected Transactions:*

Customer can do limited and selected transaction because limited customer and merchant are registered.

### 8. *Limited Fund Transfer:*

Customer cannot do fund transfer because another customer may be not registered in this system. If registered, limitation of fund transfer issues occurs.

### 9. *Indirect involvement of Bank:*

Third Party act master role in this system. Banks involved in it indirectly. So completely transaction is gone through Third Party not directly bank. If third party is not trusted or payment not done then issues occurs.

### 10. *Legal issues:*

Today almost is not perfectly clear about legal status of third party in business and the relationship between parties about their rights and obligations. This provides payment services for customers; means heavy funds or issues a large amount of electronic money. Directly Government and Main Bank Authorities do not control some extent they acts and have characteristics of banks, but they and their transactions. The legal status of the third-party online payment platform needs further clear legislation to regulate [5].

## V. CONCLUSIONS

There is lots of legal and characters issues are involved in Third Party Payment System. The major thing that the entities are registered less for transaction. Bank is not involved directly in it. Thanks to our guide Dr. V. R. Rathod for guidance in our research.

## VI. REFERENCES

- [1] Pavan P. Soni, "M-Payment Between Banks Using SMS" , ISSN:0018-9219, Pages: 903 - 905 IEEE JUNE 2010
- [2] Pavan Soni, "Card Based Secure Mobile Payment Model" , KITE-2011, 2011
- [3] Hany Harb, Hassan Farahat, and Mohamed Ezz, "SecureSMSPay: Secure SMS Mobile Payment Model" , Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on IEEE, 2008 PP. 11-17
- [4] P. Garner, I. Mullins, R. Edwards, and P. Coulton, "Mobile Terminated SMS Billing – Exploits and Security Analysis", Proceedings of the Third International Conference on ITNG, IEEE, 2006, pp. 1-10.
- [5] Guoling Lao, Shanshan Jiang, "Risk Analysis of Third-Party Online Payment based on PEST Model", Management and Service Science, 2009. MASS '09. International Conference, IEEE, 2009, PP. 1-5