# Secure and Efficient Protocol for Mobile Payments

KOTA SWETHA[1],DIVYA GOTTIPATI[2], GATTINENI ROHINI[3], SIVA PRASAD PINNAMANENI [4]
[1,2,3] *B.Tech, Computer Science, VasireddyVenkatadri Institute of Technology, Andhra Pradesh, India*
[4]*Associate Professor, Computer Science, Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India*

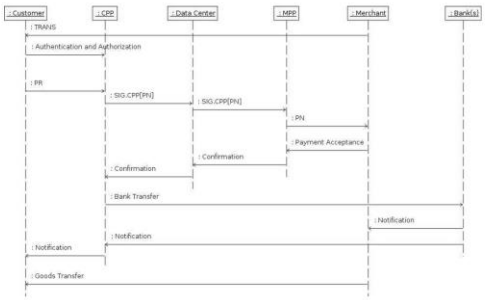
***Abstract -- Electronic payments have gained tremendous popularity in the modern world. Credit/debit cards and online payments are in widespread use. Bringing electronic payments to the mobile world offers huge utility for mobile users. Lack of standardized protocols, interoperability and security are ma-jor roadblocks in developing a mobile payment infrastructure. A scheme called SEMOPS (Secure Mobile Payment Service) has already been proposed by A. Vilmos and S.Karnouskos. This proposed SEMOPS architecture addresses these problems. However, it will work inefficiently for micropayments due to a lot of computation and communication for every payment. Good micropayment support is extremely important for mobile payment systems to succeed. This work focusses on enabling efficient micropayment sup-port in SEMOPS scheme. An analysis of the security and efficiency of the proposed method is given in this paper. Our new proposed method has been found to be very efficient for micropayments in SEMOPS.***

## I. INTRODUCTION

Mobile payments have gained potential in the modern world and offer many services than electronic payments but mobile payments lack interoperability and security. Interoperability is one of the reason why mobile payments have not become much popular. A system called SEMOPS have been introduced by A. Vilmos and S. Karnouskos to provide secure platform and good interoperable mobile payment system. SEMOPS is a mobile payment solution that is capable of macro and micro payments efficiently and securely. It can support any type of transaction type including P2P, B2C, B2B, P2M with local and international geographic coverage. SEMOPS realize a payment service with huge transaction potential, lower cost overhead and large turnover. However, in this system payment is made immediately in each transaction. This method is efficient for macro payments (payment whose cost over head is negligible compared to the overall payment value) for micro payments this method is in efficient. Micro payment scheme has been fitted in the SEMOPS with slight modification in the original SEMOPS architecture.

## II. EXISTING SYSTEM

### 2.1 SEMOPS WORKFLOW




#### 2.1.1SEMOPS ENTITIES

Users

In the SEMOPS architecture users are of two types' customers and merchants. Each user has unique PIN to authenticate and authorizes the transactions and keep the information confidential with himself.

Customers

Customer is one of the user who pays money to the merchant for goods and services he purchases. Customer is a person or PC on the internet.

Merchant

Merchant is one of the user in the SEMOPS who offer goods and services to the customer.

PAYMENT PROCESSORS

Payment processor is point of contact to users and system. It is a trusted partner in the mobile payments. It contains confidential information like account numbers, users PIN etc. SEMOPS contains two types

of payment processors they are Customer Payment Processor and Merchant Payment Processor.

Customer Payment Processor

CPP is a point of contact to the customer and the system. CPP interacts with multiple customers. When the customer wants to make a payment he/she selects the CPP which it wants to use.

Merchant Payment Processor

MPP is a point of contact to the merchant and the system. MPP interacts with multiple merchants.

Banks

Banks has the user's accounts. Any number of banks present in the system. SEMOPS contains interbank procedures in which it performs transactions from different banks.

Data Center

Data center is a centralized data storage of users and payment processors. Data center decides which payment processor should be contacted to send a message to the certain user if the user is in the data center coverage area. Mobile Network Operators maintain Data Centers.

Working of SEMOPS payment system

1. Merchant send the transactional details to the customer in TRANS. This includes details that uniquely identifies the merchant and the individual transaction.

2. Customer receives the transactional details from the merchant and combines with information that identifies his/herself. Payment request PR is prepared. Then he selects the CPP where the payment request is processed. When the payment request is ready to transfer, the customer checks its content, authorizes and sends the PR to the respective CPP.
3. The customer receives PR, identifies the customer and process PR. CPP verifies the content and process the PR. Processing includes availability of necessary funds in the bank and reservation of funds in the bank. When the processing is completed, a payment notice PN is prepared by the CPP. PN is signed by the CPP and forwarded with the digital signature to the data center.

4. Data center receives PN and forwarded to the MPP. However, in case of international transaction second data center is involved. MPP receives PN and digital signature, verifies the signature and identifies the merchant from PN. Merchant has a chance to control the content of payment notice and decides the approval or rejection of transaction. If the merchant approves the Transaction, a conformation is sent by the MPP to the CPP through the Data center.

1. CPP receives the confirmation it initiates bank transfer to the merchant's bank. Transfer is based on regular as well as interbank procedures. In case of successful transaction, merchant's bank sends a notification the merchant. Customer's bank sends a notification to the customer. If in case Merchant rejects the transaction CPP releases the funds it has reserved for the purchase.

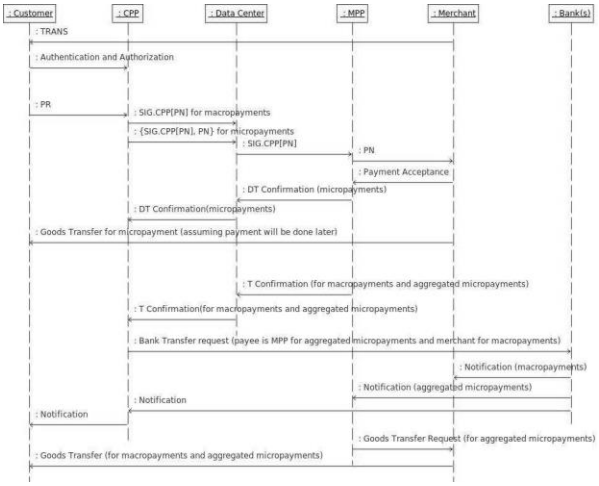
2. If in case of successful transaction transfer of goods can be done when the merchant gets a notification from its bank stating that transfer had been done.

Abbreviations & Annotations

| | |
|---|---|
| CPP | Customer payment processor |
| DC | Data center |
| MPP | Merchant payment processor |
| PR | Payment request |
| PN | Payment notification |
| PIN | Users password |

| | |
|---|---|
| ACCNO | User Account Number |
| SIG | Digital signature |
| TRANS | Transactional details |
| SEMOPS | Secure and efficient protocol for mobile payments |

## III. PROPOSED SYSTEM




Micro payment scheme has been fitted in the original SEMOPS with slight modifications in the original SEMOPS. As the users increases the number of CPP'S, MPP'S and DC'S increased in direct proportion. Lot of computation is done for every payment. This increases the overhead cost for payment. This paper suggests a scheme to enable the micro payments efficiently and securely in SEMOPS protocol. In the proposed scheme aggregation of micro payments is done.

### 3.1 SOLVATION OF MICRO PAYMEMT'S PROBLEM

Aggregation is achieved by introducing intermediaries between customer and merchant to pay the micro payment amount.

Using intermediaries

- Consider a set of customers C1, C2……Cn pays money to the merchants M1, M2….., $_{Mn}$. The intermediary I has been introduced between the customer and merchant has an account using which it makes payment.
- Suppose C1 wants to make payment to m1. Instead of paying amount directly to M1 it instructs I to make payment to M1. This instruction I gives the guarantee that C1 will redeem all the money it is supposed to pay at later time.
- I pay amount to the MPP immediately again the cost overhead is too high. Instead of paying amount immediately. Intermediary I give guarantee to M1 that it pays money later that C1 gives.
- M1 transfers goods to C1 that has asked for. This goes for every micropayment between $_{Cj}$ and $_{Mj}$.
- I keep a track of record that how much money it is supposed to receive from each customer and how much money it is supposed to pay for merchants.

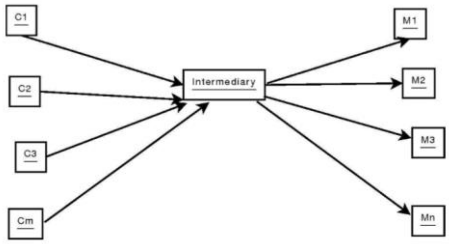



**Figure 2: Aggregating Micropayments using One Intermediary**

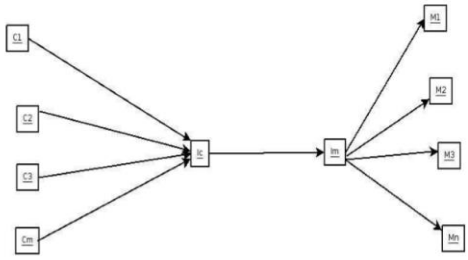



**Figure 3: Aggregating Micropayments using Two Intermediaries**

MICROPAYMENT PROPOSAL

Customer to merchant

Customer gets transaction data from merchant. Customer does not identify himself to the merchant. Merchant sends transactional details to the customer.

Payment request from customer to the CPP

Customer builds payment request and authorizes it using PIN. PR identifies the payment details and the customer. Customer selects CPP and authorizes and authenticates himself to CPP. Customer sends PR to the selected CPP. PR contains transaction details of the merchant and authorizes using PIN of the customer.

At CPP site

CPP process PR and decides whether the payment is micro payment or macro payment. If it is macro payment it checks if the funds are present in the customer's account or not. If funds are not present, then CPP intimates the customer and rejects the transaction. If funds are available in the customer account, then CPP reserves required amount of funds for the payment and builds payment notice PN using PR. PN contains only transactional details and some details that may be required.

If the payment is micro payment, CPP checks how much money the customer is supposed to pay to CPP from all previous un paid micro payment transactions. It adds the previous payment to the current payments after adding it is less than macro payment no checking is done for funds in the customer account. PN is prepared and forwarded to the MPP. If the current payment is greater than or equal to the micro payment, then it means that customer has not paid its previous micro payment transactions. CPP initiates bank transfers bank transfers from customer account to its account to get this pending amount from previous transactions. If bank transfer succeeds, then PN is prepared and the total amount is paid by the customer to CPP is made zero. If the transfer fails, the customer micro payment transaction rejected. If bank transfer succeeds, then PN is built. PN= [TRANS, CPP details] CPP then computes a signature of PN. It forms a PN Message by combining together PN and digital signature. PN Message=[SIG.CPP[PN], PN]. CPP forwards PN Message to DC. Data center receives PN Message and decides that at which MPP PN Message should be sent so that it will reach the merchant

CPP stores all the micro payment received from the customer in a data structure. The data structure should be that,

It should possible to locate all micropayment requests made by customer in a less time and possible to know how much money that a customer can be paid using this data structure in a less time.

T AND DT CONFIRMATION MESSAGES

In the SEMOP protocol confirmation message was sent to the customer. Let us call this message a T confirmation (transfer confirmation) message. If the payment is macro payment DT confirmation (delayed transfer confirmation) was sent. DT confirmation message is just an approval of transaction on behalf of the customer at later time

MPP SITE

After receiving of PN, MPP checks weather it is micro payment or macro payment and verifies the digital signature. If it is invalid it MPP rejects the transaction. Otherwise proceeds with the payment to the merchant for approval. MPP stores the PN's it received in a data structure and decides PN should be sent to the correct merchant.

## SECURITY AND EFFICIENCY CONSIDERATIONS

SEMOPS is a trust worthy platform in this system Customer trusts CPP but CPP does not trust customer. PIN authorization of customer ensures that CPP contains confidential information of customer.

Micro payment transactions are done by aggregating the group of micro payments this achieves efficiency in micro payment transactions and reduces the payment cost overhead

## IV. CONCLUSION

In the proposed system we are using RSA algorithm for calculating digital signature and k-means clustering algorithm for aggregating the micro payments to do the micro payment transactions

efficiently. By using RSA algorithm and k-means algorithm computational cost is reduced.

REFERENCES


[1] A. Vilmos and S. Karnouskos. Semops: Design of a new payment service. In Proceedings of the 14th International Workshop on Database and Expert Systems Applications, pages 1–5. IEEE, 2003.

[2] S. Micali and R. L. Rivest. Micropayments Revisited. Laboratory for Computer Science, Massachussets Institute of Technology, Cambridge, MA 02139.

[3] T. Dahlberg, N. Mallat, J. Ondrus, and A. Zmijewska. Mobile Payment Market and Research ˆaAS¸ Past,˘ Present and Future.

[4] D. N. and A. Vukasinovic. Mobile payment solution symbiosis between banks application service providers and mobile network operators. In Proceedings of the Third International Conference on Information Technology: New Generations(ITNG'06), pages 346–350, 2006.

[5] C. Brookson. GSM (an PCN) Security and Encryption. 1994.

[6] S. Karnouskos, R. J. Kauffman, E. Lawrence, and K. Pousttchi. Guest editorial: Research advances for the mobile payments arena. Electronic Commerce Research and Applications, pages 1–4, August 2007.

[7] Tsalgatidou, Veijalainen, and Pitoura. Challenges in mobile electronic commerce. In Proceedings of IeC 2000. 3rd Int. Conf. on Innovation through E-Commerce. Manchester UK, pages 1–12. Finnish National Technology Agency, November 2000.

[8] J. Ondrus and Y. Pigneur. An assessment of nfc for future mobile payment systems. In Sixth International Conference on the Management of Mobile Business (ICMB 2007),0-7695-2803-1/07, page 3. IEEE, 2007.

[9] H. H.-p. LI Xi. A secure mobile payment system. Computer Technology and Application, ISSN1934-7332, USA, 1(1):1–6, June 2007.

[10] A. Fourati, H. K. B. Ayed, and A. Benzekri. A set based approach to secure the payment in mobile commerce. In Proceedings of the 27th Annual IEEE Conference on Local Computer Networks (LCN 02, 0742-1303/02, pages 1–2. IEEE, 2002.

[11] 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.

[12] S. Karnouskos, A. Hondroudaki, A. Vilmos, and B. Csik. Security, trust and privacy in the secure mobile payment service. In 3rd International Conference on Mobile Business, pages 3–5, July 2004.