ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Quick Pay A Micro-payment

[1]Asmita More, [2]Bhakti Mahadik , [3]Tulika Harsulkar and [4]Suchita Patil
[1,2,3]U.G. Student, Department of Computer Engineering,
[4]Professor,Department of Computer Engineering,
K.J.Somaiya College of Engineering, Vidyavihar,
Mumbai,India

Abstract: Mobile Commerce is Electronic Commerce on Mobile devices to purchase goods or services in wireless environment. The development of new applications of electronic commerce that require the payment of small amount of money to purchase services or goods opens new challenges in the security and privacy fields. In this paper we present a new efficient and secure micropayment scheme for merchants and the privacy of the customers and also guarantee no financial risk. In addition, the proposed system defines a fair exchange between the micropayment and the desired good or service. In this fair exchange, the anonymity and untraceability of the customers are assured.

Keywords: Electronic Commerce, Anonymity, Untraceability, Security, Financial risk, Micropayment

I. INTRODUCTION

The field of electronic commerce (e-commerce) evolves day by day introducing new applications and services. Mobile banking is one of the e-commerce services that allow customers to do banking transactions on their mobile phone. Bank transactions, such as balance inquiry, money transfer, online payments and other mobile services usually require the transmission of critical information.

A micropayment is a mobile banking transaction involving a very small sum of money in exchange for something. Therefore, micropayments can easily be applied to the intangible selling of goods such as information (newspapers, product reviews, location-based services, etc.), virtual gifts or electronic data (music, videos, etc). They have unique functional and security requirements inside the field of electronic payments. As this involves low-value transactions, so the operational cost needs to be as low as possible in order to be profitable for merchants and customers.

There are two primary concerns for the development of micropayment systems to avoid financial risks for both merchants as well as customers – firstly security properties, secondly efficiency and cost for individual transactions.Our proposed Quick Pay application allows micro transaction for users in a secure and efficient way. It keeps the secrecy of the user identity by privacy features through anonymity, untraceability and unlinkability. It also limits the overall cost of the micro transaction.

II. OVERVIEW

A. Entities:

The entities involved in the Quick Pay Application are as follow:[3]

a. Money_Sender:

Registered user of the application who sends money to the receiver.

b. Money_Receiver:

Registered user of the application who receives money from the receiver.

c. Mobile-Money Application Server:

It receives request and sends response to the end users. It has centralized control on all activities.

d. Network Service Provider:

It provides mobile network to the subscribed users.

e. Bank:

It maintains details of the users who have bank accounts.

f. Voucher:

Vouchers are generated by the application server and made available in the market for sale.
application.[1] Hashing is used to encrypt login password of

B. Architecture :

The user to give security to transaction. The MD5 message-digest algorithm is a widely used cryptographic hash function that produces 16 byte hash value. Further Verification Number is generated every time the user login the Quick Pay application to add one more layer of security to the transaction.[4]

ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

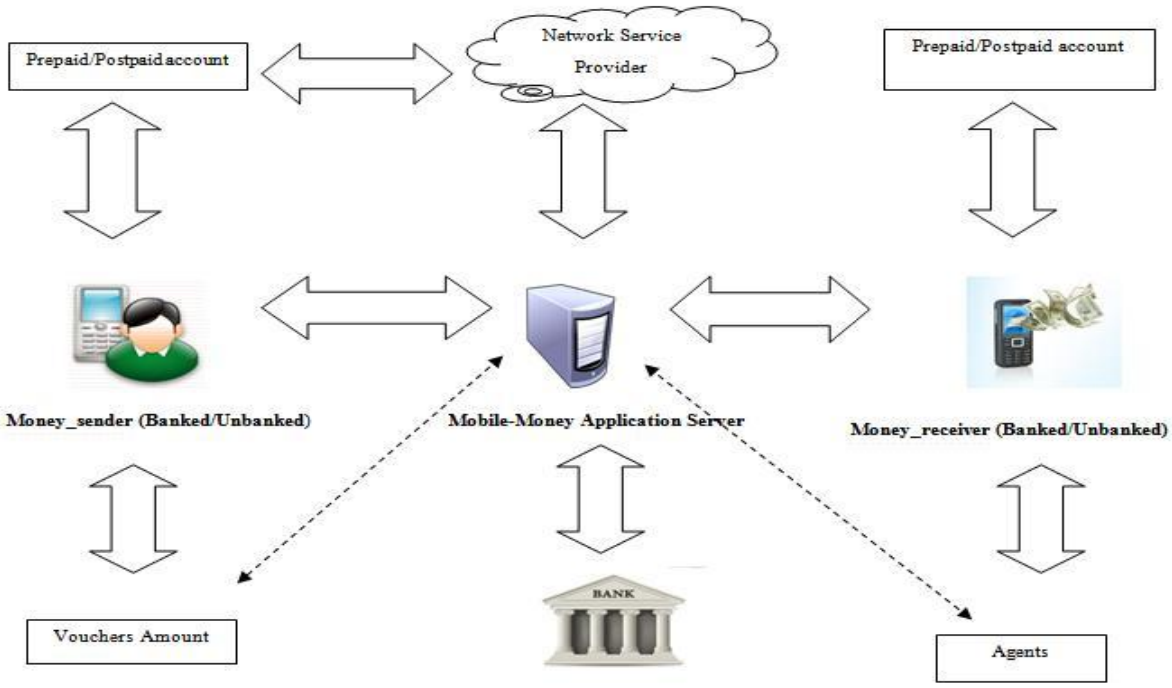

Figure 1. Architecture design of Quick Pay application.

Fig 1. Is the basic architecture for Quick Pay is illustrated in the above figure.

In the Quick Pay application, the users must be registered in the bank and the application. For using the application the user should log in the system by entering the appropriate user id and password. The user id and password are validated for security. Only if the user is registered with the bank, the user can login successfully. After logging the user can generate voucher by loading coins.

Once the voucher is generated it is send through email or message to the customer. The customer redeems the voucher money through bank.

C. System Architectural Design:

a. Module 1:

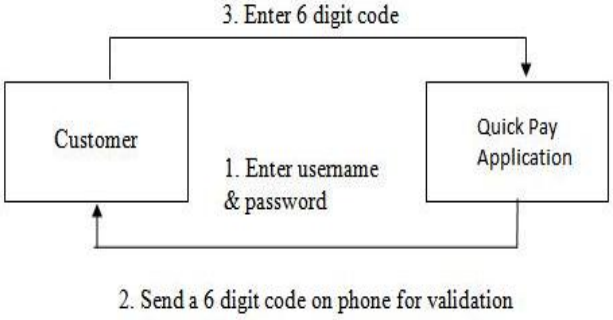

Figure 2. Device Registration

Fig 2. Is the device registration in which the customer is the registered user of bank and application. The customer login into the Quick Pay application using user name and password. A 6 digit verification code is sent to the registered mobile number of the customer. The customer then enters the 6 digit verification code to successfully login into the

b. Module 2:

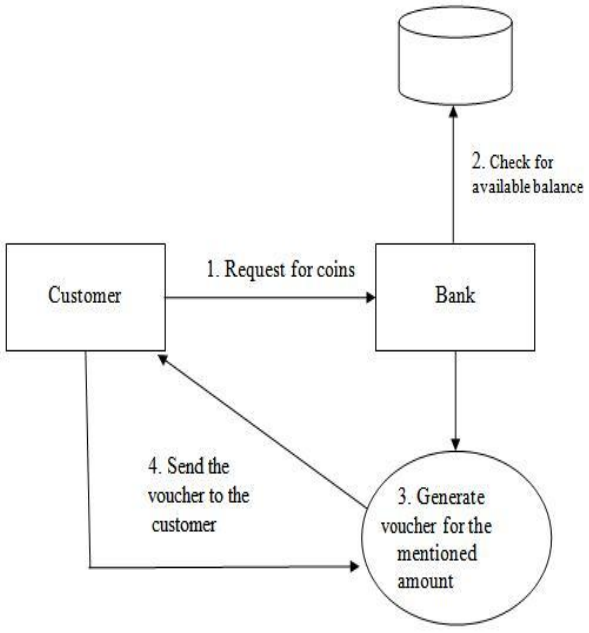

Figure 3. Coupon Generation

Fig 3. Is coupon generation,after successful login, the customer will request the required number of coins from the bank in the application. In this process, the bank checks for the available balance in the account, also the customer can manually check the balance in the application. Once it is verified the voucher for the required amount is generated.[1][3][4]

c. Module 3:

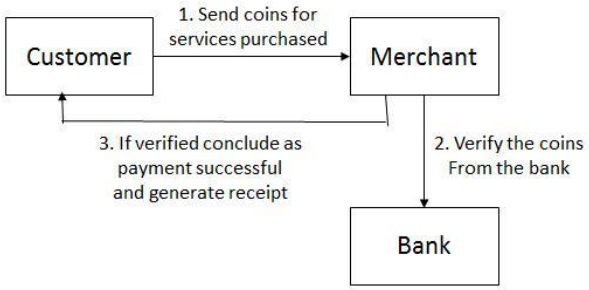

Figure 4. Make Payment

Fig 4. Describes make payment module where the customer sends receiver ID and coins from his account. Receiver ID is validated at server. If receiver is a valid user, the bank server validates the coins received from customer send to user 2.

Coins are deleted from merchant's Quick Pay account and added to customer's Quick Pay Account. Thus the transaction can be done anytime anywhere.

d. Module 4:

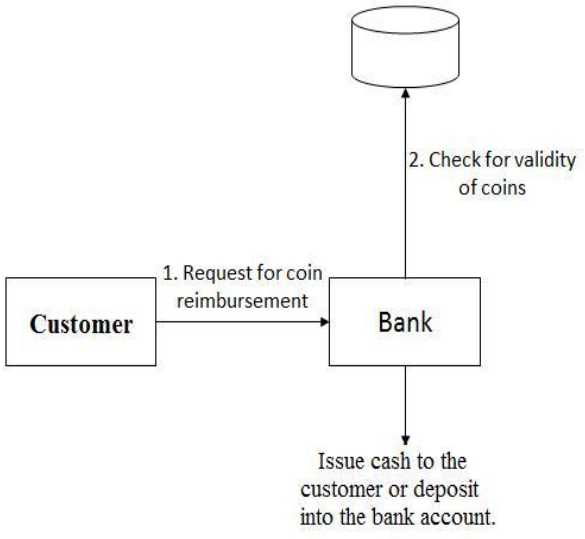

Figure 5. Reimbursement of coins

Fig 5. Is reimbursement of coins where the customer requests for reimbursement or unloading of coins. First the bank checks for the validity of the coins and unloads the coins into the application account or directly into the bank account.

D. Security Features:

The Quick Pay system accomplishes the following security requirements:[5][6]

a. Privacy:

Banking is one of the most risky sectors as far as privacy is concerned due to the highly sensitive and personal nature of information which is often exchanged, recorded and retained. The following are the privacy concerns in our system:

a) Anonymity:

The primary concern of privacy is to keep the user identity clandestine. This property allows the user to use the service without being identified.

b) Unlinkability:

Unlinkability only has a meaning after the system in which we want to describe anonymity. It establishes links between senders of different transactions. So, linkability connects different transactions to a user, but this user remains anonymous.

c) Untraceability:

It is defined as the indistinguishability of the past and future interactions of the identity of the user with the knowledge of the current transaction. Thus, the adversary has not to be able to identify the user. In general, untraceability implies anonymity.

Fair or Atomic Exchange

Services can be transferred through networks. For this kind of goods the atomic exchange of coins and services is desirable.

E. Functional Features:

The Quick Pay system accomplishes the following functional features:[1]

a. Low Transactional Costs:

The cost of each micro transaction is less than the amount transferred in the payment. Low transactional cost is achieved by making changes in the following fields:

b. Volume of information:

The volume of information transferred for payment is minimized.

c. Storage requirements:

Avoid use of large databases.

d. Use of voucher:

The security algorithm is implemented more efficiently by generating vouchers for specific services or specific providers rather than building generic vouchers for any purpose.

e. Financial Risks Control:

The assumed risks are controlled even if security measures are limited in order to minimize costs.

III. COUPON GENERATION

In the proposed system, the user loads required number of coins from which a coupon is generated. The coupon generation is implemented using hash chain algorithm.[1][3]

***A. Hash Chain*:**

A hash chain ($\omega N \cdots \omega 0$) is defined as a set of values where each ωi (with the exception of the value ωN) is obtained after the application of a one-way function

(typically a cryptographic hash chain) over the value ω(i+1), i.e., ωi = H ω(i+1) for 0 ≤ i ≤ N − 1.

In order to initialize the hash chain, the generator picks and stores in a secret way a random seed value ωN . Then, he applies iteratively the hash function H over it up to the value ω0, called root. In order to proceed to the hash chain verification, the verifier has to know the root value ω0. Then, the verification of a chained element ωi is done applying i times the hash function H over it, checking the relation Hi (ωi) ? ≡ ω0. The key feature of hash chains is that if a value ωi is provided, it is not feasible to find another ωj where j > i such that H(j−i) (ωj) = ωi.

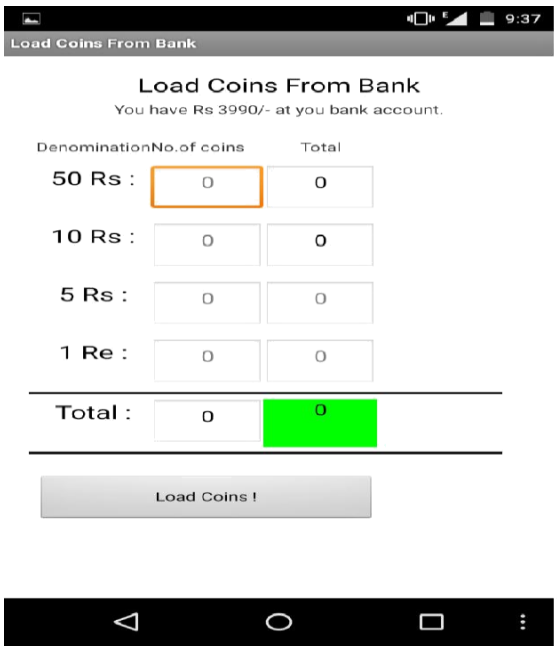

Figure 6. Loading coins from Bank account

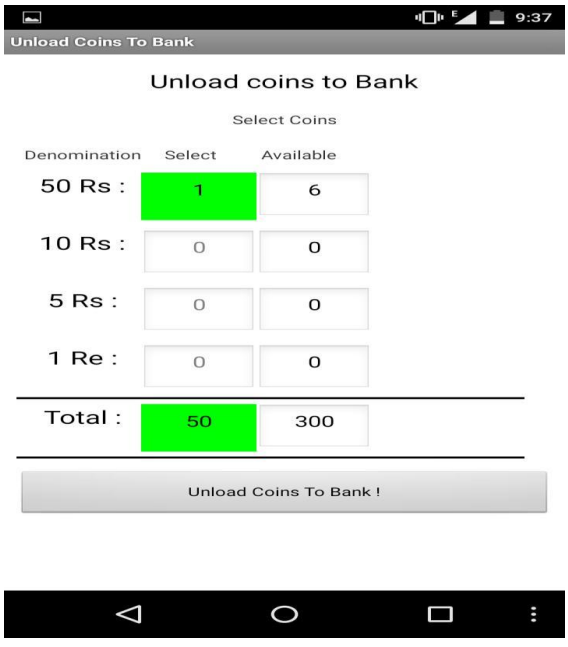

Figure 8. Unloading coins into the bank account from application account.

V. CONCLUSION AND FUTURE SCOPE

The proposed system accomplishes all the required security features while the efficiency and low cost are preserved. The key features achieved in this system are

IV. IMPLEMENTATION DETAILS

The money transfer limit for this application is Rs. 1 To Rs.1000. Minimum amount in the Quick-Pay-Account is Re. 1.The primary modules are Loading coins into application account.making payment and unloading the coins into bank account.

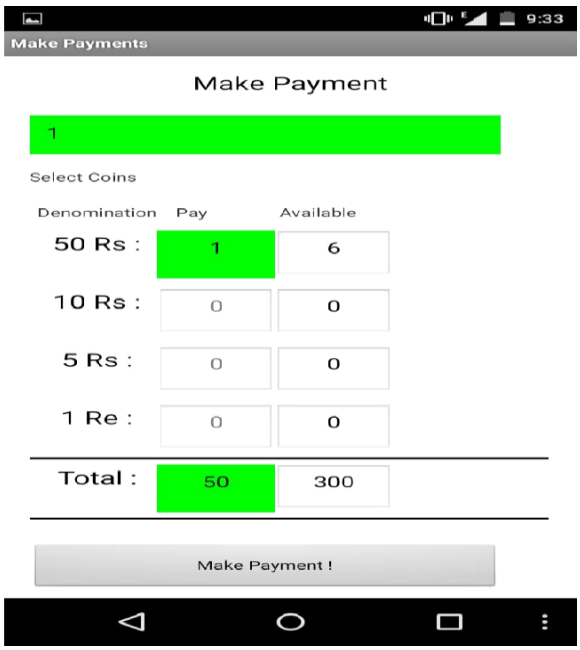

Figure 7. Make Payment

anonymity, untraceability and unlinkability. Moreover, the algorithm preserves the fairness of the payment exchange since a number of coupons are exchanged for a particular service. The system assures that it is not possible to commit fraud with the voucher. Thus, the scheme is secure against double spending, forgery and overspending.

The system does not use expensive algorithm, such as public key cryptography during the payment phase, and communication and storage costs are also low. Therefore, it is used for mobile devices.

The future work will be focused on allowing the customers to spend more than one coupon pair using the same transaction. The users can also credit application account using mobile money.

VI. ACKNOWLEDGMENT

We would like to express our deepest appreciation to all those who provided us the possibility to complete this report. A special gratitude I give to our final year project mentor, Mrs. Suchita Patil, whose guidance and contribution in stimulating suggestions and encouragement helped us to develop this project.

VII. REFERENCES

[1] Isern-Deya, Andreu Pere Payeras-Capella, M. Magdalena Mut-Puigserver, Macia Ferrer-Gomila,Josep L., "Untraceable, anonymous and fair micropayment Scheme," IEEE latin america transactions, vol. 10, no. 3, April 2012.

[2] A.P.I.Deya, L.H.Rotger, M.P.Capella and M.M. Puigserver,"Anonymous,Fair and Untraceable Micropayment Scheme: Application to LBS," IEEE Latin American Transaction,Vol.10,No.3,April 2012.

[3] Pradipta Dey, Kuntal Dey, Vinod Mankar, Sougata Mukherjea,"Towards an interoperable mobile wallet service," Emerging Technologies for a Smarter World (CEWIT), 2013 10th International Conference and Expo on 21-22 Oct. 2013.

[4] P. R. Bayyapu and M. L. Das,"An Improved and Efficient Micro-payment Scheme," Journal of Theoretical and Applied Electronic Commerce Research ISSN 0718-1876 Electronic Versión VOL4/ISSUE1 /APRIL 2009/91-100 © 2009 Universidad de Talca – Chile, DOI: 10.4067/S0718-18762009000100008.

[5] T. Poutanen, H. Hinton, and M. Stumm. NetCents,"A lightweight protocol for secure micropayments," in USENIX Workshop on Electronic Commerce, pages 25-36, August 31– September 3, 1998.

[6] C. Schmidt and R. M• uller,"A framework for micropayment evaluation,"NETNOMICS, pages 187-200, Volume 1, Issue 2 , pp 187-200, 1999, DOI 10.1023/A:1019110007282.

