A new Anonymous Mobile Payment System: MobiCash

Tejashree Gurav
tejashreedgurav@gmail.com

Pramila Daundkar
preu92@gmail.com

Vimal Gowda
vimalcomp9@gmail.com

Urmila Kute
urmi19293@gmail.com

ABSTRACT

M-commerce is a new field, extended from the combination of electronic commerce and emerging wireless and mobile networks. With M-commerce customers get new opportunities for their business from any location at any time. Mobile application transforms the mobile phone into a mobile wallet with digital cash supporting both anonymity and security. In this article we suggest a new strategy to support m-commerce transaction which provides fully anonymity with security for mobile users. Our scheme is based on 256 bit SHA algorithm which provides security to our application. The paper describes the framework, model and details of the protocol.

General Terms

Security, Anonymity, Protection

Keywords

M-commerce, e-commerce, SHA, DigiCash

1.Introduction

Nowadays m-commerce has become an important issue due to enormous growth of mobile technologies. New technologies have made wireless business transactions possible that allows mobile phones and other handheld devices to access the internet. In mobile telecommunication system, most e-payment systems are not suitable because of certain characteristics of mobile devices. Further in many payment system, customer does not want any other person to know about his/her transaction as well as the he/she does not want to be recognized. So we propose MobiCash protocol that provides fully anonymity to the user. In this paper, we try to eliminate a few drawbacks of e-payment system without losing any advantages of e-payment system.

2. Existing Systems

2.1.Credit Card Payment System:

It is one of the most frequently used system for paying on the internet. However there are some drawbacks in using credit card system such as customer can lose his/her credit card number to fake person etc.

2.2. Electronic Check:

Using electronic checks one can make a payment for any transaction that a paper check can cover and are superintended by the same laws that apply to paper check. However in electronic check customer experiences delays in payment transactions due to returned check.

2.3. Smart Card:

Smart card is an another means for purchasing. A smart card or integrated circuit card (ICC) is a pocket-sized card with ingrained unified circuits However it can be easily lost, slow adoption.

2.4. Electronic Cash:

Electronic cash is a digital portrayal of money. E-cash works in the similar form as the electronic fund. However electronic cash has many drawbacks such as failure of technology, fraud, possible tracking of individual.

2.5.Micro Payments:

A micropayment isa commercial business that involves a very small amount of money and usually one that appears online. Micropayments are normally used to purchase online goods and services such as music, memberships and e-books. However,the customer must in some instances, in the past should have opened an account with an intermediary.

3.Proposed system

In mobicash payment system,three parties are involved that are Clients, merchants and banks.

Client- Client purchases goods or pay for the services by using mobicash system.

Merchant- Merchant trades services and goods, it also interact with mobicash bank for authentication and validation of payment.

Bank- Both client and merchant should have an account in mobicash system.

As we have mentioned in Introduction, MobiCash is a payment system that provides security, efficiency and fully anonymity to the customer by which the customer remains anonymous from bank and merchant.It provides high level of privacy to the customer. MobiCash protocol is based on e-cash system.

In these paper we try to eliminate some problems of e-cash system such as over spending and double spending.

4.Major Difference in Proposed System as Compared To Existing System

In existing Mobicash system , Mobile application download is mandatory.

This paper describes application can be used over Mobile without any software download or changing the phones.

In existing system, primary account is managed with mobile number, which is insecure as mobile may loss and information can be leaked.

In MobiCash system, user have to open an account with the bank availing the facility of Mobicash with the Registered PAN number & Mobile to avoid duplicacy as well as to maintain security.

In Current system, while doing online transactions, Credit card number or account number need to be key in,which has threat to customer of losing out on confidential information over internet.

In MobiCash system, the user will be given a separate account which he can recharge with money from savings account.So limited money will be available on the account. Hence less threat & more secure.

In MobiCash system the passwords are encrypted & the only link between merchant & bank is the reference number given by bank to merchant for each transaction

5.System Architecture

The protocol has the following steps :

1. Customers visit merchant's website.

2. Then the customer has to login in mobicash bank account, for new customer he/she has to register.

- During registration on mobicash bank account, the customer has to provide mobile number and PAN number.

- The customer has to provide proper mobile number since the entire transaction is based on mobile number.

3. After signing up the customer will get his/her account details.

4. Customer has to register in mobicash client login(if new user).

- During registration the customer have to select the bank from the given list(which is tie-up with mobicash system).

5. The customer will login into mobicash after which he/she shop online/pay for services.

6. Customer will select product or services then payment procedure will start.

7. For payment, customer login to mobicash bank account where he/she has to provide banks login id and password and the transaction process starts.

8. Then customer will get details about his/her account details which contain mobile number and requested amount for verification.

9. After verification, the requested amount will be deducted from customer's account and will be deposited in merchant's account.(if the requested amount is not available in customer account then the transaction will get aborted.)

10. If the transaction is successful then unique reference number is generated and it will be send to merchant's and customer's bank.

11. At the end of transaction, report will be generated by system which can be seen by customer.This report will contain details about transaction like mobile number of customer,requested service,bank status,reference number.

12. Logout and session closed.

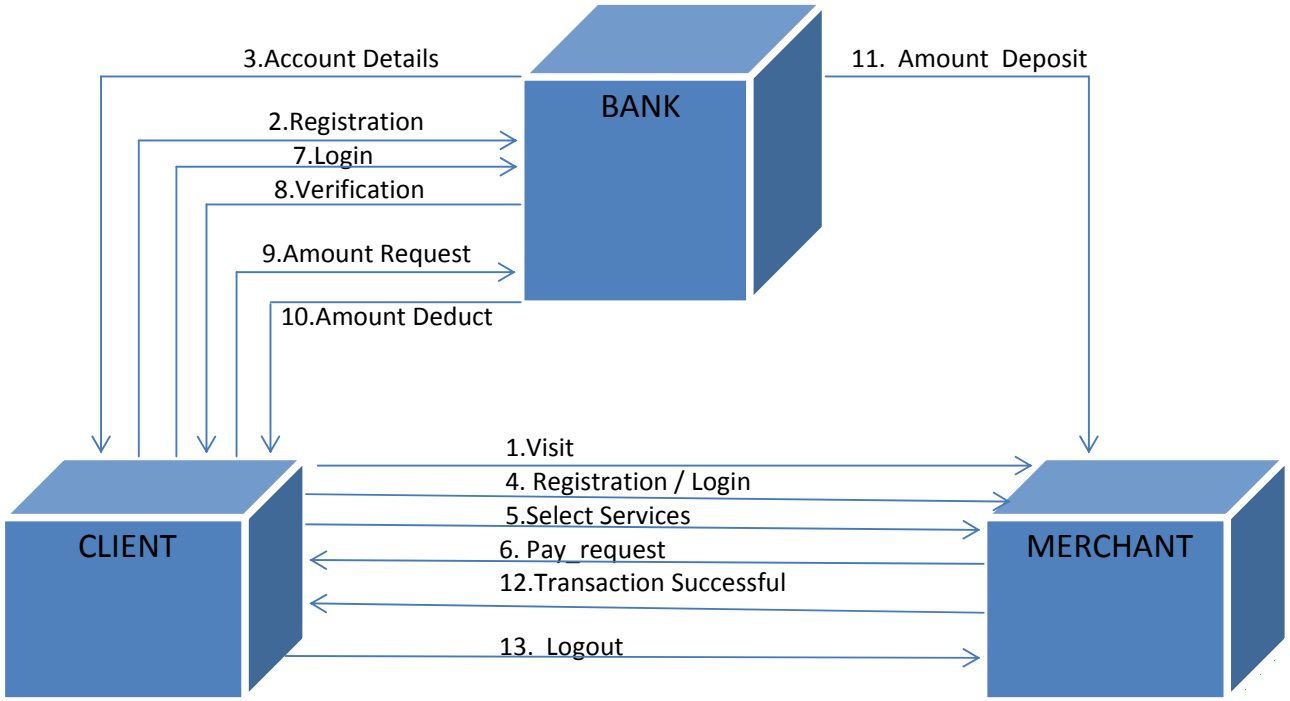

Fig 1: MobiCash Protocol

(if the requested amount is not available in customer account then the transaction will get aborted.)

A. User Interface Design
In this module we have designed the user interface for overall web application. We design the user interface to show our propagation of our web system and flow of overall design in a graphical manner or GUI. By showing the output in GUI gives more attractive and understandable to everyone. Thus we design the whole user interface in this module

B. Bank Module
In this module we have designed the overall bank module that describes the transaction between bank and customer.

C. Product Module
In this module we have designed the product and detail information about the products. This module is self explanatory and user friendly.

6.TECHNOLOGY AND CONCEPTS

The following depicts the concepts and technology used in the proposed system:

6.1 SHA Algorithm:

SHA algorithm use two 160-bit registers, consist of five 32-bit sub-registers. The basic SHA-1 algorithm is conferred as follows:

1) The algorithm starts by loading the five sub-registers of the first 160-bit register X labeled H_0, H_1, H_2, H_3, H_4 as follows:

H_0=67452301; H_1=EFCDAB89; H_2=98BADCFE; H_3=10325476; H_4=C3D2E1F0;

2) SHA-1 go over through each of the 512-bit message blocks viz. m_0, m_1, m_2,…., m_{n-1}. For each of the message block, do the following:

a. Write m_j as a sequence of sixteen 32-bit words,
$m_j = W_0 \| W_1 \| W_2 \| \dots \| W_{15}$

b. Figure out the remaining sixty four 2-bit words as follows:
- $W_t = (W_{t-3}$ xor W_{t-8} xor W_{t-14} xor $W_{t-16})$
- Cyclic shift of W_t by 1 i.e. $S^1(W_t)$

c. Copy the first 160 bit register into the second register as follows:
A= H_0; B= H_1; C=H_2; D=H_3;

E= H_4;

d. The following stepcontain a sequence of four rounds, analogous to four intervals 0<=t<=19, 20<=t<=39, 40<=t<=59, 60<=t<=79.

For t = 0 to 79,

- $T=S^5(A)+f_t(B,C,D)+E+W_t+K_t$
- E=D;D=C; C= S^{30}(B);
- B=A; A=T

e. Once all four rounds of operations are finished, the second 160-bit register (A, B, C, D, E) is added to the first 160-bit register (H_0, H_1, H_2, H_3, H_4) as follows:

- $H_0 = H_0 + A$;
- $H_1 = H_1 + B$;
- $H_2 = H_2 + C$;
- $H_3 = H_3 + D$;
- $H_4 = H_4 + E$;

3) Once the algorithm has processed all of the 512-bit blocks, the final output of X becomes the 160-bit message digest.

6.2 Encryption:
Encryption in cryptography is the process of encoding messages so that only authorized parties can read it. In encryption process,messages are encrypted using encryption algorithm. In similar way to secure our system we are providing Secure Hash Algorithm(SHA) of 512 bit. We are providing one time password scheme to bank login of our system. One time password is more secure than any other encryption scheme because the message can only be encrypted but it cannot be decrypted. Main aim of using SHA algorithm in our system is that it is latest algorithm used for protection and it is more secure than any other algorithm because it is computationally inaccessible to find a message that corresponds to a given message digest, or to find two different messages which produce the same message digest. If anyone try to innovate a message in transit,it will result in a different message digest and the signature will decline to verify.

Conclusion

Mobile Commerce is an important topic of research and application and the key technology of electronic commerce is E-cash system. In this paper, we have proposed MobiCash wallet and also shows how M-commerce can indeed have digital cash. The main focus of MobiCash is to work online for mobile devices that support security and fully anonymity for mobile users. In this paper we have tried to exclude some problem of e-cash system too.

ACKNOWLEDGMENTS

We thank our Head of Institute Dr. Shubha Pandit, Head of Department H.N.Bharati and Project guide Mrs. Rohini .Nair for encouraging us to study and explore this topic and provide the related references; our teachers who helped us understand the basic concepts related to system security. We also extend a big thanks to our parents for their constant encouragement.

REFERENCES

[1] B. Kim , “design of fair tracing e-cash system based on blind signature”thesis of school of engineering Information and Communication university of Korea, 2003.

[2] D.Chaum ,”Blind Signature for Untraceable Payments” In Advances in Cryptology-CRYPTO’ 82, pp. 199-203,1983.

[3] W.Chung ,”Mobile Commerce Security and payment methods” , Auburn University,Usa, IDEA GROUP Publishing,2005.

[4] D.O.Mahony and T.Hitesh,” Electronic Payment Systems for Ecommerce, Second Edition”, press in Artech House,2001.

[5] B.Gehling and D.Stankard ,” ecommerce security”,Information security Curriculumn Development(InfoSEcCD) conference , copyright ACM

[6] M.Y.Rhee,”Internet Security Cryptographic Principles, Algorithms’ and Protocols” press by John Wiley, 2003.

[7] H.Marko and H.Kostantin and T.Elena ,” Utilizing national public key infrastruature in mobile payment systems”,press in Elsevier, 28 march,2007.

[8] A.Nash , W.Duane and C.Joseph,”PKI Implementing and Managing Esecurity” RSA press,2001