ENHANCED PAYMENT GATEWAY FOR E-COMMERCE WEBSITE

USING SIGNCRYPTION PROTOCOL

Pradnya Rane*

Austin Lewis*

Shravan Jaiswal*

Praharsh Jha*

Abstract—

In our daily lives, we use many E-commerce websites that perform monetary transactions over the internet. In case of a transaction failure due to various reasons such as poorly maintained database, slow server or internet connection, the customer's money may get deducted from his account without actually the order being placed. Also, it may so happen that after placing an order, the customer would want to cancel the order. Money once debited has to go through bank procedure to be deposited back to the customer's account which generally requires 3 to 4 days, causing poor user experience. To avoid this, we propose a solution wherein in case of occurrence of such transaction failure, the amount of money mistakenly debited or the amount customer is liable to receive after cancellation of an order would be credited to the customer in form of Electronic cash (e-cash) immediately. This would remove any inconvenience the customer faces and betters user's online experience. Also, since money is being credited to the customer in form of E-currency, it compels the user to reuse it in the same company's website thus causing higher customer retention. Here, by using signcryption technique we avoid double spending in e-cash transactions. A single protocol is used to update all databases which helps to maintain consistencies.

***Index Terms*— E-commerce, monetary transactions, electronic cash (e-cash), signcryption, double spending.**

* Department of Computer Engineering, St. Francis Institute of Technology, Mumbai, Maharashtra, India

I. INTRODUCTION

In our daily lives, we use many E-commerce websites such as online shopping, online recharge and online ticket booking websites etc. that perform monetary transactions over the internet. In case of a transaction failure due to various reasons such as poorly maintained database, slow server or internet connection, the customer's money may get deducted from his account without actually the order being placed. Also, it may so happen that after placing an order, the customer would want to cancel the order. In either of the cases, money once debited from the account has to go through bank procedure to be deposited back to the customer's account. This bank procedure generally requires 3 to 4 days. This causes poor user experience. We address this problem in our paper.

Customer satisfaction is an important aspect for any successful E-commerce websites. Therefore it is essential to address all inconvenience that is caused to the customer and remove them. Therefore we through this paper will try to propose certain solution which will help to regain confidence of customer. Moreover, for a healthy growth of a business, customer retention is instrumental. Taking into consideration all these aspects, we propose a solution wherein the amount of money mistakenly debited or the amount customer is liable to receive after cancellation of an order would be credited to the customer in the form of E-cash immediately.

Signcryption [1] protocol is used to avoid double spending in e-cash transactions. Thus creating a foolproof payment gateway for any website.

II. PROBLEM DEFINATION

For every transaction that fails, the payment gateway takes 3-4 working days to refund this amount. This causes high customer dis-satisfaction. Also there is problem of customer retention wherein such customers may not revisit the website again. Any e-commerce website having high number of customer logging together faces this problem. These include all shopping portal as well as ticket booking websites. It is important to address all inconvenience that is caused to the customer and remove them.

III. EXISTING SOLUTION

E-payment system using signcryption is based on cryptographic primitive 'Signcryption' which performs simultaneous tasks of message encryption as well as digital signature which

reduces computational cost. Since, Signcryption satisfies Unforgeability, Confidentiality, and Non-repudiation which assures security during a transaction. Even if an adversary tries to break the security by cracking some data related to transaction, he has to know private key of issuer bank, a random number generated during computation & encryption key used in algorithm which is computationally impossible.

Since single protocol is used to update all databases of customer and merchant the issue of double spending is solved. In a single operation all databases and logs are updated thus preventing inconsistencies in databases. This also helps to reduce response time of the entire transaction which in case of various independent protocols would require more time. [1]

Off-line Electronic Payment System Based on Bilinear Pairings and Signcryption states that, electronic payment system plays a crucial role, acts as a backbone of this virtual market place. Hence, the need for more efficient electronic payments has become an essential fact. The problems encountered in e-cash systems are as follows:-

1: Bank has to maintain a large database for storing the coins series number to keep track of double spent coins.

2: Problem of security:- Often in digital cash system customer account number, password are sent without encryption via e-mail. There is a security breach due to Man-in- middle attack.

Unlike the existing e-payment system question of double spending of e-cash arises because each transaction are made unique having unique transaction id. Therefore no need for additional storage for spent coins. All transaction detail are signcrypted and hence secure. [2]

Integrated On/Off-Line Electronic Cash states that, e-cash can be classified into two types, which are on-line e-cash and off-line e-cash, and they are suitable for different applications and environments. All of the proposed e-cash schemes only focus on on-line or off-line e-cash, but not both. In these schemes, users must decide which type of e-cash they will use later when withdrawing.

In an on-line e-cash scheme, if a shop receives an e-cash from a user, it will verify the correctness of the e-cash first and then sends the e-cash to the bank to make double-spending checking immediately (checking if the e-cash has existed in the bank's database).

In an off-line e-cash scheme, when a shop receives an e-cash from a user, the shop will directly accept it after verifying its correctness. The off-line e-cash does not need to be sent to the bank for double-spending checking immediately. After a period of time, the shop deposits the received off-line e-cash into the bank, and then the bank performs the double-spending checking subsequently. [3]

IV. PROPOSED SOLUTION

To avoid this problem of delayed refund, we propose a solution wherein in case of occurrence of such transaction failure, the amount of money mistakenly debited or the amount customer is liable to receive after cancellation of an order would be credited to the customer in the form of E-cash immediately. This would remove any inconvenience the customer faces and betters user's online experience. We can thus achieve customer satisfaction, which is an important aspect for successful E-commerce. Also, since money is being credited to the customer in form of E-currency, it compels the user to reuse it in the same company's website thus causing higher customer retention.

In order to implement this we will consider aspects such as E-cash & payment gateway in the field of E-commerce as well as Encryption for transactions.

Also by using signcryption technique we avoid double spending which is highly rampant in e-cash transactions. A single protocol is used to update all databases which helps to maintain consistencies.

In this manuscript, we shall deal with purchasing e-books from an online e-book portal to understand the working of our system in an e-commerce website.

A. Flowchart

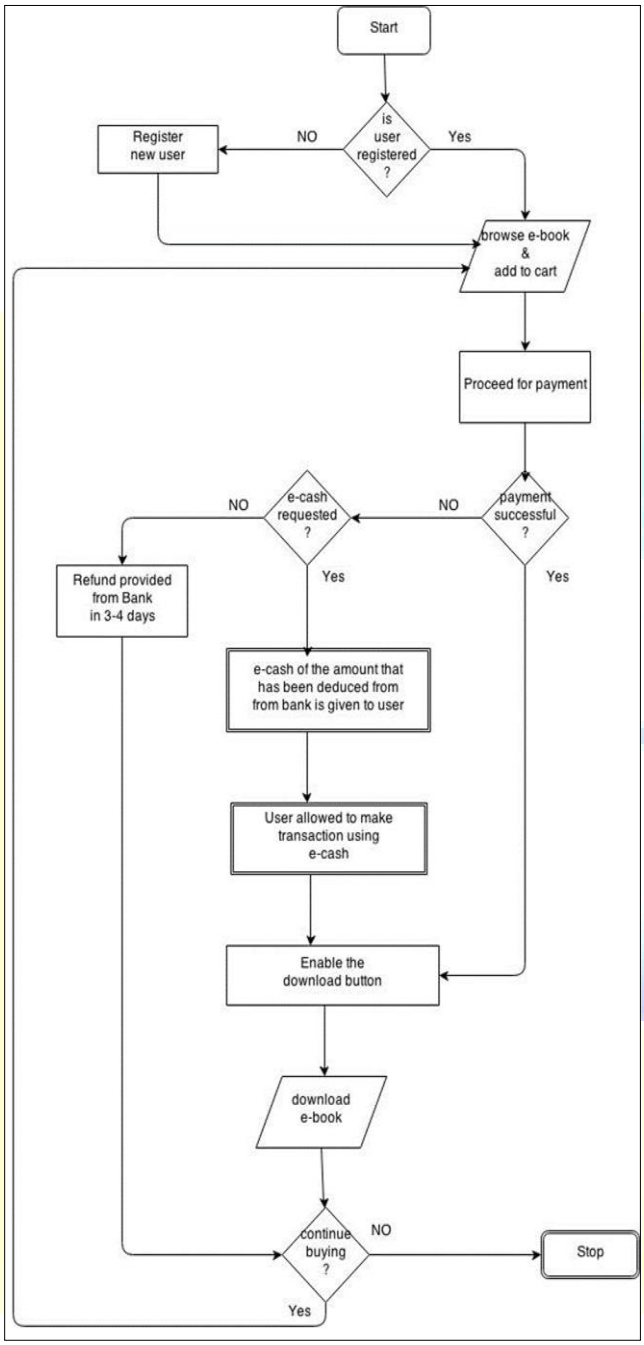

Fig. 1. Flowchart for the online e-book store

Once a user visits a site he/she is given option to login in case of registered user or else register. Once this is successful e-book is selected and added to cart. Now it proceeds for payment. In case payment is successful the download button is enabled and customer allowed to download e-book.

However if payment is unsuccessful and user requests for e-cash then e-cash of the amount debited is given. Now user is allowed to purchase using e-cash and once this is successful the download button is enabled for e-book download.

Once e-book is successfully downloaded, user is given option to either continue or exit. In case of continuation it is redirected to page to browse for further books else user exits.

B. Block Diagram

The entire system is divided into four blocks. Each block does processing in its own block and then passes this information to the next block. This helps to maintain concept of modularity thus increasing efficiency.

The four blocks are as follows:

1. E-book Buyer
2. Buyer's Bank Database
3. E-Book Store
4. Store's Bank Database

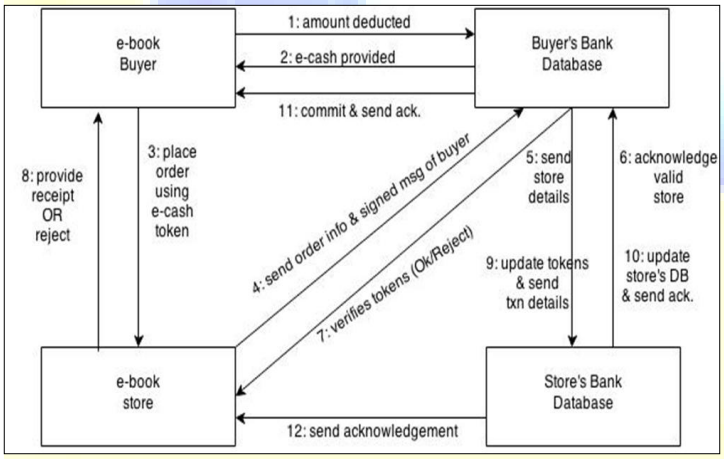

Fig. 2. Block Diagram for e-cash transaction using signcryption algorithm

1. E-Book Buyer

This block signifies the customer who is visiting the website. The buyer will first browse and select an e-book. Now when payment is initiated in case the payment has failed, the amount debited will be given as e-cash credit. After the entire transaction has been verified the e-cash is

debited from customer's bank and credited to merchant (e-book store) bank account. Then customer is allowed to download e-book.

2. Buyer's Bank Database

This block is used to provide e-cash for the amount debited. Further it also used to verify a given e-cash for double spending. Once verification is done this e-cash is transferred from buyer's bank to sender's bank and both databases updated accordingly.

3. E-Book Store

This block provides a platform for buyer to browse for website. Later once a transaction is initiated through e-cash it is used to pass message between buyer's bank and receiver (merchant's) bank account. Once e-cash is verified the e-book store receives the e-cash, databases are updated and then user is allowed to download e-book.

4. Store's Bank Database

This database keeps track of all e-cash received by the merchant. Once transaction is initiated, e-cash debited from buyer's bank is credited to store's database. Once e-cash is received by store's bank, acknowledgement is sent to e-store which will then enable download for user.

C.Algorithm for Signcryption

Step 1: Start

Step 2: Customer pays amount to bank

Step 3: Token will be generated by bank as

TI=TOKENID+SEQNO.+CUSTID+TS+VALUE+PROPS

Where

TOKENID: Unique identification number of a token;

SEQNO: Unique sequence number for each transaction;

CUSTID: Customer identification number;

TS: Time stamp of a transaction;

VALUE: Monetary value;

PROPS: other information;

Step 4: Signcrypted Token Information is generated in the form of (c,h,s,v)

Step 5: Calculation of (c,h,s,v)

a. Compute encryption key K as $K = f(TI)x_B \bmod p$, where f is a one-way function that maps from $\{0,1\}*$ to $Z*q$ & [p,q are large prime numbers]

b. Compute $c = E_K(TI)$, where E is a symmetric-key encryption algorithm.

c. Compute $v = f(TI)$

d. Choose randomly $r \in Z*p$

e. Compute $e = f(y_u r \bmod p, c)$

f. Compute $h = K \cdot e \bmod q$

g. Compute $s = r(h+x_B)^{-1} \bmod q$

Step 6: Verification of (c,h,s,v) by customer

a. Compute $e = f((y_B \cdot g^h)s.x_u \bmod p, c)$

b. Compute $K = h \cdot e^{-1} \bmod q$

c. Compute $TI = D_K(c)$, where D is a symmetric-key decryption algorithm.

d. Compute $v_c = f(TI)$ C verifies whether $v_c = v$.

If true, C accepts the token as valid else rejects.

Step 7: On purchase, Step 5 & 6 will be executed with respect to customer & merchant

Step 8: Merchant will now send request to Issuer Bank for verification, Step 5 & 6 will be executed with respect to merchant & IB

Step 9: After verifying that both customer and merchant are authentic IB sends OK signal to merchant.

Step 10: Merchant on receipt of an OK signal sends a receipt for items to C.

Step 11: IB updates the following in the token

SEQNO. = next SEQNO.

VALUE =VALUE − price.

TS =current TS

Step 12: IB updates Merchant's account by

balance = balance + price.

Step 13: IB commits the updating in token as well as in database.

V. CONSTRAINTS

Although online e-cash can be used to purchase any goods or services, it is not extended to the implementation of offline e-cash [3] transactions. Banks have to maintain large databases for storing the coins series number. [2] Also, since a single protocol is currently being used there is high overhead.

VI. CONCLUSION

In the various papers cited we analyzed how information in the e-cash network is disseminated in order to synchronize the databases. The reliance on various isolated blocks not only delays the clearing of transactions, but it also poses a threat to the network itself. Therefore a single protocol (signcryption) is used to propagate information to all the blocks involved. This helps to maintain consistency of respective databases and reduces possibility of double spending.

We through our proposed solution will able to integrate this signcryption algorithm along with conversion of failed amount in any transaction to e-cash. This shall help to create a robust payment gateway which shall be hybrid of both e-cash as well as regular banking transaction. Also it shall have safeguards to be protected in case of double spending attack using e-cash.

Future work shall include using techniques to enhance the network infrastructure for the hardware aspect so as to decrease response time of system. As single protocol is currently being

used there is high overhead. Using both these concept it is possible to develop a fool-proof system which shall be able to prevent hackers from breaking through the system or causing instances of double spending and also achieve user satisfaction as any transaction that has failed is immediately available as e-cash for immediate spending.

ACKNOWLEDGMENT

The authors would like to thank Ms. Bidisha Roy, Head of Department-CMPN, and professors of the department who have given valuable feedback which has helped to further improvise our report.

REFERENCES

[1] Arpita Mazumdar and Debasis Giri, "On-line Electronic Payment System using signcryption". International Conference on Communication, Computing and Security [ICCCS-2012].

[2] Debasis Giri and Arpita Mazumdar, "A Secure Off-line Electronic Payment System Based on Bilinear Pairings and Signcryption". International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January, 2013.

[3] Chun-I Fan and Vincent Shi-Ming Huang, "Provably Secure Integrated On/Off-Line Electronic Cash for Flexible and Efficient Payment". IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews, Vol. 40, No. 5, September 2010.

[4] Anand, R. Sai & C E Veni Madhavan. 2000. Online Transferable Ecash Payment System. INDOCRYPT 2000.

[5] Public key principles, one-way functions, RSA from: http://www.icg.isy.liu.se/courses/tsit03/forelasningar/cryptolecture06.pdf

[6] Mattias Eriksson, An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions from: http://www8.cs.umu.se/education/examina/Rapporter/MattiasEriksson.pdf