

A lightweight two-gateway based payment protocol with dynamic identity

Project report submitted in partial fulfillment

of the requirements for the degree of

Bachelor of Technology

in

Computer Science and Engineering

by

Ritesh Dash

(Roll Number: 116CS0178)

based on research carried out

under the supervision of

Prof. Sujata Mohanty



December, 2019

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Abstract

In the current world scenario, the number of mobile users are growing gradually and so is the number of people using e-commerce through mobile devices. Now majority of mobile payments are done through a single payment gateway. If a customer wishes to use two bank accounts, she has to transfer the funds into single account first, before being able to pay to the online merchant. And this will become a time consuming process. This paper is based on making the payment via two gateways for a single transaction, which is a more convenient option for the customer. Required standards such as accountability, anonymity and atomicity will be met in coming time.

Keywords: Accountability . Anonymity . Payment protocol . Payment gateway

Contents

Abstract	ii
List of Figures	iv
List of Tables	1
1 Introduction	1
2 Related Works	3
2.1 Public Key Encryption based protocols	3
2.2 Symmetric Key Encryption based protocols	3
3 Motivation and Objective	5
3.1 Motivation	5
3.2 Objective	5
4 Implementation	6
5 Results	7
5.1 Single Gateway Payment Protocol	7
5.2 2-Gateway Payment Protocol	8
6 Conclusion	9
References	10

List of Figures

1.1	Payment protocol involving Customer, Merchant, Payment gateway, Acquirer, Issuer	2
5.1	Response after a successful transaction on Customer-Merchant side for single gateway protocol	7
5.2	Response after a successful transaction on Payment Gateway side for single gateway protocol	7
5.3	Response after a successful transaction on Customer-Merchant side for 2-gateway protocol.	8
5.4	Response after a successful transaction on Payment Gateway side for 2-gateway protocol.	8

Chapter 1

Introduction

The fact that online shopping is growing at a higher rate seems to be the case right now. People using e-commerce sites as well as those who go for digital goods are behind this rapid increase. Digital goods refer to items that are produced, stored and consumed in electronic form. Portable devices like mobile smartphones, ipads, tablets are becoming popular, but the point is they have less storage as well as less computational capabilities as compared to desktop computers. They cannot efficiently perform high computational operations such as public-key encryptions. Secondly, wireless networks have less bandwidth and reliability, and higher latency. Furthermore, the connection cost to wireless networks is considerably higher.

Therefore it is not advisable to go for Public Key Encryption based protocol for lightweight mobile devices. Rather, Symmetric Encryption based protocols should be used, since they have lightweight operations involved. Symmetric Encryption uses the same key for encryption as well as decryption, so they are much faster. But there is a trade-off involved in using Symmetric Encryption, the Symmetric Encryption is less secure as compared to the PKI. Because a single key is involved and the key needs to be sent in a secure channel.

A payment protocol has to meet certain properties, Accountability being one of them. Accountability is the ability to trace an action between parties engaging in payment protocol and then hold them responsible for their transactions. Without accountability, a payment protocol may lead to disputes, so one cannot use this protocol with an untrusted party. Customer Anonymity is another important property, which can be satisfied through unlinkability and untraceability. Unlinkability refers to the fact that an unauthorised person or party cannot identify the customer and her bank account in the specific bank. Untraceability refers to the point that an attacker cannot trace a particular user from a group of customers. Going for a 2 payment gateway protocol demands that, the transaction should

rollback in case at least anyone gateway fails to complete the transaction, thus ensuring the Atomicity property.

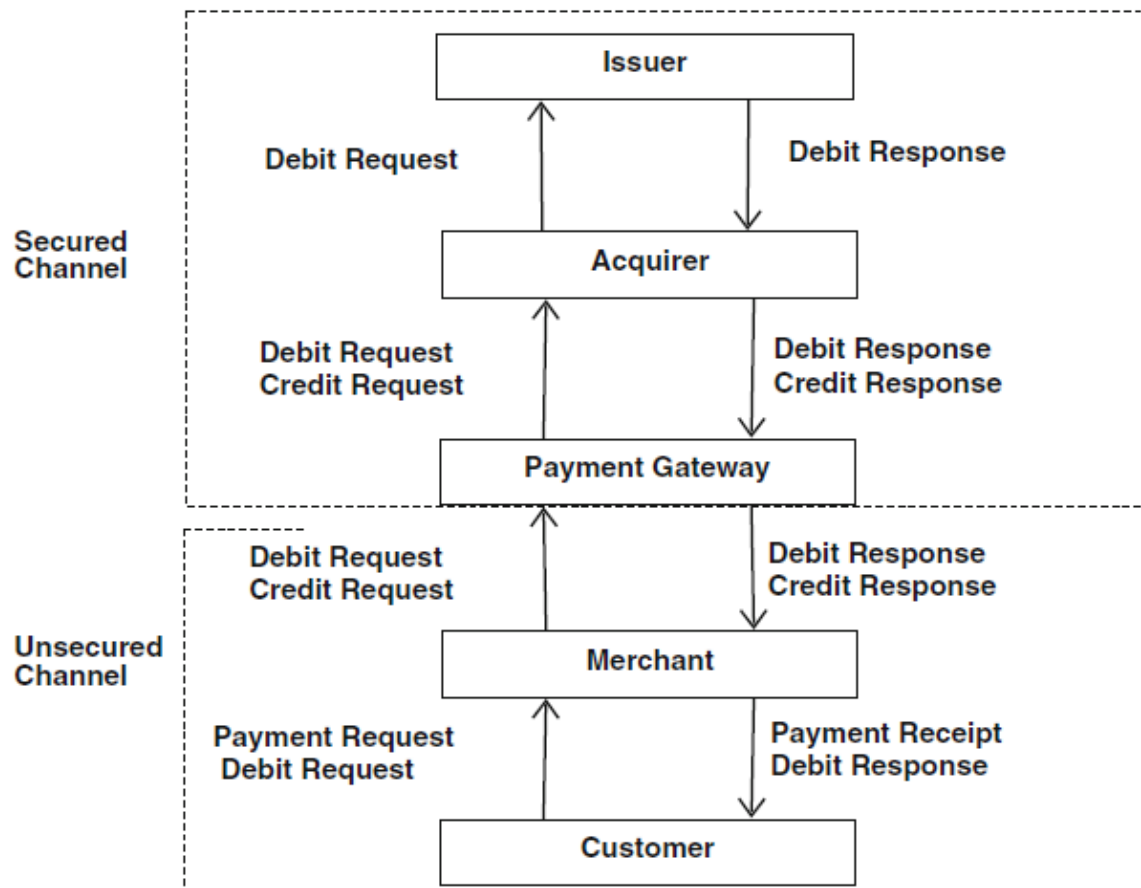


Figure 1.1: Payment protocol involving Customer, Merchant, Payment gateway, Acquirer, Issuer

As Fig 1.1 shows, the customer starts the payment initialisation, it sends the debit request to the merchant. The merchant then sends both the debit request and the credit request to the gateway. The gateway sends the same to the acquirer for conformation and the acquirer sends the debit request to the issuer to act upon. The issuer responds with the debit response and acquirer sends the debit response and the credit response to the gateway and subsequently to the merchant. The customer receives the debit response along with the payment receipt. Basically the payment gateway acts as an interface between the secured channel and the unsecured channel.

Chapter 2

Related Works

This section presents the protocols that I have gone through during the development of the project. These include both Public Key Encryption techniques as well as Symmetric Encryption techniques.

2.1 Public Key Encryption based protocols

The SET protocol [1] Is a popular online payment protocol using credit cards. This protocol requires all parties involved in the protocol to obtain public key certificates. The SET protocol has five phases, namely the initialization of transaction, purchase order, authorization, capture payment and card inquiry. In this protocol, the bank details of the client of payment are concealed from the seller and the purchase order data is shielded from the dealer.

Bellare et al. [2] proposed a family of protocols—iKP ($i = 1, 2, 3$) For secure online transaction through electronic means. Such protocols are based on public key cryptography. The protocols 1KP, 2KP and 3KP vary in how many entities have their own public key pairs. The security level relies explicitly on the number of parties that have the main pairs. iKP is dedicated to the client, retailer and transaction gateway.

2.2 Symmetric Key Encryption based protocols

Supakorn Kungpisdan et al. [3] introduced a secure payment protocol Using symmetric key cryptosystem, a secure payment protocol was introduced. At the time of the transaction, secret information (card numbers, PIN number, etc.) is not revealed in this process. The protocol consists of five entities, such as the client, merchant, issuer, acquirer and payment gateway. Customer requests subtraction of payment to the payment gateway in this protocol and the merchant requests payment claim to the payment gateway. The protocol is split into two sub-protocols, the protocol for merchant registration and the protocol for payment. The customer registers with the merchant and the payment protocol is executed to make the

payment during the merchant registration protocol.

Tan Soo et al. [4] introduced Mobile Network Operator (MNO) based lightweight payment protocol using symmetric keys for mobile environments which provides customer anonymity. The protocol consists of four parties, client, merchant, client's MNO, merchant's MNO. It consists of two phases, the registration phase and the payment phase. During the registration phase, the client sends the account information, its identity and the phone number after which the client and merchant set the Pin to generate the ID. The transaction is completed during the payment phase.

A Light Weight Two Gateway (LWTG) payment protocol has been proposed in [5] To make payment not only for one item using two cards from different banks, but also to use a dynamic ID to provide anonymity to the customer. In addition, the LWTG protocol overcomes the problems faced by existing protocols, which use the issuer bank's customer ID bulk posting mechanism to ensure anonymity. This protocol has four phases which include, payment agreement, two payment phases and finally the payment confirmation phase. There exists separate phases for payment through two gateways. The final phase handles the payment confirmation as well as generates the updated dynamic ID of the user at the end of every session.

The LWTG protocol is enhanced in [6] to satisfy the atomic property, Including correct sub-protocols and process of dedication. A nested transaction is developed where the original transaction is only committed if the two internal transactions are successfully committed. Otherwise, the entire nested transaction will roll back and the committed product can be used to resolve the issue of accountability. A fresh transaction for buying digital goods can also be started by the customer. The subprotocols include, a time based threshold which when exceeded will result in cancelling the transaction and rollback condition given that the commitment phase is not completed after both the transaction phases are completed successfully.

Chapter 3

Motivation and Objective

3.1 Motivation

Two Gateway payment protocols have a clear advantage over the single gateway payment protocols. Imagine a situation where a certain customer wishes to buy some goods from an online merchant, but the difficulty lies in the fact that none of his two cards have enough balance in them to pay for the items. Here comes the benefit of having a 2-gateway payment protocol, which can accept two cards and carry on the transaction using both the cards in the two gateways that are created.

3.2 Objective

With the motivation as outlined above, the objectives of my research work will be as follows,

- To implement a lightweight two gateway based payment protocol, that would satisfy all the properties of a secure protocol as accountability, atomicity and anonymity.
- To identify possible algorithms to improve the performance against existing payment gateways.

Chapter 4

Implementation

Implementation of a single gateway based payment protocol following the account based algorithm in [3] has been done. A sender receiver server pair has been set up using socket programming in python where the sender acts as the client-merchant side and the receiver acts as the payment gateway. After the user inputs the order amount and agrees the continue, the sender side asks the card details to both the client and the merchant. The information is then sent to the receiver which verifies the existing bank accounts and asks the user, the PIN. If entered correctly, the transaction goes through successfully and required info is displayed else a message showing unsuccessful transaction is shown.

The 2-gateway payment protocol is implemented in Python using socket programming concept. A customer-merchant server and a payment gateway server is set up, which will interact to complete the transaction. The process starts when the user enters the required items it wishes to buy from the merchant's website. The merchant then returns the total payable amount to the user, and the User can terminate the process if it decides to do so.

If the user wishes to continue, the user is asked to enter it's bank account number which will be encrypted before it is sent to the payment gateway for the transaction. The user-merchant server checks if the User has enough balance to pay for the items else it asks the User to enter another bank account if it wishes to continue the transaction. After the User enters the second bank account number, both the account numbers are merged to form a string and the string is encrypted before it is sent to the Payment gateway server.

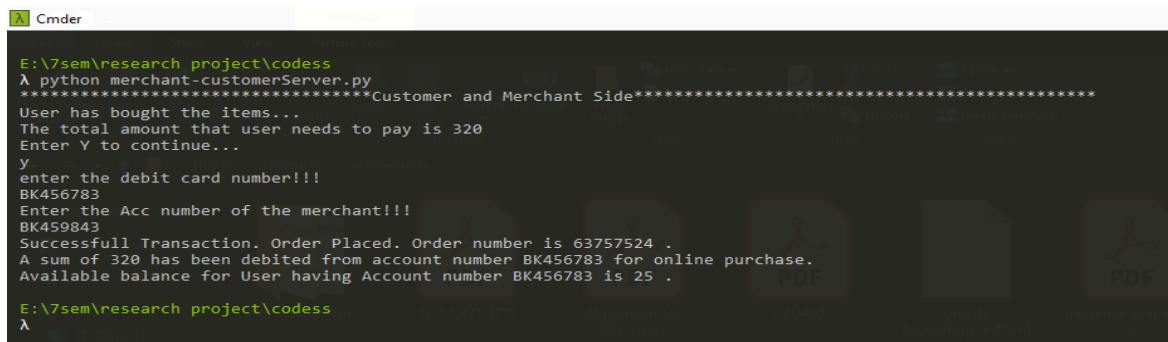
After receiving the encrypted string the, gateway decrypts the string and asks the PIN to the User. Given that the user enters the correct PIN for both the accounts, the transaction is processed, otherwise the transaction is cancelled and the User is given an error message. After the transaction is successfully completed, the User receives a message regarding the amount deducted from each account along with the order receipt.

Chapter 5

Results

5.1 Single Gateway Payment Protocol

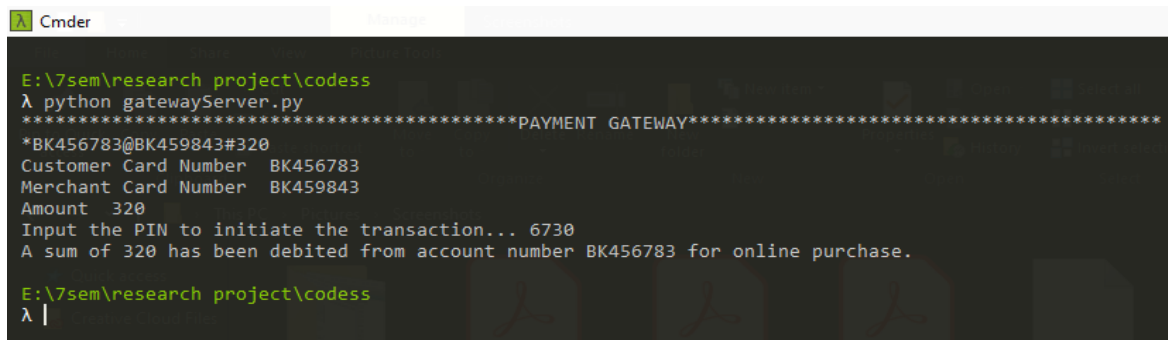
For implementing the single gateway protocol, the final amount is entered first which is followed by User bank account details. The user then switches windows to move to the gateway window where he is required to enter the bank account PIN number. The process's output can be observed below.



```
E:\7sem\research project\codess
λ python merchant-customerServer.py
*****Customer and Merchant Side*****
User has bought the items...
The total amount that user needs to pay is 320
Enter Y to continue...
y
Enter the debit card number!!!
BK456783
Enter the Acc number of the merchant!!!
BK459843
Successfull Transaction. Order Placed. Order number is 63757524 .
A sum of 320 has been debited from account number BK456783 for online purchase.
Available balance for User having Account number BK456783 is 25 .

E:\7sem\research project\codess
λ
```

Figure 5.1: Response after a successful transaction on Customer-Merchant side for single gateway protocol



```
E:\7sem\research project\codess
λ python gatewayServer.py
*****PAYMENT GATEWAY*****
*BK456783@BK459843#320
Customer Card Number BK456783
Merchant Card Number BK459843
Amount 320
Input the PIN to initiate the transaction... 6730
A sum of 320 has been debited from account number BK456783 for online purchase.

E:\7sem\research project\codess
λ |
```

Figure 5.2: Response after a successful transaction on Payment Gateway side for single gateway protocol

5.2 2-Gateway Payment Protocol

To start the 2-gateway payment protocol, the user enters the final payable amount and proceeds to enter the bank account details followed by the second bank account details, which is when he is redirected to the gateway window where he enters the PIN for both the accounts. The transaction is successfully completed and the user receives the payment confirmation and order receipt .All the above steps can be observed from the below attached output for the protocol.

```
E:\7sem\research project\codess
λ python merchant-customerServer.py
*****Customer and Merchant Side*****
User has bought the items...
The total amount that user needs to pay is 700
Enter Y to continue...
Y
Enter the debit card number of the User...
BK456783
In-Sufficient balance
Press 1 to enter another bank account and continue the transaction else to cancel the transaction...
1
Enter the second debit card number...
BK635485
Enter the Acc number of the merchant...
BK459843
b'gAAAAABd4kVzMKcPh8s6cmv2Fun8SQzbYpMvI1NUMZugu-Lc6uEpMjQ0a2hQZl00Zyr2ln8UCh8zbaN8NyxAKmLLlM2DlQa5KE08v0rKoS24kjFz8wEuHyY='
Successful Transaction. Order Placed. Order number is 27884119 .
Available balance for Account number BK456783 is 143 .
Available balance for Account number BK635485 is 142 .
E:\7sem\research project\codess
λ |
```

Figure 5.3: Response after a successful transaction on Customer-Merchant side for 2-gateway protocol.

The Payment Gateway window ask for the PIN for both the bank accounts to the user, after which it processes the transaction. After the transaction is processed, the debit response is displayed.

```
E:\7sem\research project\codess
λ python gatewayServer.py
*****PAYMENT GATEWAY*****
*BK456783BK635485@BK459843#700
Customer Card Number BK456783
Merchant Card Number BK459843
Amount 700
Enter the PIN for account number BK***783
*
*
*
Enter the PIN for the account BK***485
*
*
*
Processing.....
A sum of 202 has been debited from account number BK456783 for online purchase.
A sum of 498 has been debited from account number BK635485 for online purchase.
E:\7sem\research project\codess
λ |
```

Figure 5.4: Response after a successful transaction on Payment Gateway side for 2-gateway protocol.

Chapter 6

Conclusion

The number of people using electronic mobile devices for online payments is increasing day by day. With increasing use, we need to look for better ways to make online payments convenient and efficient. Coming into convenience, implementing the 2-gateway payment protocol provides greater convenience as compared to the more commonly used single gateway payment protocol. Not only does it allow users to use more than one bank account to complete a payment but also is efficient enough to carry on both transactions in lesser time as compared to the more traditional way of transferring money to a single bank account and then completing the transaction.

I look forward to implement DNA encryption in place of currently used AES encryption to ensure efficiency and security. More over validation of the above implemented payment protocol will be done using the widely accepted AVISPA tool along with a formal and informal security analysis using BAN Logic will be done. I look forward to complete all the above in the future period.

References

- [1] SET Secure Electronic Transaction Specification, Book 3: Formal Protocol Definition. SET Secure Electron Trans LLC; 1997.
- [2] Bellare M , Garay J , Hauser R , Herzberg A , Krawczyk H , Steiner M , et al. Design, implementation, and deployment of the ikp secure electronic payment system. IEEE J Selected Areas Commun (2000);18(4):611–27 .
- [3] Kungpisdan S , Srinivasan B , Le PD . A secure account-based mobile payment protocol. In: International conference on information technology: coding and computing. ITCC 2004, 1. IEEE; (2004). p. 35–9 .
- [4] Fun TS , Beng LY , Likoh J , Roslan R . A lightweight and private mobile payment protocol by using mobile network operator. In: International conference on computer and communication engineering. ICCCE 2008. IEEE; (2008). p. 162–6 .
- [5] Sureshkumar V , Anitha R , Rajamanickam N . Hash based two gateway payment protocol ensuring accountability with dynamic id-verifier for digital goods providers. In: International conference on computational models, cyber security and computational intelligence. Springer; (2015). p. 369–84 .
- [6] Sureshkumar, V., Anitha, R., Rajamanickam, N., Amin, R. A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity. Computers & Electrical Engineering.(2017). p .223-240 .