

# **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***



October, 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

<b>Abstract</b>	<b>ii</b>
<b>List of Figures</b>	<b>iv</b>
<b>List of Tables</b>	<b>1</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Literature Review</b>	<b>3</b>
2.1 Public Key Encryption based protocols . . . . .	3
2.2 Symmetric Key Encryption based protocols . . . . .	3
<b>3 Motivation and Objective</b>	<b>5</b>
3.1 Motivation . . . . .	5
3.2 Objective . . . . .	5
<b>4 Work done so far</b>	<b>6</b>
<b>References</b>	<b>7</b>

# List of Figures

1.1	Payment protocol involving Customer, Merchant, Payment gateway, Acquirer, Issuer . . . . .	2
4.1	Response after a successfull transaction on Customer-Merchant side. . . . .	6
4.2	Response after a successfull transaction on payment gateway side. . . . .	6

# 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 incase atleast anyone gateway fails to complete the transaction, thus ensuring the Atomicity property.

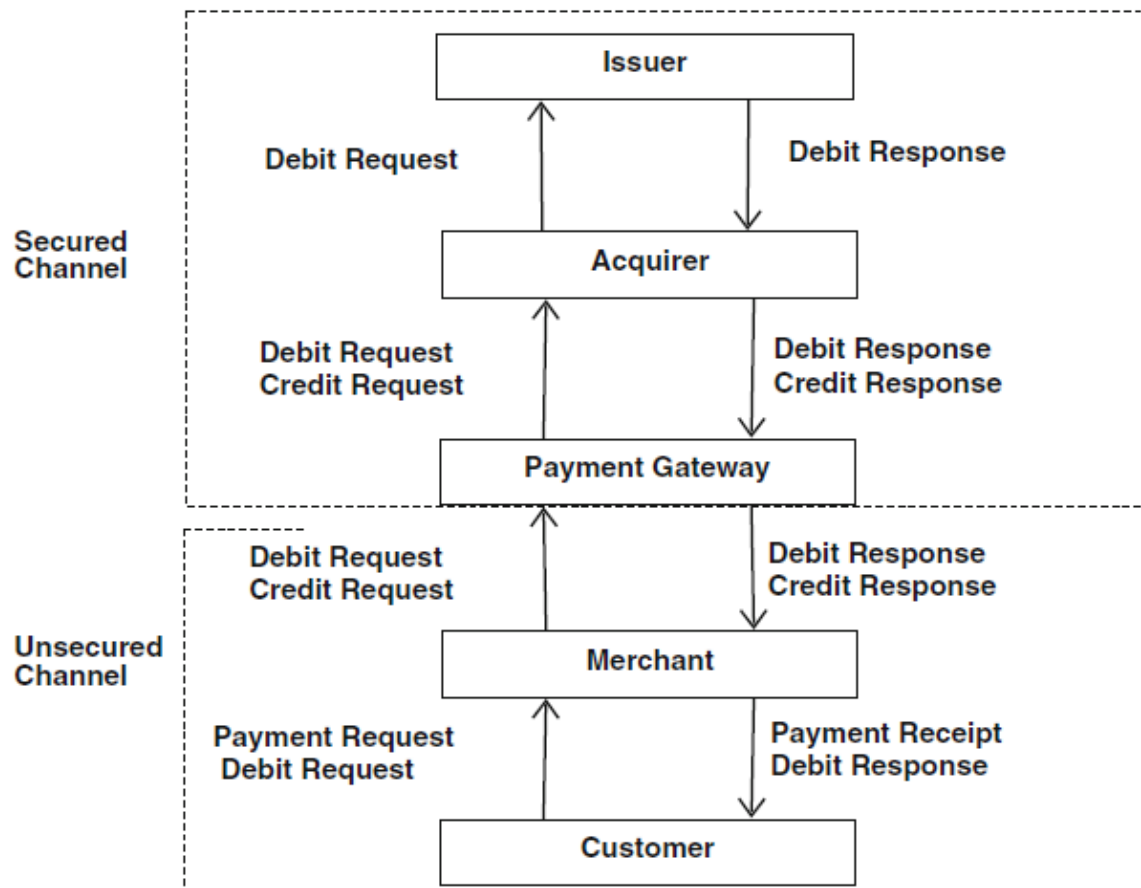


Figure 1.1: Payment protocol involving Customer, Merchant, Payment gateway, Acquirer, Issuer

## **Chapter 2**

# **Literature Review**

This section presents some of the existing payment protocols, and briefs their working mechanisms. 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 protocol for online payment using credit cards. This protocol requires the public key certificates of all the parties engaged in the protocol. The SET protocol has five phases namely payment initialization, purchase order, authorization, capture payment and card inquiry. In this protocol, the customer's bank details for payment are hidden from the merchant and purchase order information are hidden from the bank.

Bellare et al. [2] proposed a family of protocols—iKP ( $i = 1, 2, 3$ ) for secure electronic payment over the internet. These protocols are designed on the basis of public key cryptography. The 1KP, 2KP and 3KP protocols differ in the aspect of the number of parties having their own public key pairs. The level of security directly depends on the number of parties possessing the key pairs. The engaging parties of iKP are customer, merchant and payment gateway.

### **2.2 Symmetric Key Encryption based protocols**

Supakorn Kungpisdan et al. [3] introduced a secure payment protocol using symmetric key cryptosystem. In this protocol, the secret information (card details, PIN number, etc.) are not disclosed at the time of transaction. The protocol consists of five entities such as client, merchant, issuer, acquirer and payment gateway. In this protocol, client requests payment subtraction to the payment gateway and the merchant requests payment claim to the payment gateway. The protocol is divided into two sub-protocols, Merchant registration protocol and the payment protocol. During the merchant registration protocol, the client registers to the merchant and the payment protocol is executed to make the payment.

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] for not only making payment for a single item using two cards from different banks, but also for using a dynamic ID to provide customer anonymity. Further, the LWTG protocol overcomes the issues faced by the existing protocols, which use the mechanism of bulk posting of the customers ID from the issuer bank 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, by including suitable subprotocols and commitment phase. A nested transaction is developed where the original transaction commits only if the two inner transactions are committed successfully. Otherwise, the whole nested transaction rolls back and the committed product can be used to resolve accountability issue. The customer can also start a fresh transaction for buying digital goods. 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. Let us consider a situation in which a customer uses two different bank cards for the online payment. If the total cost of the product is more than the balance in a single bank, then the customer tends to use the second card also to make the payment. In this case, the customer is unable to make the payment through the single gateway based payment system. This scenario requires an efficient payment protocol for the online payment system, where the customer can pay the required amount through two gateways.

### **3.2 Objective**

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

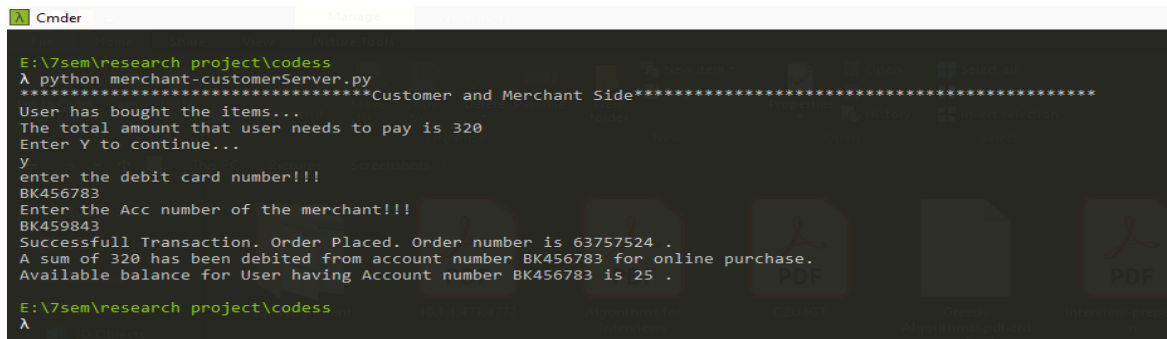
- To implement a lightweight two gateway based payment protocol, which would satisfy accountability, anonymity and atomicity.
- To identify possible algorithms to improve the performance against existing payment gateways.

## Chapter 4

### Work done so far

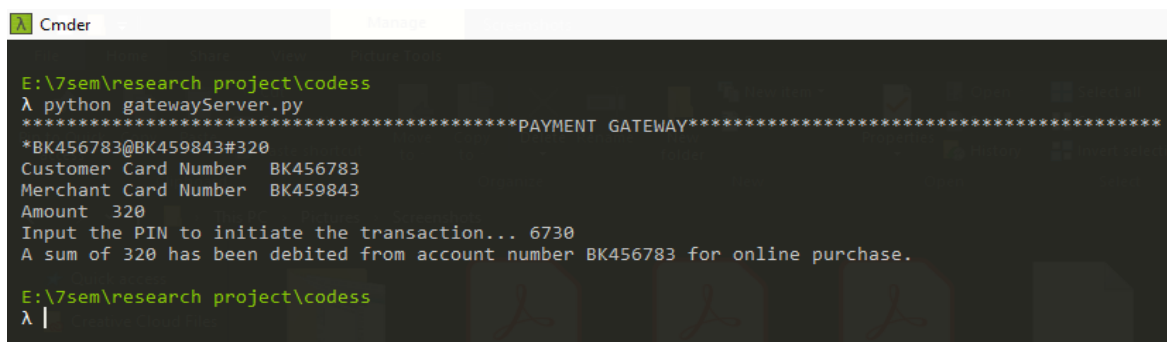
Implementation of a single gateway based payment protocol following the account based algorithm in [3] has been done.

A sender receiver 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.



```
Cmder
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 4.1: Response after a successfull transaction on Customer-Merchant side.



```
Cmder
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 4.2: Response after a successfull transaction on payment gateway side.

# 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 .