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

March, 2020

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 convinient 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

List of Figures

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 atacker 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.

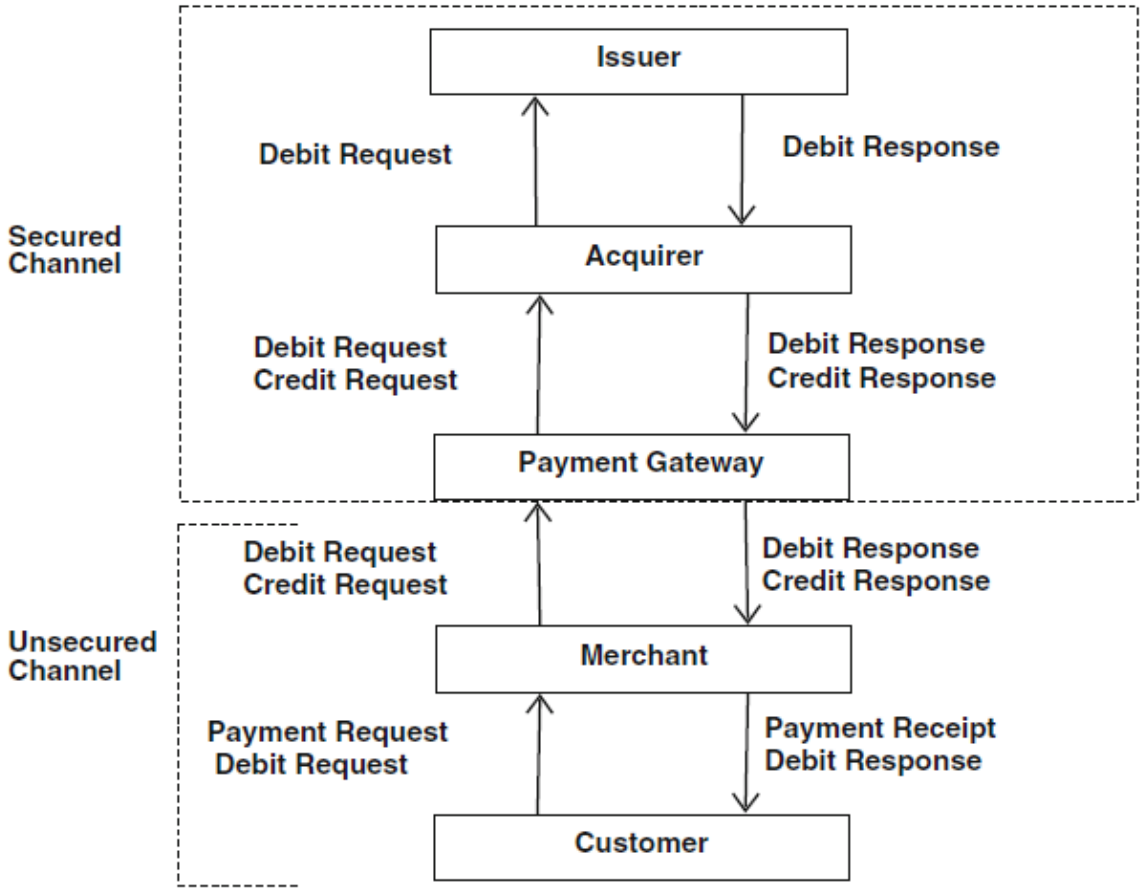

Figure 1.1: Payment protocol involving Customer, Merchant, Payment gateway, Acquirer, Issuer

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

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, it's 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

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. In our case, the payable amount is entered by the user for better convenience.

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 along with the order amount 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

The single gateway payment protocol has the following features,

- The gateway prefers a single gateway in case the first bank account does not have enough balance but the second card has enough balance.
- If the required orderAmount is greater than a threshold amount, the gateway breaks into several chunks before each chunk is transferred into the merchant's account.

Considering the case, where there is enough balance in the first bank account. After the bank details are entered, the gateway proceeds to ask for the PIN, and if the PIN is entered correctly, the transaction goes through successfully.

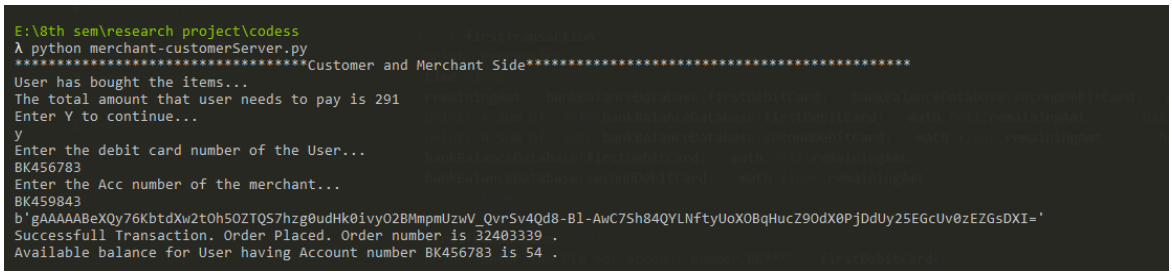

Figure 5.1: Response after a successful transaction on Customer-Merchant side for single gateway protocol when first account has required balance

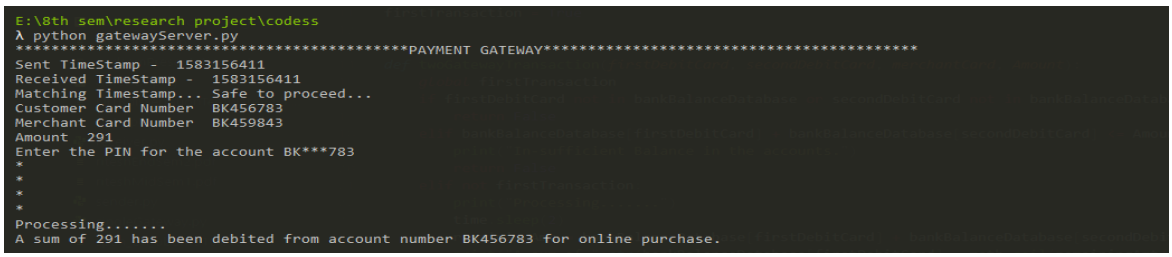

Figure 5.2: Response after a successful transaction on Gateway side for single gateway protocol when first account has required balance

Consider the next case, when the first bank account does not have required balance but the second bank account has the required balance. It would be inefficient if we carry on a 2-gateway payment even though a bank account has enough balance. The gateway proceeds to ask for the PIN, and if entered correct, the transaction is completed successfully.

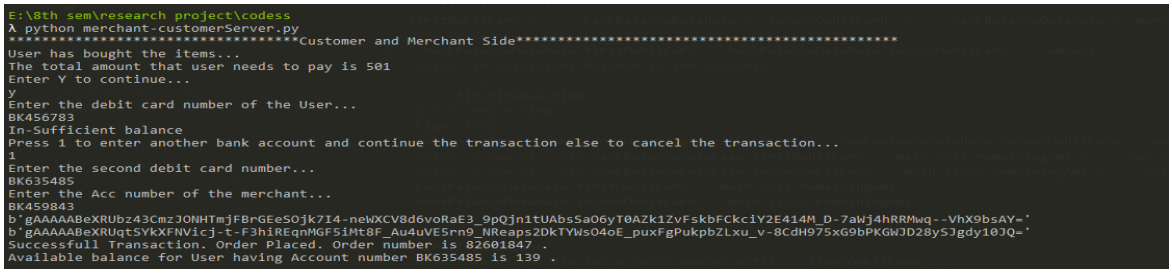

Figure 5.3: Response after a successful transaction on Customer-Merchant side for single gateway protocol when second account has required balance

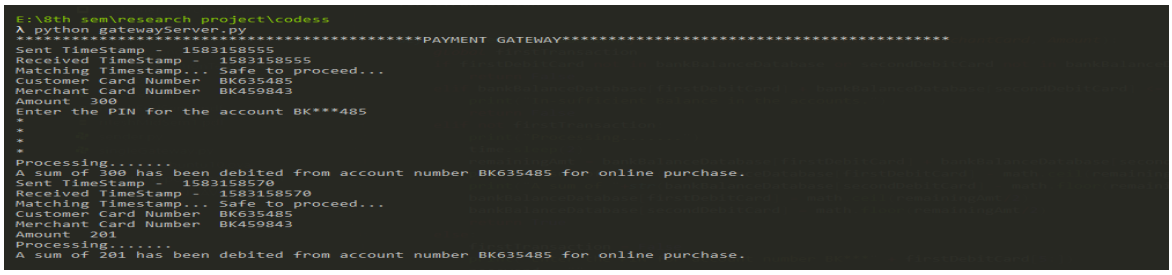

Figure 5.4: Response after a successful transaction on Gateway side for single gateway protocol when second account has required balance

5.2 2-Gateway Payment Protocol

The 2-gateway payment protocol has the following features,

- Checks if first account has enough balance, and then proceeds to ask for another bank account.
- Money is deducted from each account in such way, that neither get zero balance by the transaction.
- If orderAmount is greater than threshold amount, the orderAmount is broken down to chunks and the transfer is done, for elevate security.
- Once the customer enters the PIN for the first chunk, he doesn't need to enter the PIN for subsequent chunk transfers.
- Time-Stamp is attached with the string that the gateway receives, so as to compare the time the string is sent with the time it is received.

To start the 2-gateway payment protocol, the user enters the orderAmount 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 after dividing the orderAmount into chunks if the orderAmount is greater than fixed threshold 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

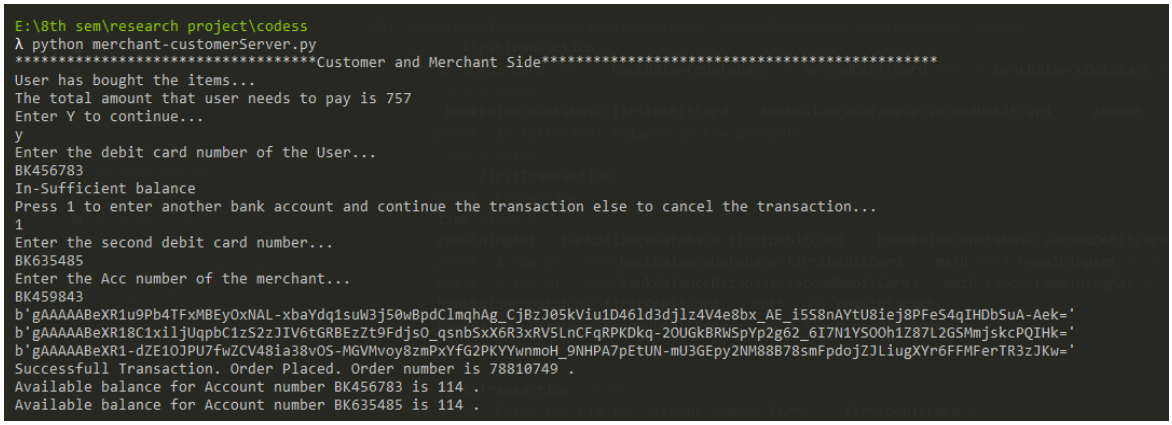

Figure 5.5: Response after a successful transaction on Customer-Merchant side for 2-gateway protocol

Below, the response of the gateway server can be seen, for a successful transaction.

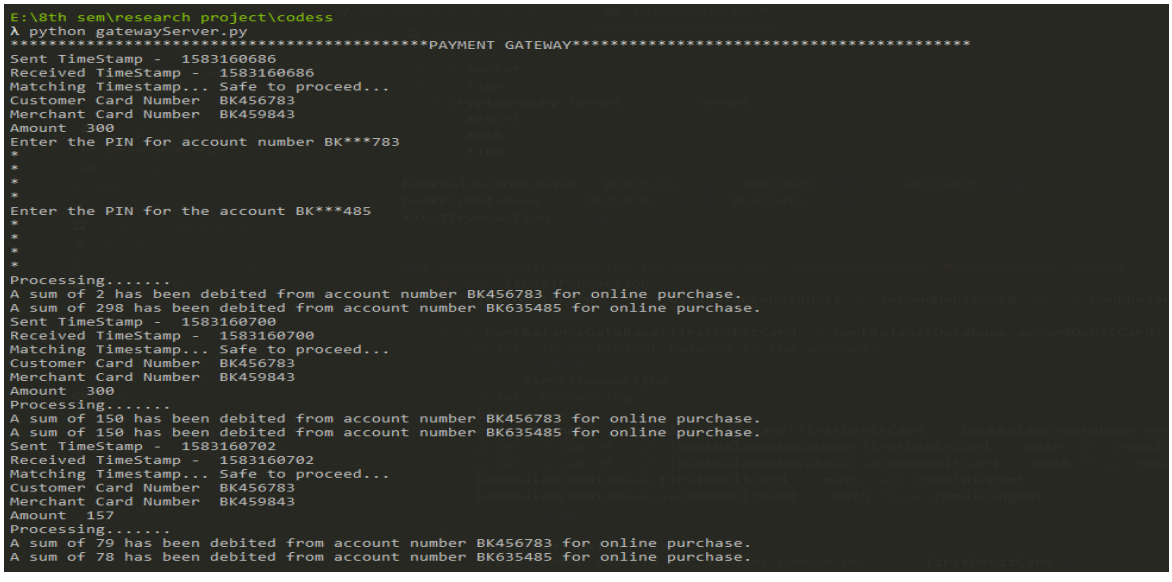

Figure 5.6: Response after a successful transaction on Gateway side for 2-gateway protocol

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 as well as secure. Coming into convenience, implementing the2-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. Breaking up the larger amount to chunks, makes sure the whole amount is not lost even if the attacker steals the information during a transaction, thus making the protocol relatively more secure.

I look forward to implement DNA encryption in place of currently used AES encryption to ensure efficiency and security. Moreover, the customer details need to be stored in a database, so that the project is easily scalable when the customer count increases.

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 .