Ritesh_ka_swag

by Akshat Jaiswal

Submission date: 24-May-2020 05:04PM (UTC+0530)
Submission ID: 1330865366
File name: ight_Weight_2-Gateway_Payment_Protocol_with_Dynamic_Identity.pdf (610.22K)
Word count: 4651
Character count: 25105

A Lightweight Two-gateway based Payment Protocol with Dynamic Identity

Ritesh Dash

Department of Computer Science and Engineering
National Institute of Technology Rourkela

A Lightweight Two-gateway based Payment Protocol with Dynamic Identity

Thesis 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

May, 2020

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Prof. Sujata Mohanty
Associate Professor

May 27, 2020

Supervisor's Certificate

This is to certify that the work presented in the thesis entitled ''*A Lightweight Two-gateway based Payment Protocol with Dynamic Identity*'' submitted by *Ritesh Dash*, Roll Number 116CS0178, is a record of original research carried out by him under my supervision and guidance in partial fulfillment of the requirements of the degree of *Bachelor of Technology* in *Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

_____
Sujata Mohanty

Dedication

This project is dedicated to all those people who have helped us in different stages of life. We're thankful to our teachers, friends and family who supported us during the tenure of this project.

Signature

Declaration of Originality

We, *Ritesh Dash*, Roll Number *116CS0178* hereby declare that this thesis entitled ''*A Lightweight Two-gateway based Payment Protocol with Dynamic Identity*'' presents our original work carried out as a undergraduate student of NIT Rourkela and, to the best of my knowledge, contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of NIT Rourkela or any other institution. Any contribution made to this research by others, with whom I have worked at NIT Rourkela or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged under the sections ''Reference'' or ''Bibliography''. I have also submitted my original research records to the scrutiny committee for evaluation of my dissertation.

I am fully aware that in case of any non-compliance detected in future, the Senate of NIT Rourkela may withdraw the degree awarded to me on the basis of the present dissertation.

May 27, 2020
NIT Rourkela

Ritesh Dash

Acknowledgment

I would like to show my sincere gratitude to my guide Prof. Sujata Mohanty for the constant support in my study and research, for her endurance, motivation, interest,and immense knowledge. Her supervision assisted me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my final year research project.

May 25, 2020
NIT Rourkela

Ritesh Dash
Roll Number: 116CS0178

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

List of Tables

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.

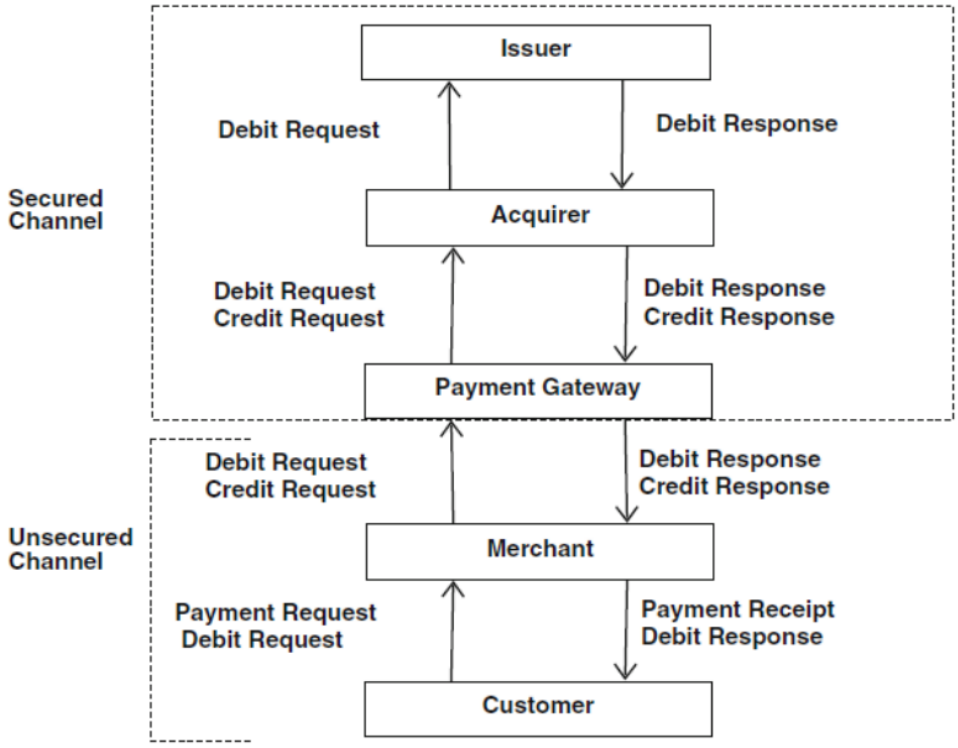

Figure 1.1: Payment protocol involving Customer, Merchant, Payment gateway, Acquirer, Issuer

As Fig 1.1 Supakorn Kungpisdan et al. [3] 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.

1.1 Related Work

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.

1.1.1 Public Key Encryption based protocols

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.

1.1.2 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.

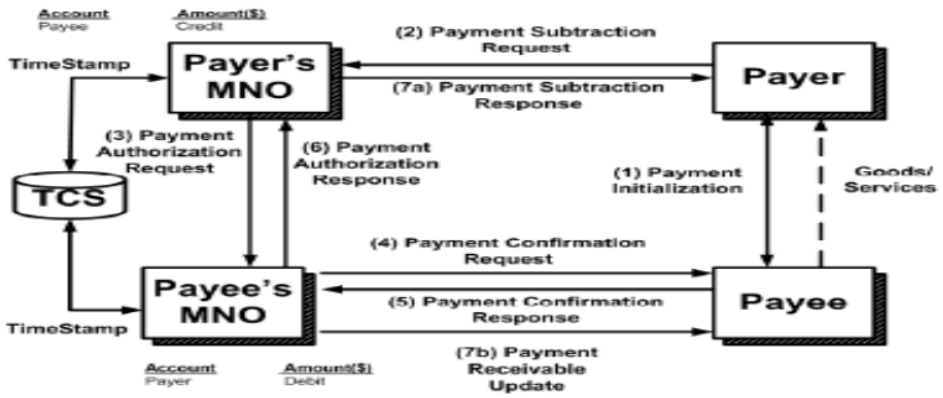

Figure 1.2: Payment Protocol involving Mobile Network Operator

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 as shown is Fig 1.2 . 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]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.

LWTG protocol is enhanced in [6] to satisfy the atomic property, Including correct

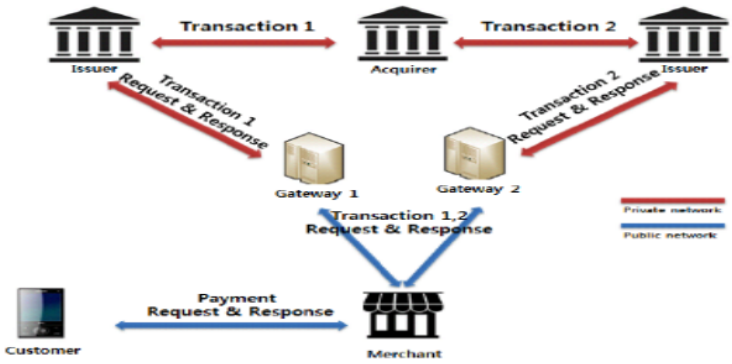

Figure 1.3: A 2 gateway payment protocol

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.

1.2 Motivation and Objective

1.2.1 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.

1.2.2 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 2

Proposed two-gateway based payment protocol

In this section, the protocol is explained and the implementation of the same is also explained. The major components of the protocol are, the customer, the merchant, the issuer and the acquirer. The issuer wants to have a debit request that is to be agreed by the customer and the acquirer desires to get the amount. Both of these are fulfilled in the gateway server of our implementation.The whole protocol can be divided into 3 phases,

- Initialisation of payment transaction
- Payment through gateway G1
- Payment through gateway G2

2.1 Proposed Protocol

Implementation of the 2-gateway 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. The transaction begins, once the customer enters the order amount and enters it's card details. The merchant is also allowed to enter the card details, to receive the order amount. The process moves to the gateway where the customer is required to enter the PIN and the transaction takes place given that the entered PIN is correct otherwise a message showing unsuccessful transaction is displayed to the customer, who can initiate the transaction again.

The various notations used in the phase description can be found in Table 2.1.

Table 2.1: List of Notations

Notation	Description
M	Merchant
C	Customer
G1	Gateway 1
G2	Gateway2
OD	Order Description
amt	Amount

2.1.1 Phase 1 - Payment agreement

As shown in Fig 2.1, 2-gateway payment protocol is initiated when the C enters the required items it wishes to buy from the M's website. The merchant then returns the total payable amount amt to the customer, and the customer can terminate the process if it decides to do so. In the protocol, the payable amount is entered by the customer for better convenience.In case the customer wishes to continue, the customer 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 customer-merchant server checks if the customer has enough balance to pay for the items else it asks the customer to enter another bank account if it wishes to continue the transaction. After the customer enters the second bank account number, both the account numbers are merged along with the order amount to form a string.

For added security, a new feature is implemented which lets the payment gateway

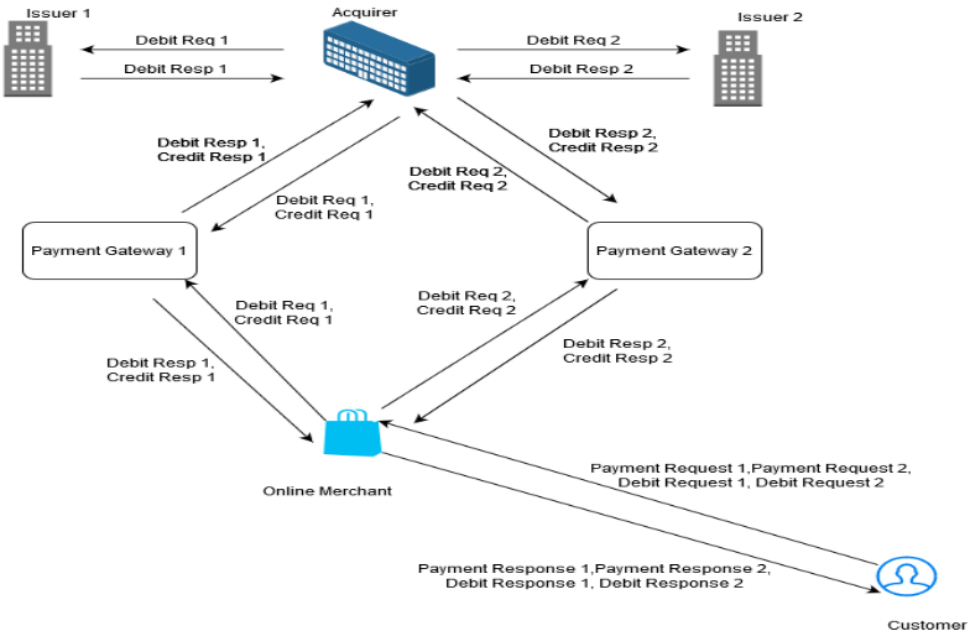

Figure 2.1: Payment using 2 Gateways

regulate the maximum amount that can be transferred in a single transaction. In case the amount is lesser than the set limit, the transaction is completed in one go. If the amount is greater than the set limit, the amount is broken down to chunks and the encrypted strings containing bank information and the amount are sent required number of times to the payment gateway server using UDP socket.

2.1.2 Phase 2 - Payment through G1

After receiving the encrypted string the, gateway decrypts the string and asks the PIN to the customer. Given that the customer enters the correct PIN for both the first account, the transaction in G1 is processed, otherwise the transaction is cancelled and the customer is given an error message. After the transaction is successfully completed, we move to the next phase.

2.1.3 Phase 3 - Payment through G2

Both the gateways are assumed to be blocks, rather than separate server programs to reduce complexity. The customer is asked the PIN for the second bank account and if correct PIN is entered, the whole transaction goes through. The customer receives an OD with an order number and a message indicating a successful transaction.

2.2 Assumptions considered for the protocol

The assumptions of the lightweight 2 gateway payment protocol, whose implementation was explained above can be listed as follows,

- The customer browses through the merchant site and adds items to the cart and enters the final amount that is required to pay.
- The customer has already registered with both the banks before the transaction starts.
- The customer can initiate one transaction at a time. If the user decides to go for a new transaction, he must cancel the current transaction first, which will rollback.
- The 2 gateways are implemented as 2 separate blocks as opposed to 2 separate servers, each block is assumed to act a server to reduce complexity

Chapter 3

Analysis of Proposed Scheme

In this section, various properties of the implemented protocol are analysed as well the protocol is compared with a few existing payment protocols. This will show necessary advancements in the case of the implemented protocol.

3.1 Security Feature Analysis

This section lists various properties of the implemented protocol, which are deemed to be necessary in case of a payment protocol. Below analysis proves how various properties are present in the protocol.

3.1.1 Accountability

Accountability is the ability to prove that an action is associated with a unique principal or server. This helps the verifying party to identify which server was compromised during a faulty transaction. To make a particular server responsible, the generated messages or the logs have to be checked on the compromised server, and it needs to be proved that the messages are generated but are not sent from the other server.

Consider a case in which two servers S1 and S2 are interacting with each other. S1 receives all the messages that is sent from S2, we can say that S1 is compromised when a message 'm' is received by S1 but m is not generated by S2.

In the implemented protocol, the logs and the token can be used to held a server accountable for the failure of the transaction. After being held accountable, the transaction is cancelled and the process starts all over again where the customer card details and merchant card details will be asked. This way, accountability is provided by the protocol.

3.1.2 Mutual Authentication

Authentication on both sides, the merchant-customer side and the gateway side is referred to as Mutual Authentication. This is ensured by checking the tokens received by both the

servers, in case the token is a counterfeit one, the transaction is cancelled and is rolled back. If the tokens are genuine, the transaction is carried forward.

In this case a private string value is considered to be the token, which is present in both the servers beforehand. The token is concatenated to the encrypted string and sent,the data is decrypted at the destination server to check it's authenticity.

3.1.3 Anonymity

Anonymity refers to the fact that the customer remains unidentified during all points of the transaction. In the implemented protocol, the data sent to the gateway goes through an unsecured network, where data can be compromised. The data sent is an encrypted string comprising of the customer's card number, merchant's card number and the amount. Even if the data is comprised, the customer remains untraceable due to lack of data like name, address or contact number. Moreover since the PIN is asked only after the gateway is functional, the customer can stay allay without the fear of getting robbed.

3.1.4 Atomicity

Transaction taking place from two bank accounts are considered to be one, that is if one transaction fails, the whole transaction fails. To promote Atomicity, both the transactions are written in different blocks and a conditional statement is put to check if both went down successfully which will lead to an overall successful transaction, else if any one fails, the whole transaction is rolled back.

The deducted money is deposited in the appropriate bank account. To know how much amount is deducted from which account, the gateway server logs can be used and utilised for further transactions.

3.1.5 Fairness

The data that is sent from one server to another consists of either the bank account numbers and the payable amount or either the confirmation message saying if a transaction has been successful or it failed. No unnecessary data is sent which reflects the Fairness property of the protocol. Sending in vulnerable and unnecessary data like Customer name, address, contact number which are not required for completion of transaction violates the fairness of a protocol

3.2 Comparative Analysis

This section provides a comparison between the discussed light weight two gateway payment protocol and few existing protocol in the number of necessary properties satisfied.

Table 3.1: Comparative analysis of protocol features

Protocol	Accountability	Anonymity	2 Gateway	Infrastructure
Set[1]	Yes	No	No	PKI
iKP[2]	Yes	No	No	PKI
KSL[3]	Yes	Yes	No	SKI
MNOP[4]	Yes	No	No	SKI
KZO[7]	Yes	Yes	No	PKI
Our Protocol	Yes	Yes	Yes	SKI

In the above table, Table 3.1, PKI refers to Public Key Infrastructure while SKI refers to Symmetric Key Infrastructure. As the table shows, the lightweight two gateway protocol stands most advantageous over rest of the payment protocols.

Coming to the number of cryptographic calculations, the number of symmetric key encrptions/decryptions in the lightweight two gateway protocol is 6.While for the protocol suggested by Tan Soo et al.[4] has 11 symmetric key encrptions/decryptions, which is roughly the double as compared to the discussed implementation.

Chapter 4

Results of Implementation

4.1 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.

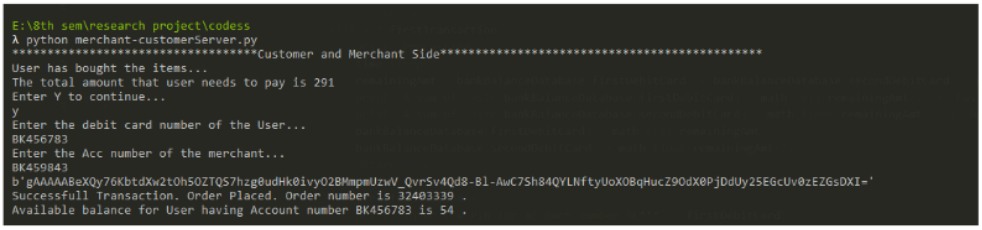

Figure 4.1: Response after a successful transaction on Customer-Merchant side for single gateway protocol when first account has required balance

Figure 4.2: 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.

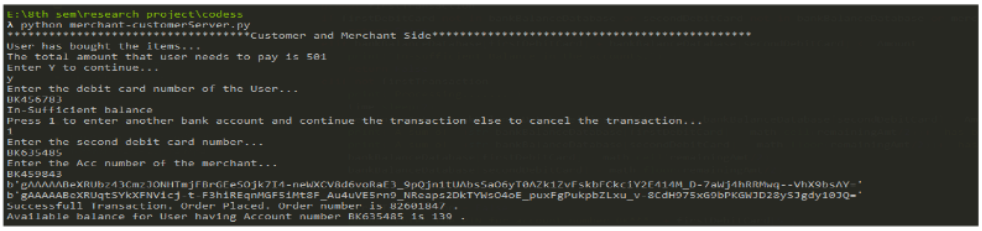

Figure 4.3: Response after a successful transaction on Customer-Merchant side for single gateway protocol when second account has required balance

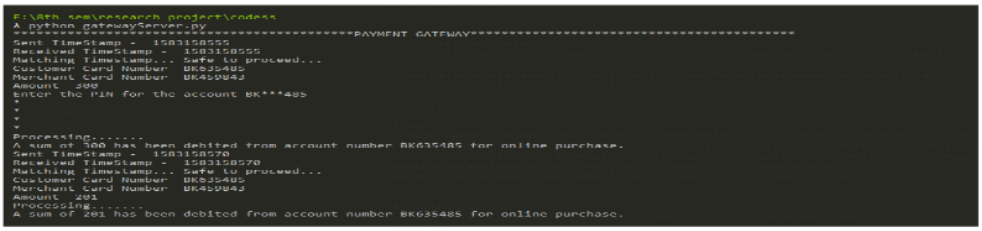

Figure 4.4: Response after a successful transaction on Gateway side for single gateway protocol when second account has required balance

4.2 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

```
E:\8th sem\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 757
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'gAAAAABeXR1u9Pb4TFxMBEyOxNAL-xbaYdq1suW3j50wBpdClmqhAg_CjBzJ05kViu1D46ld3djlz4V4e8bx_AE_i5S8nAYtU8iej8PFeS4qIHDbSuA-Aek='
b'gAAAAABeXR18C1xiljUqpbC1zS2zJIV6tGRBEzZt9FdjsO_qsnbSxX6R3xRV5LnCFqRPKDkq-2OUGkBRWSpYp2g62_6I7N1YSOOh1Z87L2GSMmjskcPQIHk='
b'gAAAAABeXR1-dZE1OJPU7fwZCV48ia38vOS-MGVMvoy8zmPxYfG2PKYYwnmoH_9NHPA7pEtUN-mU3GEpy2NM88B78smFpdojZJLiugXYr6FFMFerTR3zJKw='
Successfull Transaction. Order Placed. Order number is 78810749 .
Available balance for Account number BK456783 is 114 .
Available balance for Account number BK635485 is 114 .
```

Figure 4.5: 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 in Fig 4.6.

```
E:\8th sem\research project\codess
λ python gatewayServer.py
************************************PAYMENT GATEWAY*********************************************
Sent TimeStamp -  1583160686
Received TimeStamp -  1583160686
Matching Timestamp... Safe to proceed...
Customer Card Number  BK456783
Merchant Card Number  BK459843
Amount  800
Enter the PIN for account number BK***783
*
*
*
*
Enter the PIN for the account BK***485
*
*
*
*
Processing.......
A sum of 2 has been debited from account number BK456783 for online purchase.
A sum of 298 has been debited from account number BK635485 for online purchase.
Sent TimeStamp -  1583160700
Received TimeStamp -  1583160700
Matching Timestamp... Safe to proceed...
Customer Card Number  BK456783
Merchant Card Number  BK459843
Amount  300
Processing.......
A sum of 150 has been debited from account number BK456783 for online purchase.
A sum of 150 has been debited from account number BK635485 for online purchase.
Sent TimeStamp -  1583160702
Received TimeStamp -  1583160702
Matching Timestamp... Safe to proceed...
Customer Card Number  BK456783
Merchant Card Number  BK459843
Amount  157
Processing.......
A sum of 79 has been debited from account number BK456783 for online purchase.
A sum of 78 has been debited from account number BK635485 for online purchase.
```

Figure 4.6: Response after a successful transaction on Gateway side for 2-gateway protocol

Chapter 5

Conclusion

The number of people using electronic mobile devices for online payments is increasing day by day. With increasing use, better ways need to be explored to make online payments convenient and efficient. 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.

Scope for Further Research

The proposed algorithm will require necessary modifications if more than 2 gateways need to be involved. As a future work, the algorithm and the implementation can be modified such that they can involve as many number of gateways as the user wishes. That being said, there should be a maximum limit after which the whole transaction becomes vulnerable to attacks.

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 .

[7] Kyaw Zay Oo . Design and Implementation of Electronic Payment Gateway for Secure Online Payment System. International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 3 Issue 5, August 2019

Ritesh_ka_swag

ORIGINALITY REPORT

23%	16%	16%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ethesis.nitrkl.ac.in Internet Source	7%
2	Venkatasamy Sureshkumar, R. Anitha, N. Rajamanickam, Ruhul Amin. "A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity", Computers & Electrical Engineering, 2017 Publication	5%
3	archive.org Internet Source	4%
4	Sureshkumar, Venkatasamy, R. Anitha, N. Rajamanickam, and Ruhul Amin. "A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity", Computers & Electrical Engineering, 2016. Publication	1%
5	Submitted to University of Glasgow Student Paper	1%

6	Submitted to National Institute of Technology, Rourkela Student Paper	1%
7	www.ijecse.org Internet Source	1%
8	vdocuments.mx Internet Source	1%
9	Hakjun Lee, Jiye Kim, Jongho Moon, Dongwoo Kang, Dongho Won. "A Security Enhanced Lightweight Mobile Payment Scheme Based on Two Gateways", International Journal of Computer and Communication Engineering, 2017 Publication	<1%
10	Advances in Intelligent Systems and Computing, 2016. Publication	<1%
11	Submitted to Institute of Graduate Studies, UiTM Student Paper	<1%
12	Mourad Debbabi. "A Survey of Secure B2C Commerce for Multicast Services", 2006 Canadian Conference on Electrical and Computer Engineering, 05/2006 Publication	<1%
13	K. Rothermel. "Bringing confidence to the Web - combining the power of SET and reputation	<1%

systems", 2003 International Symposium on VLSI Technology Systems and Applications Proceedings of Technical Papers (IEEE Cat No 03TH8672) CCNC-04, 2004
Publication

14	www.netmode.ntua.gr Internet Source	<1%
15	fedetd.mis.nsysu.edu.tw Internet Source	<1%
16	Submitted to University of Stellenbosch, South Africa Student Paper	<1%
17	waseda.repo.nii.ac.jp Internet Source	<1%
18	waset.org Internet Source	<1%
19	www.anbousi.com Internet Source	<1%
20	www.scribd.com Internet Source	<1%
21	Chian Techapanupreeda, Roongroj Chokngamwong, Chalee Thammarat, Supakorn Kungpisdan. "An accountability model for Internet transactions", 2015 International Conference on Information Networking (ICOIN),	<1%

2015
Publication

22 Jesús Téllez Isaac, Sherali Zeadally. "Design, implementation, and performance analysis of a secure payment protocol in a payment gateway centric model", Computing, 2013 <1%
Publication

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		