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

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

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.Goods that are traded and used in digital form are called Digital goods. Portable devices like mobile smartphones, ipads, tablets are becoming popular, but the point is they have less storage. Besides having relatively less storage as compared to desktop systems, they have less processing power due to which they cannot handle public-key encryptions in the same way they can handle the symmetric key encryption. Being wireless in nature, the transmitted data is relatively less and higher latency is involved.

Hence 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 described as being held responsible for a particular event which is in this case, held responsible for a fraudulent transaction. Accountability, if not involved lets a huge flaw in a payment protocol. 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.

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