Efficient Method of Transaction Processing for Secure Mobile Bill Payments: Pay2S (Save&Safe)

Pensri Pukkasenung, Rajabhat Rajanagarindra University, Thailand

The Asian Conference on Sustainability, Energy & the Environment 2016
Official Conference Proceedings

Abstract
This paper proposed a new method for transaction processing of secure mobile bill payment. Focusing on the performance of the bill payment system which comparison between the transaction processing of new method and the trandition method. The transaction processing of tranditional method is single bill single transaction (SB-ST) and this method is multiple bills single transaction (MB-ST). Two dimensions of transaction processing method comparison were Save&Safe, (Save: memory usage , time usage, energy consumption and Safe: security: confidentialily, integrity, availability and non-repudiation). The peformance is testing on this paper by developed the Pay2S $^{(save\&safe)}$ application with Java on Android. The measure of save dimension are turnaround time, message size and cpu energy consumption. The security measure is analyze the message by using cryptography technique : encryption, decryption, Has function, and HMAC (Message Authentication Code). The environment for experimental consist of four parties : mobile client, intermediary, merchant, and payment service provider. All parties have a share secret key for exchange the message for protect the people who attack the system or replay attack. The result founded the performance of the new method get the better than the tranditional method and the seurity properties are same. So, the Pay2S (save&safe) application should development to the new business product for support the new lifestyle.

Keywords: Mobile bill Payment, Pay2S, Transaction Processing, Secure mobile Payment

Introduction

Nowadays, The mobile phone is one of the most important technological developments of our age. It has become the primary tool of people around the world for communication and business applications. The trend of global mobile phone usage increased from the year 2012 from 1.2 billion people to 4.5 billion people in 2018[2]. One of the applications that people use is a mobile payment (m-payment), which can pay for goods and services on mobile phone by using the prepaid or postpaid method. Currently, worldwide mobile payments are showing vigorous growth. Gartner, Inc., a leading research company, predicts that in 2016 there will be 448 million m-payment users, in a market worth $617 billion. The Asia/Pacific region will have the most m-payment users[3]. There are many applications from the payment service providers that were developed for supporting mobile payments including: issuer, card network and, mobile company. Examples of the application are Apple pay, LoopPay, Google Wallet, Paypal, Paypass, Dwallo, and Square Financial. However, most of the applications mentioned above use the traditional form transaction processing: one bill, one transaction. In the future, this may affect the performance potential of the mobile payment process.

The Research Framework

a) Mobile payment concept

In concept, the primitive mobile payment is composed of three basic steps. Payment: Client makes a payment to the merchant. Value Subtraction: lient requests to the payment gateway for his debit. Value Claim: Merchant requests to the payment gateway to credit transaction amount into his account.

b) Mobile Payment Framework of Pay2S (save&safe)

Mobile payment framework consists of Merchant, Customer and Counter Service. The processing of framework start at the merchant sent bills to the customer , then the customer using the mobile application (Pay2S (save&safe)) to pay for bill or using counter service. Currently, almost customer pay by counterservice. But now the authors design a new method for bill payment. It provided a high performance : low cost, low time, convenience, high security. The framework of mobile bill payment depict in Figure 1.

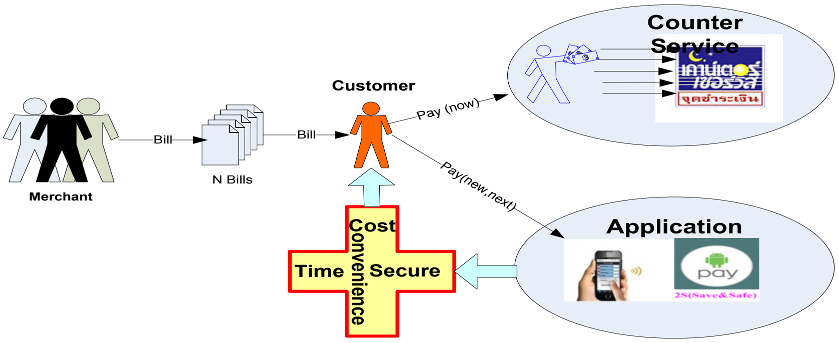

Figure 1: Pay2S (save&safe) Model

c) **Method of Secure Mobile bill Payment**

- Symmetric Key cryptography
- Symmetric Key + Shared Key
- Hash Function
- MAC
- HMAC

Transaction Processing Model

Transaction Processing Model consist of 2 type as belows:

a) Single Bill Single Transaction (SB-ST) : The system execute the transaction processing of one bill per one transaction.

b) Multiple Bills Single Transaction (MB-ST): The system excute the transaction processing many bills per one transaction depict Figure .

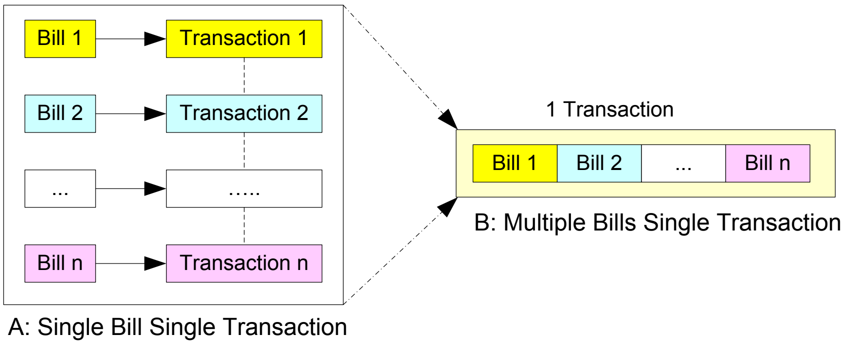

Figure 2 : Transaction Model

Security and Performance Issue

The proposed model ensure the security properties : CAIN. All messages that are transfers on network by using a cryptographic technique that consist of symmetric key cryptography, hashing. And provided a high performance

-The security properties of CAIN
-Confidientiality : Ensures that private or confidential information is not made available or disclosed to unauthorized individuals. Encryption technique using a symmetric key with secret key, hash function and hash function with MAC (Message A*uthentication* Code). These provided the desired properties.

- Authentication : Authentication: Ensures that the origin of a message is correctly identified, with an assurance that the identity is not false. Encryption technique using a symmetric key with hash function with MAC that provided authentication properties.

-Integrity : Ensures that only authorized parties are able to modify computer system assets and transmitted information. Encryption technique using a symmetric key with secret key and MAC, and hash function are provided in the properties.

-Non-Repudiation : Ensures that the user cannot deny that he/she has performed a transaction and he/she must provide proof if such a situation occurs. Encryption technique using a symmetric key with MAC is provided in the properties.

-Performance Analysis

In this view point we focus on three approaches to measure the performance of the mobile payment system . These consist of:

- Memory usage : The memory that is used for data processing at that time. It is measured in bytes.
- Time usage: The time it takes to process an application at that time. It is measured in millisecond (ms).
- Power consumption : The energy use in processing the application. It is measured in Millijoules (Mj) : 1 Mj = 3.6 Kwh (Kilowatt hour)

Experiments

The experiments were conducted on wireless network and fixed network for comparison of performance and security. TheArchitecture of the experiments depict Figure 3**.**

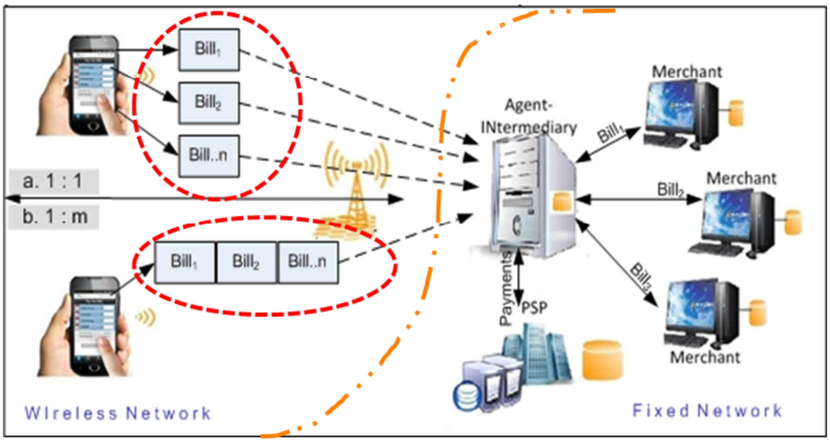

Figure 3: Architecture of the model

-Tools
This scenario uses many tools for testing the security and performance. These were designed for hardware, software requirement and function of the system.

-Hardware Requirment
Client: Samsung Galaxy S5 (CPU : 2.5 GHz Quad core, RAM 2 GB, Internal Storage 16 GB, OS : Android 4.4.2 (Kitkat)
Intermediary, Merchant, Payment Service Provider : HP Pavillion 23-g025x (CPU : Intel Core i5-4570T processor, 4M cach, up to 3.60 GHz), RAM 4 GB DDR3, Storage 1TB 7200 RPM, OS : Windows 7 Enterprise

-Software Requirement
Apache HTTP Server: HTTP Server for Web Services Deployment
PHP: Programming Lanugage for Web Services
Android SDK : Development Tools for Client Mobile Application
SQLite (Embedded with Android OS): Embedded Database for Client Mobile

-Application
MySQL : DBMS for Intermediary, M and PSP
C#: Programming Language for IN, M and PSP Application
Security Function in C# and Java and tool
GenerateAESkey(): Symmetric key algorithm (AES 128 bit)
AESEnc(): Hash Function (MD5)
AESDec(): Key-Hash Function (HMAC-MD5)
Power Tutor: Monitoring Power Consumption
DDMS: Monitoring Android Application
Wireshark: Testing the security properties

Results

From the experiments, we can conclude the results on the table I. The security properties of the two payment types provides confidentiality, authentication, Integrity and non-repudiation. The performance of the payment methods are base on transaction processing. We found that the one to one relationship payment has a time average of 31.50 (ms), memory usage is 1,414 bytes and CPU energy consumption is 262.13 Mj. The one to many relationship payment has a time average of 17.37 (ms), memory usage of 756 bytes and CPU energy consumption is 66.55 Mj.

In summary, overall performance of the one to many relationship delivers better performance than one to one relationship. That makes the new protocol suitable for a new era which uses mobile phones to support convenience, because it is high in performance and security.

Table I Result of Testing the Security and Performance

Tx : Bill	Security				Performance		
	C	A	I	N	Time Average (ms)	Memory Usage (byte)	CPU energy Consumption (mj)
1 : 1	Y	Y	Y	Y	31.50	1,213	162.13
1 : M	Y	Y	Y	Y	17.37	756	56.55

Tx : Transaction , ms :millisecond , mj : milli joule

From the results in Table II. we compare the security properties and performance between two types of transactions. The security properties tested by using the Wireshark program that decrypts message at the destination. This ensures confidentiality, authentication, integrity and non-repudiation of both types. The performance was tested by running the mobile application and monitoring by DSK program and Power Tutor. We tried to input a the different number of bills when testing the performance, such as time testing using fourteen bills per transaction, memory testing use three bills per transaction and CPU energy consumption using fourteen bills per transaction. As a result, we discovered that the performance of the proposed protocol delivers better performance than traditional transaction processing.

Discussion

The result of experiments shows the improved performance of a secure mobile bill payment application. The characteristics of model are lightweight platform, high security , memory conservation, less time consumption, and reduced cpu energy consumption. In accordance with the requirements of the 21st century, it also supports a change in the concept of the “Bill Gates”, which, in the latest Gate Notes annual letter, Microsoft founder and philanthropist Bill Gates writes about the effect smartphones and mobile banking will have in the next 15 years. He observed that “Digital banking will give the poor more control over their assets and help them transform their lives and, by 2030, 2-billion people who don’t have a bank account today will be storing money and making payment with their phones"[12].

In the real world we have many mobile payment applications such as Apple pay, LoopPay, Google Wallet, Paypal, Paypass, Dwallo, Square Financial, etc. These currently do not supporting multiple bill payment. In The future, we should adjust the mobile payment system to accommodate the needs of a new era.

Conclusion

This paper proposes experiments to measure the performance of mobile payment Applications***(Pay2S*** $^{(save\&safe\ )}$) , which are applied form a lightweight agent-base secure mobile payment protocol that supporting the multiple payment. We developed the application for testing security and performance. The security properties use an encryption technique that supports CAIN: confidentiality, authentication, integrity, and non-repudiation. The performance is tested by placing the application on the experimental design. Overall, the experiments revealed that the one to one relationship between transaction and number of bills provides far less performance than the one to many relationships. It should be develop into a the business product.

Reference

Fun, T. S., Beng, L. Y., Roslan, R. and Habeeb, H. S. (2008). Privacy in newmobile payment protocol, World Academy of Science, Engineering and Technology. Vol:2, pp. 198-202.

Kungpisdan, S., Srinivasan, B., Le, P. D. (2004). A secure Account-based Mobile Payment protocol , Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004) , available online at https://en.wikipedia.org/wiki/Mobile_payment

W., Stalling, "Cryptography and Network Security," Principles and Practice 6th Edition. 2013, Prentice Hall International, Inc.

Daniel O. R. et al., "Adaptive Query Algorithm for Location Oriented Applications" Roedunet International Conference (RoEduNet), 2013 th, Romania

10 of the hottest trends in consumer behavior in 2015. http://www.manager.co.th/Weekly54/ViewNews.aspx?NewsID=9560000157612&TabID=3&

https://mobiforge.com/research-analysis/global-mobile-statistics-2012-section-f-mobile-payment-nfc-m-commerce-m-ticketing-and-m-coupons