Computer Engineering and Applications Vol. 1, No. 1, June 2012

# Design of Prototype Payment Application System With Near Field Communication (NFC) Technology based on Android

Huda Ubaya

*Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya*
*Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Ilir, South Sumatra 30662*
*huda@unsri.ac.id*

## ABSTRAKSI

Sejak akhir tahun 1990-an, orang-orang telah menikmati gaya hidup yang nyaman. Perangkat *mobile* yang didukung oleh perkembangan jaringan nirkabel telah menyebar ke seluruh dunia. Orang-orang dapat memperoleh informasi, memesan tiket, mengunduh lagu dan melakukan transaksi komersial yang disebut *mobile commerce*. Aplikasi *mobile commerce* menjadi aplikasi yang paling digemari bagi para pengguna perangkat *mobile* yang menginginkan melakukan transaksi bisnis dan keuangan dengan mudah dan aman, kapan saja dan dimana saja mereka berada. Saat ini penggunaan uang tunai secara fisik sedang mengalami penurunan popularitas di dunia bisnis, karena mulai digantikan oleh pembayaran non-fisik yang sering disebut uang elektronik (*electronic money, e-money*). Sebuah teknologi penting di balik pembayaran *mobile* adalah *Near Field Communication* (NFC). Sebagai indikasi bahwa NFC mempunyai potensi bisnis yang luar biasa, perusahaan terkemuka seperti Nokia, Microsoft, Visa Inc. dan MasterCard Worldwide dan NXP Semiconductors, secara aktif terlibat menggarapnya. Proses pembayaran yang terintegrasi dengan teknologi NFC berbasis sistem operasi *mobile* yang sedang *trend* saat ini yaitu Android yang mendukung teknologi NFC yaitu versi 2.3.3 Gingerbread. Prototipe aplikasi bayar dirancang untuk 2 sisi pengguna yaitu pada sisi *user* sebagai konsumen dan pada sisi *merchant* sebagai pedagang/penjual dengan menggunakan *handset* yang sudah memiliki teknologi NFC yaitu Google Samsung Nexus S. Prototipe aplikasi bayar juga mengimplementasikan konsep keamanan dalam transaksi *e-commerce* dengan menggunakan protokol *Tag-to-Tag* sehingga kebutuhan pengguna untuk keamanan dan kenyamanan selama bertransaksi finansial terpenuhi.

**Kata Kunci:** Android, NFC, pembayaran, *mobile*, *Tag-to-Tag*, *e-money*

## ABSTRACT

Since the late 1990s, people have enjoyed a comfortable lifestyle. Mobile devices supported by the development of wireless networks have spread throughout the world. Mobile commerce applications become the most popular application for mobile device users who want to do business and financial transactions easily and securely, anytime and anywhere they are. Today the use of physical cash is experiencing a decline in popularity in the business world, because it is being replaced by electronic money (e-money). An important technology behind mobile payments is now called Near Field Communication (NFC). As an indication that the NFC has tremendous business potential, leading companies like Nokia, Microsoft,

Visa Inc., and MasterCard Worldwide and NXP Semiconductors, is actively engaged on them. Payment processing integrated with NFC technology based mobile operating system that is a trend today, Android. The prototype application is designed to pay for the user side as consumer and the merchant side as a trader or seller by using the handset that already have NFC technology is Google Samsung Nexus S. This application prototype also implements the concept of security in e-commerce transactions by using the protocol Tag-to-Tag so that the user needs for security and comfort during the financial transaction are met.

**Keywords**: Android, NFC, payment, mobile, Tag-to-Tag, e-money

## 1. INTRODUCTION

Since the early 2000's, wireless networks have been developed in Europe and Asia. Currently, the penetration rates of mobile devices in the countries reach 80-90%. Mobile commerce applications become the most popular application for mobile device users who want to do business and financial transactions easily and securely, anytime and anywhere they are.

Analysts predict there are three main regions for mobile payments is the Far East Asia and China, Western Europe and the United States, which as a whole will account for more than 70 percent of overall mobile payment in financial transactions in 2013 [1].

An important technology behind mobile payments is called Near Field Communication (NFC). As an indication that the NFC has tremendous business potential, leading companies such as Nokia, Microsoft, Visa Inc., And MasterCard Worldwide and NXP Semiconductors, actively engaged in the NFC Forum, a nonprofit group comprised of industry players both technical and non-technical-minded to make a standard NFC-based transactions.

In this thesis offers a prototype payment application using mobile phone device in which the technology is already integrated Near Field Communication (NFC). The discussion in this research focused on the security of NFC based communication when making the payment process between user and merchant. This study protocol implements Tag-to-Tag as NFC based communication security protocols. Testing is done by simulating the actual payment process by using 2 mobile devices Samsung Nexus S, each of which acts as a user and merchant.

## 2. MOBILE COMMERCE

Mobile commerce is the buying and selling of goods or services through wireless devices such as mobile phones, personal data assistants (PDAs), smart phones and handheld gaming devices. Mobile commerce is also described as any transaction with monetary value which conducted through mobile telecommunications networks. Mobile commerce using mobile devices to communicate interact and conduct transactions over mobile networks or wireless networks. Mobile commerce is all about the wireless e-commerce using mobile devices to conduct business on the internet. Mobile commerce is also defined as the exchange value or the purchase


ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

and sale of financial products, services or information on the internet using mobile devices. Mobile commerce according to Ericsson (http://www.ericsson.com) is the trusted transaction services through mobile devices to exchange goods and services between consumers, merchants and financial institutions. So during the transaction or transfer money to an intermediary mobile device, it can be categorized as mobile commerce. [2]

Mobile commerce seen globally is very helpful and very beneficial for users but also has its advantages and disadvantages. The advantages of mobile commerce are;

1. customer satisfaction, cost savings and new business opportunities,
2. transactions can be done anywhere and anytime,
3. owner has control over the data while the mobile device can be synchronized,
4. allow for considerable profit, and customer relations became closer.

## 3. MOBILE PAYMENT

Mobile payments [3][8][9][10] are also defined as the process of exchanging financial value between two entities using mobile devices to pay for a product or service. As depict in Figure 1, alternative payment options that consumers able to pay for products or services anywhere and anytime with the convenience of using mobile devices such as mobile phones, or smart phone. The system is designed to operate using wireless technology (wireless) such as Infrared, Bluetooth, Wi-Fi (802.11), WiMAX (802.16) and the latest technology that is Near Field Communication (NFC).

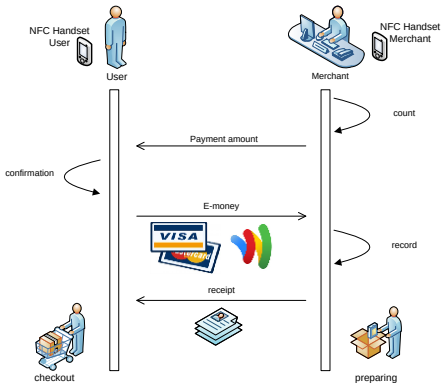


Figure 1. The process of paying

The main driving factor of mobile payments is the use of mobile phones are increasingly widespread and evenly, and the trend toward electronic money (digital cash). Mobile payments have three functions:

1. Enhance consumer convenience / user by providing the flexibility to use this service anytime and anywhere, or in other words, mobile payments provide an economical solution to save time and money.

2. Promoting competition opportunities in the payments market. Mobile payments offer new services to market and facilitate the payment of the effectiveness of using the payment system by introducing the concept of electronic money.
3. Offers new opportunities for mobile service providers and financial institutions in the mobile market with a variety of new and innovative business models.

## 4. NEAR FIELD COMMUNICATION (NFC)

Near Field Communication (NFC) [4][5] is a new wireless connectivity technologies to the radius of the short range, which evolved from the combination of contactless identification and interconnection technologies (RFID). NFC operates at a frequency of 13.56 MHz and has a data transfer rate of up to 424 Kbps. Effective communication and optimal between two NFC-enabled devices occurs when they are at a distance of 0 to 10 cm. Simple movement as twist or swing closer connections between devices can initiate NFC, which will also be compatible with Bluetooth or Wi-Fi (show in Figure 2).


Figure 2. NFC Technology

NFC technology is a combination between the smartcard and reader that is planted in a single device, such as mobile phones or smart phones. With the NFC device planted on a mobile device, then the transaction activities such as micro-payments or payment transactions can be done by juxtaposing it to the NFC reader, which is at the terminal point of sale (POS) at the location of the transaction. With a feature like this then NFC referred to as device that supports the contactless transaction.

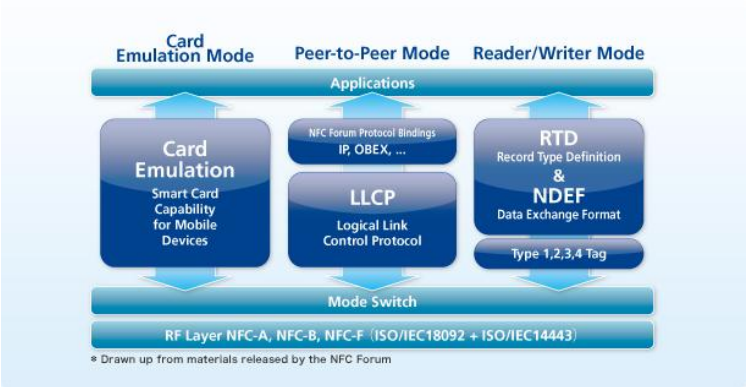


Figure 3. NFC operation modes


ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

As for some applications that can be developed using NFC technology are as follows.

1. Ticketing
   NFC can provide the ability for users to perform secure payment processing, shopping with electronic money, and can also make purchases, sales and electronic ticketing, such as music tickets, airline tickets, bus tickets and more.
2. Electronics key
   An example is the use of mobile phone as car keys, house keys or office keys.
3. Identification
   In addition, NFC can make things possible that your mobile phone will be used as identity documents.
4. Social networking
   Data stored on the tag objects such as a DVD box or poster can be accessed by mobile phone for example, to upload movie trailers, street maps, show schedules, comments about events and much more.
5. Set-up Service
   To avoid complex configuration process, NFC can be used to set up other wireless technologies like Bluetooth and wireless LAN.

## 5. ADVANCED ENCRYPTION SYSTEM (AES)

Encryption is a block cipher symmetric key cipher which operates on the length groups of bits are often called blocks with the same transformation. When a block cipher encryption process takes n-bit block of plaintext as input and outputs the same amount with the input n-bit block cipher as well as text. After the delivery process, the receiver section will perform the decryption process which in principle is similar to the encryption process at the sender (transmitter) is decryption algorithm will take the same n-block cipher with a secret key and produce original n-bit block of plain text. [6][7]

Rijndael supports key length of 128 bits to 256 bits with 32 bits step. Key length and block size can be selected independently. Because AES is determined that the block size must be 128 bits and key length should be 128, 192, and 256 bits, then known as AES-128, AES-192, AES-256.

A de-facto, there are only two variants of AES, namely AES-128 and AES-256, because the user will very rarely use 192-bit key length. Since AES has a key length of at least 128 bits, the AES resistant to exhaustive key search attack with current technology. With 128-bit key length, then there are 2,128 ≈ 3.4 x 1038 possible keys. If used a machine with one billion processors in parallel, each one can calculate a lock every one Pico second, it would take 1,010 years to try all possible keys also Rijndael operates in the orientation of bytes to allow for an efficient implementation of the algorithm into software and hardware.

## 6. ANDROID

Android [11][12] is an operating system developed by Google, which promises openness, affordability, open source, and quality framework, to meet the needs of the operating system that supports standard and publishing APIs and can be utilized as a whole with low cost.

Until now, Android has released several versions of Android to refine the previous version. Besides according numbering, on every version of Android there is a code name based on the names of the dessert. Android 1.5 released on 30 April 2009 was named Cupcake, Android 1.6 was released on 15 September 2009 was named Donut, and for the tablet version of Android 3.2 was released in May 2011 was named Honeycomb while for mobile Android phone last version 2.3.6 was released on September 2, 2011 with the name of Gingerbread with tech support for Near Field Communication (NFC).

Android's built-in on the Linux kernel (open Linux kernel), with a virtual machine that has been designed and to optimize use of memory and hardware resources on the mobile device environment of the Dalvik virtual machine. DalvikVM has the advantage of using the base processor registers because the device has been optimized for mobile phone-based execution registers.

The application has a life cycle (cycle) is initiated when the Android initialize the component to respond to the intent to complete when the instance is destroyed. Figure 4 shows the process life cycle of an Android application.


Figure 4. Android's lifecycle

## 7. TAG-TO-TAG PROTOCOL

For security during the payment [14] process takes place between the merchant and the user is required optimum safety. In this study used the AES algorithm with 128-bit key length is the author of the quite reliable, especially on mobile devices with limited computing resources. As for the design of security protocols of


ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

communication between the merchant and the user during the process of payment transactions take place depicted in Figure 5, which uses protocol Tag-to-Tag [13] with the following caption.

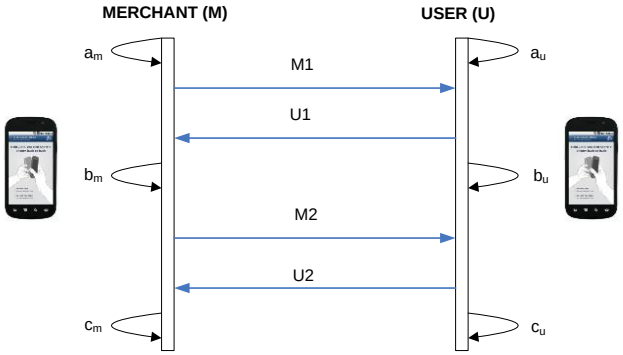


Figure 5. Tag-to-Tag Protocol

1. Starting from the process $a_m$ and $a_u$, merchant and user generate a session key shared (shared session key) that $K_{SM}$ and $K_{SU}$ are used in the process of encryption and decryption takes place during the payment process.
2. Merchant sends a message to the user that contains the ID number, transaction number, the payment amount, encrypted account number, authentication code, and the $K_{SM}$ key.
3. User sends a message to the merchant that contains the ID number, transaction number, balance, an encrypted account number and password, authentication code, and the $K_{SU}$ key.
4. In the process of $b_m$, merchant check the amount of payment and the balance position of the user. If AMOUNT <ACCBALANCE then the PAY_M value is 1 (ACCEPT, the payment is received). And if AMOUNT> ACCBALANCE then the value of PAY_M is 0 (REJECT, the payment is rejected).
5. In the process $b_u$, user checks the amount of payment and the balance position. If AMOUNT <ACCBALANCE then the PAY_M value is 1 (ACCEPT, the payment is received). And if AMOUNT> ACCBALANCE then the value of PAY_M is 0 (REJECT, the payment is rejected). Status of PAY_P validated by confirmation from the user by pressing the 'OK' or 'NO' on the screen.
6. Merchant sends a message to the user that contains the ID number, transaction number, payment amount, PAY_M, the encrypted account number, $MAC_M$, and $K_{SM}$.
7. Users send a message to the merchant that contains the ID number, transaction number, payment amount, PAY_P, account numbers and passwords are encrypted, $MAC_P$, and $K_{SP}$.
8. In the process of $c_m$, the merchant verifies the value of PAY_P. If PAY_P = 'ACCEPT' & PAY_M = 'ACCEPT' the payer payment of funds deposited on the merchant's account, transactions are recorded and printed receipts. In the $c_u$ process, the user verifies the value of PAY_M. If PAY_P =

'ACCEPT' & PAY_M = 'ACCEPT' balance payer then the position will be reduced and the status of the application recorded payment.

## 8. SYSTEM DESIGN

Basically the system consists of two applications, namely on the merchant's payment application and pay application on the user. Application on the user or called nBelanja can do some things that

1. nBelanja provide the login page to activate the security features for transactions took place with the merchant,
2. nBelanja receives payment data from nBayar from the merchant,
3. nBelanja provides features to better secure PIN transactions taking place between the user and the merchant,
4. see the balance on the user by setting the value of the maximum balance of Rp.1,000,000 (one Million Rupiahs) to the level of micro-payments,
5. transaction record, with this facility the user can do and see footage of payment transactions that have been made between the user and merchant.

Applications on the merchant or called nBayar there are several functions that can be done by merchant

1. payment, serves to provide payment data information that must be paid by the user, in this process occurs the connection / relationship between p2p users with a merchant to exchange information and confirmation with an encrypted channel,
2. records of transactions, recording transactions serve to see who has done between the merchant and the user which includes transaction time (day, date and hour), number of transactions and the amount paid by the user.

Users do pay process by juxtaposing their device into the merchant device. Then the user receives payment data that must be paid according to results of previous shopping process from the merchant via the communication peer-to-peer based NFC. After the user approve the payment and enter your PIN, if true then the application will check the balance on the user's position and if sufficient then it will be forwarded to the process of sending data to the merchant's payment confirmation via peer-to-peer NFC-based payment transactions and make the records

While in the merchant communicates with the user to transmit payment data information that must be paid users using peer-to-peer NFC-based channel that is encrypted in accordance with the security protocol in Section VII. Furthermore, the merchant awaiting confirmation of payment from the user through the same channel and after receiving confirmation, the application will record the transaction records in the database.

nBelanja special applications on the user added features of electronic money (e-money, virtual money) that will be created in the encrypted form of a special file that can only be accessed by the main database with encryption and decryption process-based AES 128 bits. Restrictions on the implementation process of designing and manufacturing in this research utilizing pure NFC technology available on the Samsung Nexus S.


ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

## 9. RESULTS AND DISCUSSION

In this test performed simulations of merchant payment processing to the user. The process of implementation and testing of applications on hardware made directly to the Google Samsung Nexus S in pairs. While testing performed, the running time of each activity on the application process can be seen using DDMS and log process data delivery process from the user to the merchant.

Table 1
Results of functional testing and processing time in the user

| Testing Activity | Result | |
|---|---|---|
| | **Success** | **Time (ms)** |
| NFCBelanjaActivity | √ | 389 |
| TopupActivity | √ | 431 |
| RekamActivity | √ | 356 |
| HistoryActivity | √ | 355 |
| P2PActivity | √ | 2,531 |
| SaldoActivity | √ | 257 |
| KonfirmasiActivity | √ | 405 |

From the test results as shown in Table 1 and 2 can be seen that in every activity does not require a long processing time less than 1 second except for P2PActivity. To process P2PActivity need longer time because it takes longer to process communication between 2 devices as well as encryption and decryption process, but not so influential because the time is only about 2,531 ms or equal to 2.5 s.

Table 2
Results of functional testing and processing time at the merchant

| **Testing *Activity*** | **Result** | |
|---|---|---|
| | **Success** | **Time (ms)** |
| NFCMerchantActivity | √ | 354 |
| HistoryActivity | √ | 282 |
| P2PActivity | √ | 2,523 |
| KonfirmasiActivity | √ | 544 |
| RekamActivity | √ | 343 |

In addition to functional testing and processing time on the activity carried out safety testing also performed by comparing the time required to perform encryption and decryption for processing load 1,000 times. Figure 6 and 7 show the results of safety testing for encryption and decryption respectively.

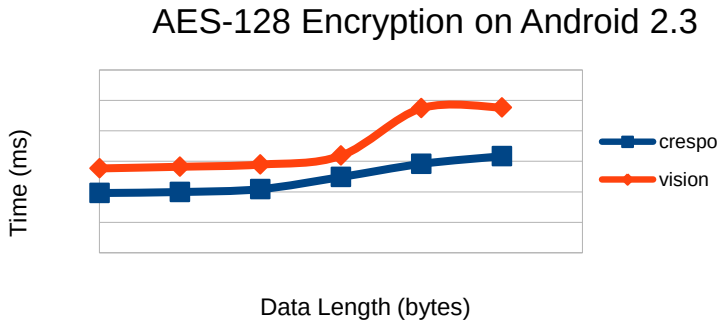


Figure 6. Comparison of the AES 128 bit encryption

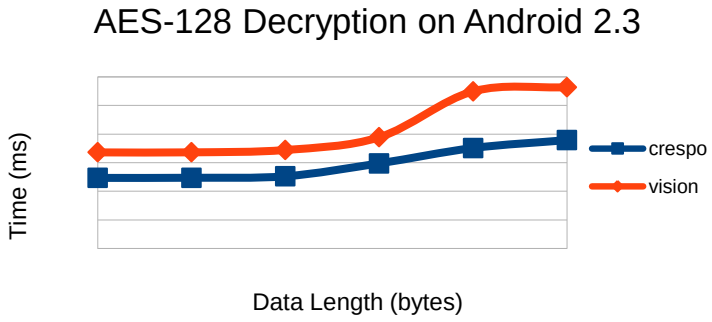


Figure 7. Comparison of 128-bit AES decryption time

Analysis of test results from both applications and hardware used to is already running well. Hardware test results are very good with the use of the handset that is designed specifically with NFC technology. Overall nBelanja applications for users and nBayar for merchants with design is not real but still in the form of simulation has been able to show workflow processes as in real conditions. But nevertheless still many shortcomings and the need for more in-depth study covers the following issues

1. The security level of the interaction between applications and security in accessing the electronic money (e-money),
2. The process going forward must be made client - server to better be able to control the system from the merchants and third-party security including authentication and centralized management and database management better,

## 10. CONCLUSSIONS AND FUTURE WORKS

Several conclusions can be drawn from this study are as follows.

1. Applications nBelanja and nBayar created as a model process payment with NFC technology that allows users to make the process pay by using mobile devices. Applications created with ease of understanding and designing made simple and adapted to process pay a more effective and user friendly making it easier for users to make the payment process. Application created a prototype


ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

that shaped the future still remains much to do development and improvement of existing models.

2. The database used is a SQLite database which is owned by the Android platform so that the process will be faster and less computing resources in the process of reading the database.
3. Application processing time is done not too long and still in the process tolerance limits, not more than 1 second while for communication and information exchange process P2P NFC about 2.5 seconds.

Future works of this study are:

1. Because this research is still a prototype or model of the actual process so that there are limitations to its use in real, then it is advisable in the future to be able to collaborate on NFC technology with the model client - server so that the process would be better. Combining the use SQLite databases and database servers like MySQL, Posgresql, or Oracle on the part of merchants enables the development process for the better, so that the merchants themselves can make the process better database management and more controlled.
2. Security process is still limited in the process of exchanging data / information from the user to the merchant through the device and need to be improved so that more secure from intrusion irresponsible for example by use of embedded device Secure Element as an important information storage medium
3. Further development is recommended to further involve a third party or third party such as Bank, Issuer or TSM (Trusted Service Management) so that the process of pay in this application is more real because of the process of authentication and verification process of such third party.

## REFERENCES


[1]. _____, _____, http://www.cellular-news.com/story/34222.php , Over 400m Mobile Ticketing Users by 2013, 20 Juni 2011, 08.15 WIB.

[2]. Ade Hendraputra, Arif Budiono, Bayu Erfianto, Wardani Muhammad (2009). *Aplikasi E-Commerce.* Politeknik Telkom Bandung, Indonesia.

[3]. S. Nambiar; C. T. Lu; and L. R. Lian (2004). Analysis of Payment Transaction Security in Mobile Commerce, *in Proceedings of the IEEE International Conference on Information Reuse and Integration (IRI'04)*. Nevada, USA, pp. 475-480.

[4]. _____,(2011). *Introduction to NFC,* Forum Nokia http://www.adafruit.com/datasheets/Introduction_to_NFC_v1_0_en.pdf , June 22, 2011, 09.35 GMT+7.

[5]. _____,(2011). *Near Field Communication Technology and the Road a head*, Forum NFC http://www.nfc-forum.org/resources/presentations/, June 30, 2011, 07.59 GMT+7.

[6]. Dr. Thalal Alkharabi.(2007), *Encryption Block Chiper*, Lecture Notes, http://www.ccse.kfupm.edu.sa/~talal/Sec/crept_Block.pdf , August 28, 2011, 08:24 GMT+7.

[7]. Stalling W (2005). *Cryptography and Network Security: Principles and Practice.* Prentice Hall, Fourth Edition.

[8]. Dandash Osama; Wu Xianping; Le Phu Dung (2005). Wireless Internet Payment System Using Smart Cards, *Proceeding Of International conference on Information Technology : Coding and Computing.* IEEE Xplore, 0-7695-2315-3/05

[9]. Rafael Martinez-Pelaez; Fransisco Rico-Novella; Christina Satizabal and Jhon J Padilla (2008). *Performance Analysis of Mobile Payment Protocols over the Bluetooth Wireless Network*, http://www.imaginar.org/ecollecter/fullpapers/p84-PerformanceAnalysisOfMobilePaymentProtocols.pdf, August 30, 2011, 08:21 GMT+7.

[10]. Supakorn Kungpisdan (2005). *Modelling, Design, and Analysis of Secure Mobile Payment Systems*, http://www.csse.monash.edu.au/~srini/theses/Keng_Thesis.pdf, August 12, 2011, 09:31 GMT+7.

[11]. Reto Meier (2010). *Professional Android 2 Application Development*. Willey Publishing Inc, Indianapolis.

[12]. Dominik Gruntz (2011). *NFC with Android.* University of Applied Sciences Northwestern Switzerland, Brugg-Windisch, http://www.fhnw.ch/technik/imvs/publikationen/artikel-2011/Jazoon_NFC.pdf, Sept 16, 2011, 13.24 GMT+7.

[13]. Husni, E.; Kuspriyanto; Basjaruddin, N.; Purboyo, T.; Purwantoro, S.; and Ubaya, H. (2011). Efficient Tag to Tag NFC Protocol for Secure Mobile Payment, *in Proceeding Of International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME).* Bandung, Indonesia, pp. 97-101.

[14]. HaselSteiner Ernst; Breitfub Klemens (_____). *Security in Near Field Communication*, http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002-SecurityinNFC.pdf , August 10, 2011, 11:15 GMT+7.

[15]. _____, (_____), Moserware, Jeff Moser's Software Development Adventure, http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

[16]. Husni, E., Kuspriyanto, Basjaruddin, N., Purboyo, T., Purwantoro, S., and Ubaya, H., (2011), Efficient Tag to Tag NFC Protocol for Secure Mobile Payment, *in Proceeding Of International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME),* Bandung, Indonesia, pp. 97-101.


ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)