European Journal of Computer Science and Information Technology
Vol.3, No.3, pp.1-10, June 2015
Published by European Centre for Research Training and Development UK (www.eajournals.org)

A SECURED MOBILE PAYMENT TRANSACTION PROTOCOL FOR ANDROID SYSTEMS

C. Ugwu, T. Mesigo
Department of Computer Science, University of Port Harcourt, Rivers, Nigeria

ABSTRACT: *The smart-phone industry has witnessed tremendous growth in recent history simply because of the emergence of the android operating system. It is now easier to make payments on our mobile phones but one major hindrance lies in transaction security. The objective of this paper is to develop a secure transaction protocol for an android based mobile payment system using quick response code technology and a hybrid cryptographic scheme. To achieve a better security in the system, we implemented symmetric, asymmetric cryptography alongside hashing and message authentication codes simultaneously in the system protocol. The results obtained depict a secure mobile payment system which makes use of dual authentication mechanism by two distinct entities.*

KEYWORDS: A*ndroid mobile wallet, QR code, transaction protocol, cryptographic protoco*

INTRODUCTION

The emergence of smart phones has brought about a shift from electronic commerce to mobile commerce. Mobile payment is a process of two participants exchanging monetary value using a mobile device in response for merchandise or services [1]. Mobile commerce is a technology which is a result of merging electronic commerce and wireless computing [2]. Mobile payment is considered as the accelerator of mobile commerce [3]. Mobile payment systems can be classified based on its technology, transaction size, location, user etc. [4] There are two categories namely proximity and remote payments. [5]. Proximity payments require both sender and receiver to meet physically in order to complete a transaction while remote payments does not require the physical interaction of both parties. [5] Transaction security is one of the major challenges facing mobile commerce today. In order to secure transactions in mobile payment systems, the art of cryptography is usually employed. Cryptography can be defined as the science and study of secret writing [6]. Cryptography is the art of achieving security by encoding messages to make them non-readable [7]. Encryption is the process of transforming plain text into ciphertext while the reverse is called decryption. Cryptography provides secrecy for data sent over channels where eavesdropping and message interception is possible [6]. The emphasis of cryptography is secrecy, authentication and integrity [8]. Cryptographic systems makes use of a key and an algorithm. The algorithm is usually known but the key is always secret. The three kinds of cryptographic schemes are secret key cryptography, public key cryptography and hash functions. Secret key cryptography involves the use of a single key which is shared among the parties involved secretly. The public key cryptography involves the use of two keys, the public key and the private key. The public key is always known to the public while the private key is only known to the administrator. Hash functions are another type of cryptographic scheme but it

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

does not make use of any key. Our study relates more to the proximity type of mobile payments. The Objective of this paper is to develop a secure transaction protocol for mobile payments using a hybrid cryptographic scheme.

RELATED WORKS

In order to effectively analyze and conduct a study in a particular subject, it is very important to study what others have done in that area. We have conducted a literature review of related works already published on this subject. Vorugunti et al in their paper titled a secure account based mobile payment protocol with public key cryptography, presented an account based payment protocol for m-commerce in wireless networks based on public key cryptography[2]. Aboud in his paper titled public key cryptography for mobile payment, investigated mobile payment and its security, while explaining elliptic curve with public key encryption[1]. Ayu Tiwari et al in their paper titled a multi factor security protocol for wireless payment-secure web authentication using mobile devices, proposed a new transaction protocol using multi-factor authentication system[9]. Pawandeep et al in their paper titled a secure account based mobile payment protocol with public key cryptography and biometric characteristics, presented a secure account based transaction protocol using public key cryptography [10]. Douglas et al in their paper titled a protocol for secure transaction , presented a secure transaction protocol that provides relational properties in addition to the normal properties of secure messages[11]. Houssam et al in their paper titled a secure electronic transaction payment protocol design and implementation, designed a new secure payment protocol which offers an extra layer of protection for users[12]. Miroslav S., in his thesis titled implementation of payment protocol on NFC-enabled mobile phone examined feasible solutions for implementation of payment protocol on the NFC-enabled mobile phone (with Android operating system)[13] .

From our reviews in the literature, we discovered that most protocols make use of public key cryptography for their security and also authentication is done by a single entity. This makes the existing systems less secure since a single entity can easily be compromised leaving the whole system insecure.

ANALYSIS

There exist four unique business models in the mobile payments industry. They are the mobile operator centric model, the Bank centric model, the independent service provider (ISP) centric model and the collaboration model. The mobile operator centric model is built around the mobile network operator (MNO). The MNO develops, deploys and manages the mobile payment system. Most times, the funds are withdrawn from the user's airtime. The bank centric model is built around the banks or major financial institutions. The users must have an account with the bank or open one during subscription. The accounts are managed and serviced by the banking institutions. The independent service provider model usually has an independent intermediary between the financial institutions and the operators. Finally, the collaboration model involves the financial institutions collaborating with any other major stakeholder in the industry in order to manage tasks and provide mobile payment services.[14]

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

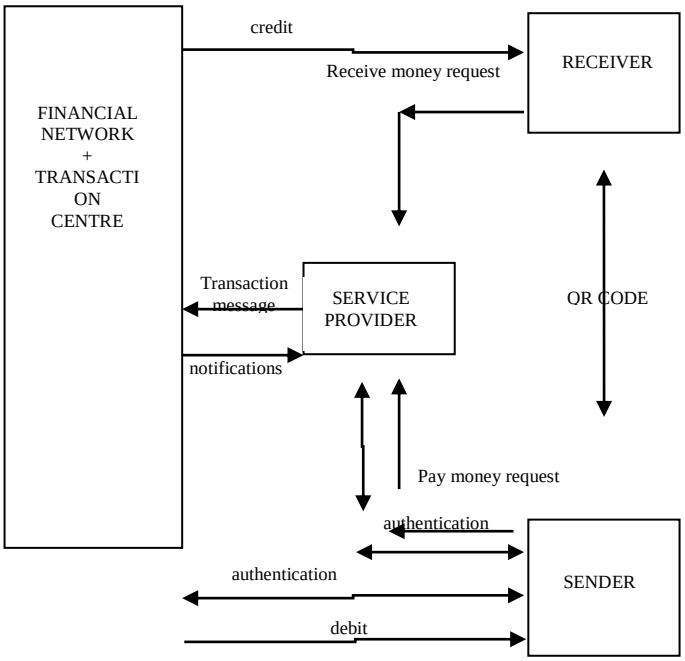

Fig 1: Proposed Mobile Payment Architecture

The mobile payment architecture in Fig 1 shows collaboration between the service provider which can be a third party company and the financial network which includes the banks and financial institutions. The financial network as shown in Fig 2 is made up of various banking institutions with a common clearing house known as the transaction centre TC. The transaction centre is responsible for the actual transfer of financial value from one user to another.

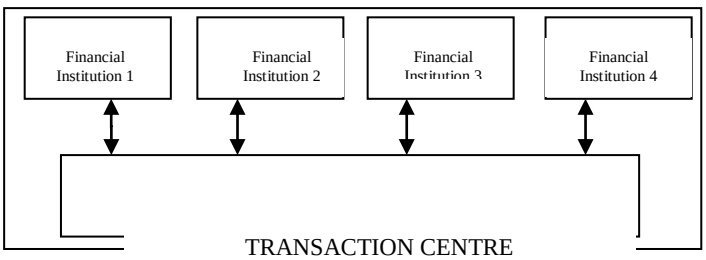

Fig 2: Financial Network Architecture

In fig. 3, the diagram describes the major activities that make up the system. The application starts with a default activity known as the splash screen activity. This is just a welcome page activity that has a three seconds timer. The splash screen activity gives way to the dashboard after the three seconds has elapsed. The dashboard activity is like the home of the application from where other various activities are tied to. It has the history, pay money, receive money and setup links. The history enables one to view recent transactions, the pay money and

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

receive money enables the user to perform a financial transaction, while the setup activity allows the user to edit his account settings and add money accounts.

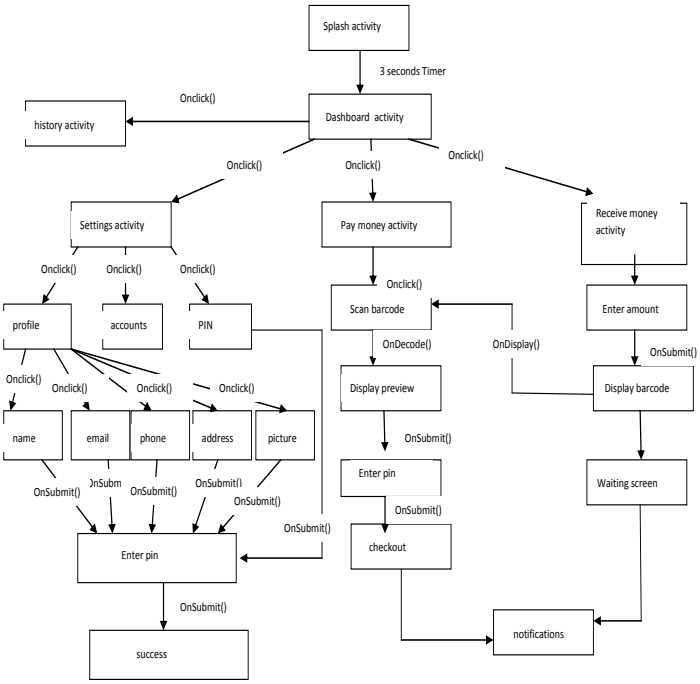

Fig 3 System Activities

PROPOSED TRANSACTION PROTOCOL

The Following Assumptions were made in the design of this protocol, such assumptions are:

- The application is owned and managed by the service provider.
- There exists a financial network which comprises of banks and financial institutions collaborating together under a unit to process financial transaction.
- Before any transaction can take place, both the sender and the beneficiary must download and configure the mobile application from the service provider.
- The Sender and the beneficiary is known are both are connected in an QR peer-to-peer mode.

Other notations used in this protocol include
R :RECIPIENT
S: SENDER
SP: SERVICE PROVIDER
FN: FINANCIAL NETWORK
P: Price
$E._{sign}$: Entity's signature
$E._{pub}$: Entity's public key
$E._{pri}$: Entity's private key
CR: $[P||T_{id}||Sess_{id}||Ts||R.Acct._{id}]$
$Acct._{id}$: Account identification number
H[x]: Hash Function of x

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

TC: Transaction Center
K_1 : MAC calculation key
K_2: Message Authentication Code (MAC)
$TM:[R.Acct._{id}||S.Acct._{id}||P||T_{id}||Sess_{id}||Ts]K_1.SP_{sign}[K_2]TC_{pub}.SP_{sign}$

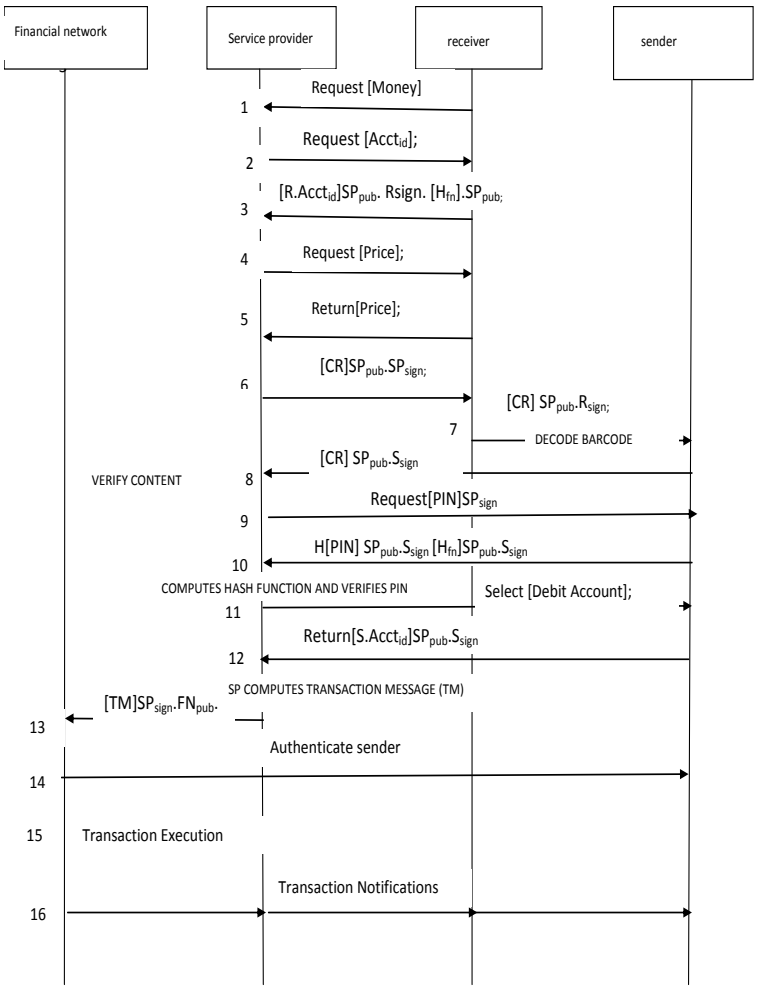

Fig.4 Proposed Transaction Protocol

1. R→ SP: Request [Money] ; Recipient sends a message to the service provider requesting for money. To initiate a payment transaction, the recipient will send a request money message to the service provider to indicate interest in receiving financial value.
2. SP→ R: Request [$Acct_{id}$]; Service provider then requests for account identification from the recipient. In order to process a transaction, the service provider will require the account details of the recipient which is requested in this message.
3. R→ SP: [$R.Acct_{id}$]SP_{pub}. Rsign. [H_{fn}].$SP_{pub;}$ The recipient sends a message to the service provider containing the Account id which is signed by the Recipient's signature and secured by the service provider's public key. Also appended to the message is the Hash function which will be used to decode the account id.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

4. SP→ R: Request [Price]; The service provider requests for the price of the transaction from the recipient. This will prompt the receiver to enter the amount of money expected.
5. R→ SP: Return[Price]; Recipient inputs the price and sends back to the service provider.
6. SP→ R: [CR]SP_{pub}.$SP_{sign;}$ Service provider sends a credit request message intended for the sender to the recipient. This is signed by the SP's signature and secured by SP's public key. Since nobody else has the SP's private key, nobody else can decode the message.
   CR= [P||T_{id}||$Sess_{id}$||Ts||R.$Acct._{id}$]
7. R→ S: [CR] SP_{pub}.$R_{sign;}$ The receiver's phone then generates a corresponding QR code and displays it to the sender to scan. The credit message is secured by the service provider's public key and the receiver's signature. The signature verifies to the service provider that the message was actually sent by the receiver and has not been altered as well.
8. S→ SP:[CR] SP_{pub}.S_{sign} The sender after scanning the QR code, sends the same message back to the Service provider who verifies the authenticity and validity of the message.
9. SP→S: Request[PIN]SP_{sign} The service provider now request for proper identification of the sender by requesting the PIN to authorize the transaction and enforce non-repudiation. The request is accompanied with a signature from the service provider to ensure authenticity.
10. S →SP:H[PIN] SP_{pub}.S_{sign} [H_{fn}]SP_{pub}.S_{sign} The sender then sends a hashed PIN to the service provider with the hash function secured with the SP's public key, and a digital signature from the sender. The pin is hashed to secure it in the event that it was hacked which will make it almost impossible to decode.
11. SP→S: Select [Debit Account]; The service provider requests the sender to select the particular account from which the transaction will be made from.
12. S →SP: Return[S.$Acct_{id}$]SP_{pub}.S_{sign} the sender selects an account from his/her profile and the selected account is returned to the service provider. It is secured by the SP's public key, Sender's private key and signature.
13. SP→FN: [TM]SP_{sign}.FN_{pub}. the service provider then prepares a transaction message for the financial network with all the necessary details for the transaction.
14. FN→ S Verify[sender]. Upon receipt of the transaction message, the financial network verifies the sender usually with a PIN or password and if successful, checks for enough account balance and thereafter proceeds with the transaction execution by the transaction center.
15. FN: Transaction Execution by the transaction center
16. FN→ SP R S: Transaction Notifications After a successful transaction, The financial network now sends notifications/receipts to all participating entities in the transaction.

IMPLEMENTATION AND RESULTS

The object oriented analysis and design methodology was adopted for the design. Zebra Crossing library (Zxing) was used to implement the Quick response code technology in the

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

project. The implementation was done with java programming language in the development of the target android based mobile wallet and Android Studio as our integrated development environment (IDE).

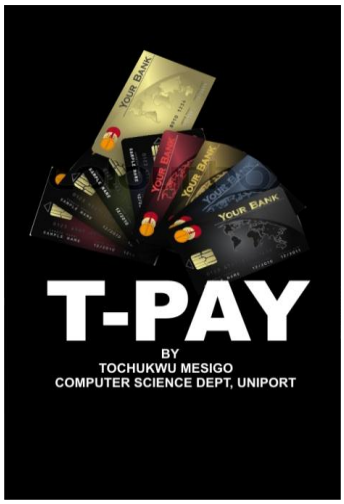

Figure 5: Splash Screen

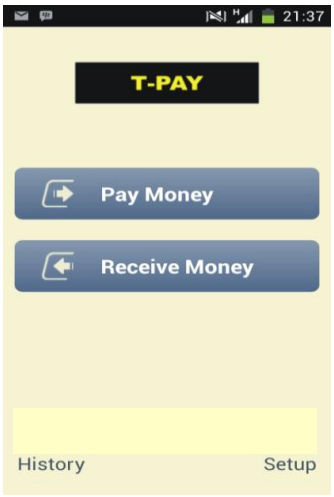

Figure 6: Dashboard

Figure 7: Input Amount

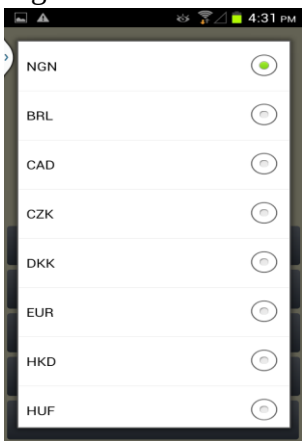

Figure 8: Currency List

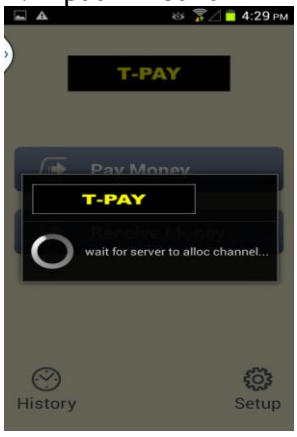

Figure 9: Generating QR Code

Figure 10: QR Code

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

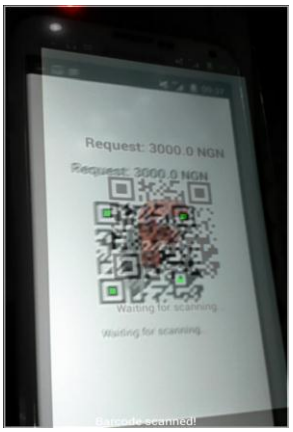

Figure 11: Scanning QR Code

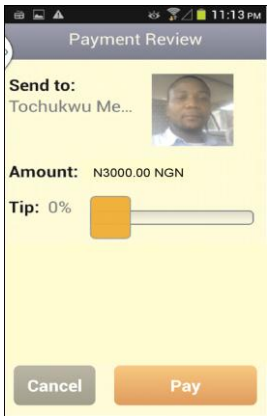

Figure12: Payment Preview

Figure 13: Receiver's Waiting Screen

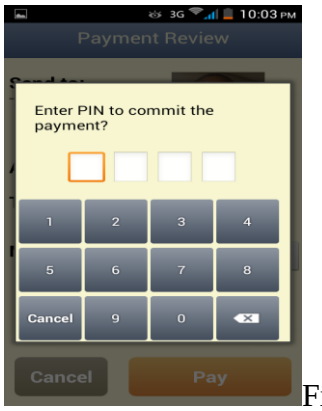

Figure 14: Service Provider's Authentication

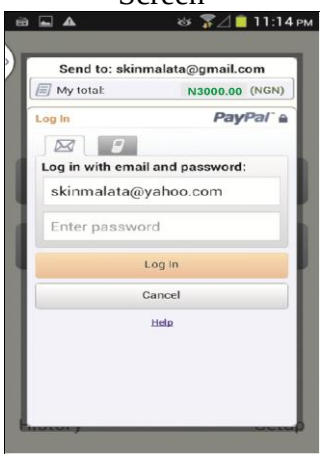

Figure 15:Paypal Authentication

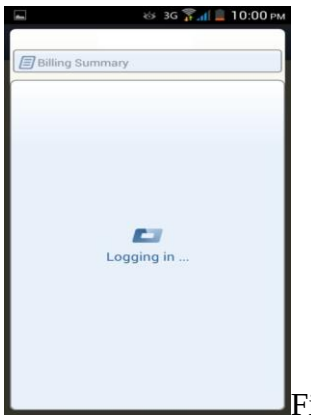

Figure 16: Login Successful

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

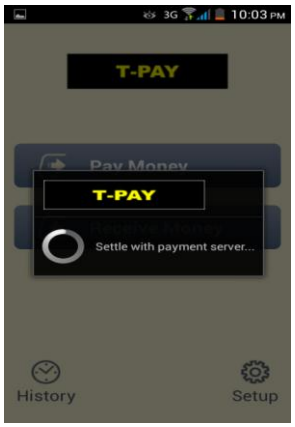

Figure 17: Settling Payment

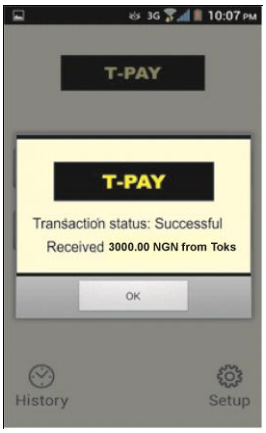

Figure 18: Notification

DISCUSSION OF RESULTS

The splash screen activity shown in fig 5 is launched as the default activity immediately the application is launched. The splash screen has a timer of 3 seconds upon which it gives way for the dashboard module for a registered account or the registration module for the unregistered account. From the dashboard as shown in fig 6, a user can either pay money or receive money. The user can as well view his transaction history or setup and edit account functions. To pay money, the user selects pay money from the dashboard and then scans the QR code of the other party he is paying to as shown in fig 11. After successful scanning, the payment preview activity is displayed as shown in Fig 12. In order to complete payment, the user is prompted to enter his PIN for authentication by the service provider and then his password for authentication by the financial institution as shown in fig 14 and 15 respectively. Once both authentication are successful, the payment server initiates the final transfer of financial value from the sender to the receiver as shown in fig 17. At the end of the transaction, transaction notifications are sent to both parties to signal the completion of the transaction. The results shows that the objective of this study has been attained with the achievement of developing a secure android based mobile payment system using QR code technology and a hybrid cryptographic scheme.

CONCLUSION

We have developed a secure transaction protocol which is based on a hybrid cryptographic scheme. The mobile payment system developed runs on android operating system and uses QR code technology for peer to peer communication. The authentication was handled by two entities instead of a single entity which makes it more secured since a single entity can easily be compromised, but it will be harder if two different entities handle authentication since one will remain intact even when the other is compromised thereby ensuring the integrity of a transaction.

REFERENCES

[1] Sattar J Aboud, "Public Key Cryptography for mobile payment", Special Issue of Ubiquitous Computing Security Systems UbiCC Journal - Volume 5, pp1789-1793, 2005

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

[2] Vorugunti Chandra Sekhar, Mrudula Sarvabhatla, "A Secure Account-Based Mobile Payment Protocol with Public Key Cryptography", ACEEE International Journal on Network Security , Vol. 03, No. 01, pp 5-9, 2012

[3] Vibha Kaw Raina, U.S Pandey, Munish Makkad, "A user friendly transaction model of mobile payment with reference to mobile banking in india", international journal of information Technology, vol 18, No 7, pp 1-25, 2012

[4] Raina V. K., Pandey U. S., and M. Makkad, "A User Friendly Transaction Model of Mobile Payment with reference to Mobile Banking in India," International Journal of Information Technology, vol. 18, No. 2, pp 1-6, 2012.

[5] C.Ugwu, T.Mesigo, "A novel mobile wallet based on android os and quick response code technology", international journal of advanced research in computer science and technology, vol 3, no 1, 2015

[6] Dorothy Elizabeth, Robbling Denning, "cryptography and data security", Addison-Wesley publishing company, 2012

[7] Ayushi, "A symmetric key cryptographic algorithm," international journal of computer applications vol1, No 15, pp 1-4, 2010

[8] Gurpreet Kaur, Kamaljeet Kaur, ". Digital watermarking and other data hiding techniques", international journal of innovative technology and exploring engineering vol2, issue 5, pp 181-183, 2013

[9] Ayu tiwari, sudip sanyal ajith abraham, svein johan knapskog, sugata sanyal, "A multi-factor security protocol for wireless payment- secure web authentication using mobile devices", iadis international conference applied Computing pp 1-8, 2007

[10] Pawandeep Singh Aujla1, Harneet Arora, "A Secure Account based Mobile Payment Protocol with Public Key Cryptography and Biometric Characteristics", International Journal of Science and Research IJSRVolume 2 Issue 3,pp 428-431, 2013

[11] Douglas H Steves, Chris Edmondson-Yurkanan, Mohamed Gouda, " A protocol for secure transactions", University of Texas, department of computer science, 1996

[12] Houssam El Ismaili, Hanane Houmani, Hicham Madroumi " A Secure Electronic Transaction Payment Protocol Design and Implementation ", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 5 pp 172-180, 2014

[13] Miroslav Svítok , "Implementation of Payment Protocol on NFC-enabled mobile phone" , Masarykova Univerzita ,pp 8-35,2014, unpublished

[14] L. Chaix, and D.Torre. "Four models for mobile payments". University Nice Sophia-Antipolis, JEL Classification: E42, O33, 2011.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)