Secure Mobile Payment Protocol using Asymmetric Encryption for Authorization

Sherif Elfakharany
Computer Engineering, Arab Academy for Science, Technology and Maritime Transport

Ahmed Fahmy Amin
Computer Engineering Head of Department, Arab Academy for Science, Technology and Maritime Transport

Mohamed Zaki
Systems and Computers Engineering, Faculty of Engineering, Al Azhar University

Abstract – The widespread use of the Internet has highly supplied the growth of e-commerce. Technological progress in mobile phones (e.g. Smartphones) has also contributed to carrying out e-commerce via mobile phones (m-commerce). M-commerce involves the use of mobile devices such as mobile phones in carrying out electronic transactions. Applications in this domain range from normal information consumption to high security financial electronic transactions. Just like e-commerce, the security of m-commerce applications is critical, especially when it involves applications that deal with user sensitive data such as credit cards details. In this paper we present a secure mobile payment protocol which is suitable for m-commerce to transfer the payment using asymmetric cryptography based on Needham-Schroeder public-key protocol. Our protocol performs encryption for authorization and satisfies more security requirements compared to existing standard payment protocols. In the implementation, the buyer uses the browser to shop online as usual, at the checkout he is sent to the mobile application provided and secured by the bank. The parties communicates through three different channels (VPN tunneling, SMS messaging and HTTPS) to enhance the security. The application has to implement some kind of authentication to make sure the mobile owner is the one who is using it. After the purchase is complete the buyer is returned to the browser to continue his usual internet experience. This protocol ensures that the buyer critical information is never passed over the internet to be able to purchase and at the same time the browsing experience has little interruption. Also it introduces little overhead on the merchant and the banks to be able to provide such service. To make sure the protocol works as intended, an android application was made that communicates with web servers representing the buyer bank, the merchant website and merchant bank. All communications between the application and the buyer bank were through VPN and SMS. In the implementation the buyer uses a mobile application provided and secured by the bank. The parties communicates through three different channels (VPN tunneling, SMS messaging and HTTPS) to enhance the security. The protocol typically has some kind of authentication to make sure the mobile owner is the one using it. The proposed protocol provides the security property and includes Non-repudiation and customer privacy protection properties.

Index Terms – Mobile Payment, Security, Account based, Asymmetric Cryptography, Encryption, Authorization.

1. INTRODUCTION

Mobile commerce is a powerful technology in which e-commerce is carried out through a Mobile. M-commerce represents extended application of e-commerce, in which the user uses a mobile device, such as a mobile phone, to carryout transactions. The payment transactions in m-commerce are called mobile payments, they range from basic applications such as mobile marketing to high security mobile payment applications.

Mobile payments will allow users to pay anyone, anywhere at any time for any purpose. Service providers will compete in this marketplace by offering lower prices but, more and better services, security and privacy. The number of people worldwide who possess mobile devices grows rapidly, it will exceed the number of people who hold bank accounts and carry credit cards.

Mobile payment applications face some security risks such as Insufficient transport-layer protection, Poor authorization and authentication, Broken cryptography, Sensitive information disclosure…etc [1]. Also when shopping using the mobile internet browser, it is required to provide a payment method which is both practical and secure.

Authorization and secure payment are major security issues when it comes to carrying out mobile financial transactions remotely. Improving security while maintaining the buyer experience on the web and reducing implementation overhead are considered challenges to mobile payment protocols. Also acquiring Authentication, Confidentiality, Integrity of Payment Data, Authorization, Non-Repudiation, Privacy Protection and Anti-Replay Protection aspects [2].

One of the risks that involve online purchasing is the disclosure of sensitive credit-card/bank-account information over the internet. Also SSL was proved to be vulnerable to penetration [3] leading to the risk of theft of this information. Even when this information is stored at third party payment sites (e.g. PayPal [4]), still this third part might get hacked, and still the user name and password might be stolen too.

To handle these issues, a protocol is proposed that uses public key encryption for authorization and secure tunneling for communication between buyer/merchant and their respective banks to ensure that the credit-card/bank-account information is never passed through the internet. There is no need for the buyer to expose critical information to be able to make the purchase. This protocol takes advantage of the mobile phone applications to be able to provide such functionality. Another aim of that protocol is to allow the buyer to do his traditional online shopping with little overhead as will be shown later.

2. RELATED WORK

In this section several mobile payment research works are analyzed briefly.

2.1. Traditional payment [5]

In the traditional payment the payment process runs as follows:

1- The buyer chooses to pay for an item at an m-commerce store using a credit card (e.g. visa, MasterCard etc.). Inputs credit card details.
2- M-commerce application request authentication by sending card information and cost of product (transaction details) to merchant processor.
3- Merchant processor detects card brand (visa, MasterCard etc.) based on cards first 6 digits, and sends an authorization request to the identified card association.
4- Card association identifies the (based on internal database) bank that issued the card, and sends the authorization request to the issuer bank.
5- The issuer bank will either approve or decline the transaction based on their set criteria. The decision is sent back to the card association.
6- The card association sends the decision back to the merchant processor.
7- The merchant processor relays the decision back to the m-commerce store.
8- In the case where the transaction was approved, the m-commerce application sends it to the merchant processor for processing.
9- The merchant processor sends the transaction to a merchant bank where the m-commerce store has an account.
10- The merchant bank pays the amount involved in the transaction into the m-commerce store account. It then requests an equivalent amount from the identified (message 3) card association.
11- The card association re-sends the request for payment to the bank that issued the card.
12- The issuer bank deducts the requested amount from the buyers bank account tied to the credit card. It then transfers the amount to the card association.
13- The card association transfers the money to the merchant bank.

Note: The m-commerce store returns transaction result (completed, pending, denied etc.) to the buyer. This can take place any time after message 7, and based on whether the transaction was authorized or not.

2.2. SecureSMSPay Secure SMS Mobile Payment model [6]

A model that uses symmetric cryptography. It is based on SMS as a transport channel. The payer receives a secured SMS message (invoice) based on the mobile number, waiting for his/her confirmation (yes/no). The payment gateway will be responsible for routing transactions based on the mobile number. Used for m-payment, without browsing the internet.

2.3. Online Based Authentication and Secure Payment Methods for M-Commerce Applications [5]

Based on One-Time Password (OTP) via SMS-Password authentication (OSP) method. The OSP system sends an OTP to the user's mobile device, the user completes the process by retrieving and providing the retrieved OTP.

2.4. PayPal [4]

This is a system which makes use of a one-factor authentication. The strength of this system lies in the underlying fact that users are mandated to choose strong passwords. Although a strong password can be chosen, such one-factor systems have been shown to be vulnerable to attacks such as password cracking and is not considered secure enough [5].

2.5. Summary

The following aspects in many of the existing researches focusing on security for mobile payment transactions are not fully covered:

1- Applying an appropriate balance between security and practicality.
2- Performing sufficient integrity and isolation protection for the security demands.
3- Providing a platform integrity protection solution.
4- Dealing with the online shopping experience via the web.

3. PORPOSED PROTOCOL

3.1. Introduction

The following figure shows the different parties of the system.

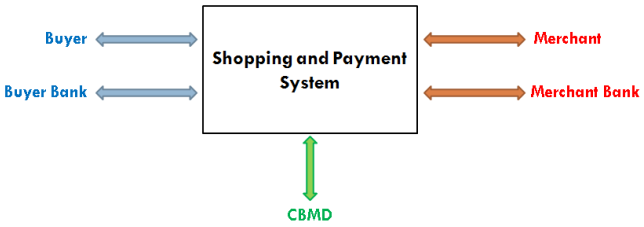

Figure **Error! No text of specified style in document.**.1: The parties of the system

These parties are: buyer, buyer bank, merchant, merchant bank and CBMD. The following sections describe each of the roles in that system, then the proposed protocol will be described in details.

3.2. The protocol parties

Buyer

The buyer is a party who requests to purchase products or services from a merchant.

The buyer is represented as the buyer mobile phone. It has the following components:

1- Any mobile web browser to be able to browse the merchant website and initiate the checkout.
2- A mobile application (typically provided by the bank) to do the payment which can contact the bank (via secure channels using VPN and SMS) and the merchant website's web service through HTTPS.

Buyer Bank

The buyer bank is the buyer's financial institution. It has the buyer's account established. Its task is to manage the buyer's account including fund transfer. Many banks now provide their clients with a mobile application through which they can access the bank services. This application provides secure communication between the buyer and the bank. An extension to this application can be added to provide the buyer with online payment service according to the proposed protocol.

In the proposed protocol, the buyer bank should be able to communicate with the following:

1- The buyer through the secure channel provided through the mobile application.
2- The merchant bank through the secure banks' channel.
3- A repository containing online merchant information.

Merchant

The merchant has products or services offered to the client.

The merchant is represented as a web server which has the following components and interfaces:

1- The first is the website which shows the catalog of the merchant products and through which the buyer can check out his shopping bag.
2- The second is a web service which interfaces with the mobile payment application on the buyer's phone.
3- The third is the component in the web server which communicates with the bank through a secure channel (e.g. VPN).

Merchant Bank

The merchant bank is the merchant's financial institution. It has the merchant's account established. Its task is to manage the merchant's account. Many online stores can contact their banks to process credit card information for payment and validation. The same method can be used to transfer the proposed protocol's data between the merchant and the bank.

In the proposed protocol, the merchant bank should be able to communicate with the following:

1- The merchant's website through the secure channel which the website typically uses for credit card processing.
2- The buyer's bank through the secure banks' channel.
3- A repository containing online buyers' information.

Common Buyer Merchant Directory (CBMD)

As mentioned before, there should be a repository containing the buyer and merchant information. This repository should contain data for the buyer and merchant that can be used to authenticate the buyer/merchant. It should be accessible at the banking private network side. In this study, this repository will be called the Common Buyer Merchant Directory (CBMD).

The CBMD stores a record which contains the following: ID, public key and the bank owning this ID. For the merchant, it also has a field containing the URL used on his website to initialize payment.

The merchant and the buyer provide their CBMD IDs to each other which their respective banks use to get the CMBD record of the other party. Once the bank gets the record, it uses the information about the bank to contact the other party's bank, and the public key to do the encryption required by the protocol. The buyer bank sends the payment URL back to the buyer for the application to do the rest of the protocol steps.

When the merchant registers his website for online payment, his bank registers a record for him in the CBMD. When the buyer registers for the online payment option, his bank registers a record for him in the CBMD.

There should be a central authority responsible for controlling and maintaining the CBMD.

3.3. The protocol steps

This assumes the use of a public key encryption algorithm for authorization.

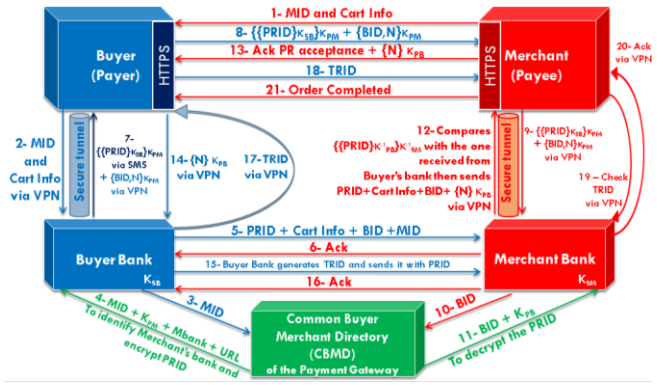

Figure **Error! No text of specified style in document.**.2: The protocol scheme

Here, Buyer (B), Merchant (M), Buyer's Bank (BB) and Merchant's Bank (MB) use a trusted server CBMD (Common Buyer Merchant Directory) to distribute public keys on request. These keys are:

- KPB and KSB, respectively public and private halves of an encryption key-pair belonging to B (S stands for "secret key" and P stands for "Public key").
- KPM and KSM, similar belonging to M.

Keywords:

- MID ... Merchant ID
- BID ... Buyer ID
- CI ... Cart information
- PRID ... Payment Request ID
- VPN ... Virtual Private Network
- ACK ... Acknowledgment
- PRA ... Payment Request Acceptance

The protocol runs as follows:

1- M → B : MID, CI (HTTPS)

M sends MID and CI to B via HTTPS.

2- B → BB : MID, CI (VPN)

B sends MID and CI to BB via VPN.

3- BB → CBMD : MID (banks network)

BB sends MID to CBMD via banks network and requests K_{PM}.

4- CBMD → BB : MID, K_{PM}, MB (banks network), URL

CBMD responds with MID, K_{PM}, MB and URL to BB via banks network to identify MB and encrypt PRID.

5- BB → MB : PRID, CI, BID, MID (banks network)

BB sends PRID, CI, BID and MID to MB via banks network.

6- MB → BB : ACK (banks network)

MB sends ACK to BB via banks network.

7- BB → B : $\{\{PRID\}K_{SB}\}K_{PM}$ (SMS) + $\{BID,N\}K_{PM}$, URL (VPN)

BB encrypts the PRID with the buyer's secret key, and then by the merchant's public key and sends it to B via 2 SMSs.

BB encrypts the BID and random number (N) with the merchant's public key, so that it can't be decrypted except by MB, and sends it with the merchant's website URL to B via VPN.

8- B → M : $\{\{PRID\}K_{SB}\}K_{PM}$ + $\{BID,N\}K_{PM}$ (HTTPS)

B sends the message received from BB to the M via HTTPS.

9- M → MB : $\{\{PRID\}K_{SB}\}K_{PM}$ + $\{BID,N\}K_{PM}$ (VPN)

M sends the message received from B to the MB via VPN.

10- MB → CBMD : BID (banks network)

MB performs $\{\{PRID\}\ K_{SB}\ \}K^{-1}{}_{SM}$

i.e. decrypts the PRID by the merchant's secret key.

Also MB performs $\{BID,N\}K^{-1}{}_{SM}$

i.e. decrypts the BID and N by the merchant's secret key.

In addition MB sends BID to CBMD via banks network and requests K_{PB}.

11- CBMD → MB : BID, K_{PB} (banks network)

CBMD responds with BID and K_{PB} to MB via banks network (so that MB can decrypt the PRID once more, to obtain the plain PRID).

12- MB → M : PRID, CI, BID, $\{N\}\ K_{PB}$ (VPN)

MB performs $\{PRID\}K^{-1}_{PB}$

i.e. decrypts PRID once more with the buyer's public key.

MB encrypts the N with the buyer's public key, so that it can't be decrypted except by BB,

$\{N\}\ K_{PB}$

Finally MB compares the decrypted PRID with the one received from BB in step5.

If they match, then MB sends the corresponding PRID, CI, BID and $\{N\}K_{PB}$ to M via VPN.

13- M → B : PRA, $\{N\}\ K_{PB}$ (HTTPS)

M sends PRA and $\{N\}\ K_{PB}$ to B via HTTPS.

14- B → BB : $\{N\}\ K_{PB}$ (VPN)

B sends $\{N\}\ K_{PB}$ to the BB via VPN.

15- BB → MB : TRID, PRID (banks network)

BB performs $\{N\}\ K^{-1}_{SB}$

i.e. decrypts N by the buyer's secret key.

BB compares the decrypted with the one sent in step 7.

If they match BB generates TRID and sends it with PRID to MB via banks network.

16- MB → BB : ACK (banks network)

MB credits BB with the payment value in TRID, and sends ACK to BB via banks network.

17- BB → B : TRID (VPN)

BB sends TRID to B via VPN.

18- B → M : TRID (HTTPS)

B sends TRID to M via HTTPS.

19- M → MB : TRID (VPN)

M sends TRID to the MB via VPN, to check that the transaction is accomplished.

20- MB → M : ACK (VPN)

MB sends Payment ACK to M via VPN.

21- M → B : Order Completion Page (HTTPS)

M navigates B to the Order Completion Page via HTTPS.

3.4. The protocol sequence diagram

A construct of the sequence chart showing how parties interact, arranged in time sequence. Vertical lines represent the parties, and horizontal arrows represent the messages exchanged between them, in the order in which they occur.

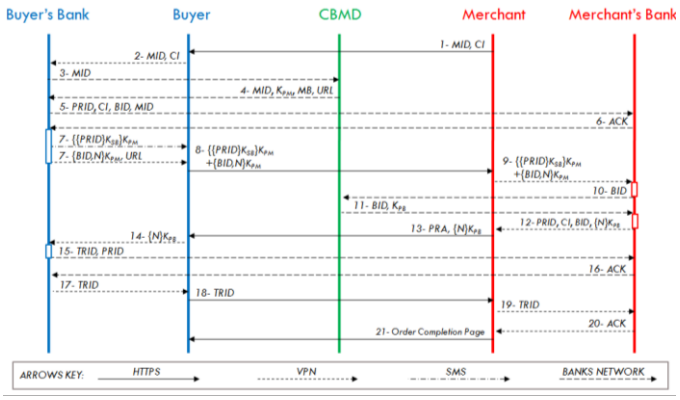

Figure **Error! No text of specified style in document.**.3: The protocol sequence diagram

3.5. The protocol essential features

1- Card Not Present (CNP): the card information is not transferred during any of the payment process stages.
2- Non-repudiation: discussed in the case studies section 4.2.
3- Asymmetric cryptography: also known as public-key cryptography[7].
4- Three different channels of communication: VPN tunneling, SMS messaging and HTTPS channels are used to enhance security.
5- User friendly interface: the implemented buyer mobile application is an easy to use application to minimize the user overhead.
6- Easily implemented: the integration with the merchant website is made as simple as adding a hyperlink to the webpage.

4. IMPLEMENTATION

4.1. Experimental setup

An android application was created as an example of a bank application on the buyer's mobile phone. This application was created using Eclipse ADT.

To represent the merchant website, a web application was created using Eclipse, Tomcat and java servlets. This application does the tasks required to be implemented in the merchant's online shopping website to support the proposed protocol.

To represent the banks for the buyer and the merchant, another two java servlet applications were created.

The experimental environment used an android device (Samsung galaxy s3) and a computer having a Tomcat application server on it to host the merchant website and the bank applications.

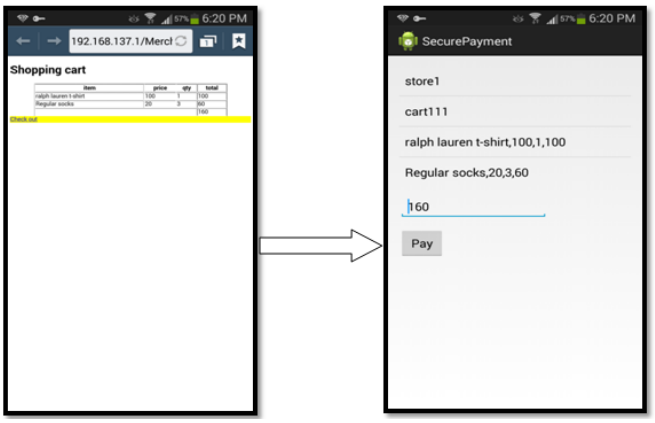

Figure **Error! No text of specified style in document.**.4: Screen shots of the experimental setup

Each of the merchant website and the bank applications are in separate applications on the application server. They can be deployed on different application servers on different platforms without any problem.

In this experiment, the VPN tunnel is implemented between the android device and the buyer bank application. The tunnel between the merchant and the merchant bank and the communication between the banks is not implemented since they are considered out of scope of this study.

The protocol used for communication between any of the components above is done through HTTP. For the android device to connect to the buyer bank through VPN, it calls the HTTP at the address of the VPN instead of the address of the computer. In real life, the protocol used between the merchant and the buyer would typically be HTTPS, the protocol used over the VPN between the buyer/merchant and their respective banks could be HTTP, HTTPS or even TCP as it is dependent on how the bank would like to secure its communication with its clients.

4.2. Case studies

Some case studies will be discussed in this section, which are repudiation, dispute mitigation, intrusion, impersonation and theft.

- Case 1: Repudiation

If the buyer repudiates his shopping process, the following can be used to deny his claim:

1- The buyer sent the encrypted PRID {GKXw1xHLFYn…}, to the merchant. It is decrypted using the merchant secret key (K_{SM}), then the buyer public key (K_{PB}), to give (8258554381). This is a proof of being sent by the buyer, as it is encrypted using the buyer secret key (K_{SB}) (which is only available to the buyer via his bank).
2- For confirmation, the buyer bank sent the PRID (8258554381), cart information (cart id = cart1, 2 shirts, 100$), the BID (B1) and MID (M1) accompanied by the payment, to the merchant bank.

- Case 2: Dispute Mitigation

If the buyer receives the goods with different specifications, the following can be used to confirm his claim:

1- The buyer received SMS of the encrypted PRID {MbK05Q15L7kT0....} corresponding to (3612758849). The buyer bank sent PRID (3612758849), cart information (cart id = cart2, 1 t-shirt & 3 socks, 160$), BID (B2) and MID (M2) to the merchant bank. By getting PRID (3612758849) at the merchant bank, and comparing the goods in the cart information accompanied to it (1 t-shirt & 3 socks), with the received goods (1 t-shirt & 2 socks), they don't match.
2- The merchant website sent MID (M2) and cart information (cart id = cart2, 1 t-shirt & 3 socks, 160$) to the buyer, which don't match the received goods (1 t-shirt & 2 socks).

- Case 3: Intrusion

If an intruder tries to replace the BID by his own ID to buy from the merchant using the buyer data, this can't be done because:

If the intruder takes the buyer's PRID (1365126104) encrypted as {EI92NPcuZcKC… } and BID (B3) encrypted as {eScRAof…}, and exchanges the BID (B3) with his own ID (B4), and encrypt it by the merchant public key (K_{PM}), so that it will be {1Df3#5…}. The merchant bank will then compare the PRID (1365126104) and the BID (B3) sent by the buyer bank, with the one received from the intruder via merchant (before decryption: EI92NPcuZcKC…, 1Df3#5… / after decryption: 1365126104, B4). So if the BIDs don't match, the merchant bank will not complete the transaction.

- Case 4: Impersonation

If an intruder tries to impersonate the buyer to contact the buyer bank, this can't be done because:

1- The buyer contacts his bank through a secure tunnel, which is not applicable except between the registered buyer and his bank (using a password).
2- The payment completion depends on the encrypted PRID {G0b7ph6NTVL…} sent to the buyer via SMS, which requires having access to the mobile and the SIM card, identified to the registered buyer.

- Case 5: Theft

If an intruder obtained the Mobile Station (Phone + SIM), The intruder will not be able to perform a payment transaction because he will still need to bypass the security of the application so that the application would let him perform the payment. The application would typically ask for at least a password that should only be with the device owner. Advanced banking applications could extend that to use multi-factor authentication using tokens, biometric information…etc.

5. COMPARATIVE STUDY

In this section the proposed protocol is compared to other m-payment researches and systems. This comparison is demonstrated in the table blow.

Aspects / System	Card Not Present (CNP)	Number of channels	Non-repudiation	Encryption type	Signatures	Based on security protocol
Modeling, Design and Analysis of Secure Mobile Payment Systems [8]	No	1 (Internet)	available	Asymmetric	Shared key	Authenticated key exchange (AKE)
SecureSMSPay [6]	Yes	1 (SMS)	available	Symmetric	Unsigned	Simple cryptography
A proposed architecture for secure two-party mobile payment [9]	No	2 (Internet-SMS)	available	Symmetric	Digital Signature Algorithm (ECDSA)	AES Symmetric key cryptography
Online Based Authentication and Secure Payment Methods for M-Commerce Applications [5]	No	2 (Internet-SMS)	available	No Encryption	Using password	OTP via SMS-Password authentication (OSP)
Secure Lightweight Mobile Payment Protocol [10]	Yes	1 (Internet)	available	Symmetric	Symmetric key	Symmetric key cryptography
The System for Secure Mobile Payment Transactions [11]	Yes	1 (Internet)	available	Asymmetric	Using private key	SAFE system
PayPal [4]	No	1 (Internet)	available	Asymmetric	API key	Secure Socket Layer (SSL)
Proposed Protocol	Yes	3 (VPN-SMS-HTTPS)	available	Asymmetric	Using private key	Needham-Schroeder [12]

Table 1: Comparison of m-payment systems

6. CONCLUSION

The technology improvement and wide spread use of mobile phones has led to the growth of m-commerce. M-commerce applications are used in social networking, online stores, and financial applications. The work conducted in this study involved (1) Customer centric mobile payment protocol based on asymmetric key cryptography and (2) Implementation of a prototype platform-independent payment protocol for m-commerce applications.

The proposed protocol can be used with the advantages of non-repudiation, Card Not Present, three different channels of communication (VPN/SMS/HTTPS) and ease of implementation.

REFERENCES

[1] A. K. Jain and D. Shanbhag, "Addressing security and privacy risks in mobile applications," IT Prof., vol. 14, no. 5, pp. 28–33, 2012.
[2] T. S. Fun, L. Y. Beng, and M. N. Razali, "Review of Mobile Macro-Payment Schemes," J. Adv. Comput. Networks, vol. 1, no. 4, pp. 323–328, 2014.
[3] R. Bozhinovski, V. Dimitrova, B. Jakimovski, and S. Ristov, "SECURITY PENETRATION TEST ON FCSE ' S IT SERVICE S," in The 10th Conference for Informatics and Information Technology (CIIT 2013), 2013, no. Ciit, pp. 208–211.
[4] "PayPal Account login." [Online]. Available: https://www.paypal.com/uk/cgi-bin/webscr?cmd=_login-run&dispatch=5885d80a13c0db1f8e263663d3faee8d422be6d275c375afb284863ba74d6cdc.
[5] K. Senanu and K. Krause, "Online Based Authentication and Secure Payment Methods for M-Commerce Applications," University of Gothenburg, 2011.
[6] H. Harb, H. Farahat, and M. Ezz, "SecureSMSPay: Secure SMS mobile payment model," 2nd Int. Conf. Anti-counterfeiting, Secur. Identification, ASID 2008, pp. 11–17, 2008.
[7] Wikipedia, "Public-key cryptography," 2013. [Online]. Available: https://en.wikipedia.org/wiki/Public-key_encryption.
[8] [8] S. Kungpisdan, "Modelling , Design , and Analysis of Secure Mobile Payment Systems," Master Thesis, 2005.
[9] J. E. Rice and Y. Zhu, "A proposed architecture for secure two-party mobile payment," in IEEE Pacific RIM Conference on Communications, Computers, and Signal Processing - Proceedings, 2009, pp. 88–93.
[10] [V. C. Sekhar and M. Sarvabhatla, "Secure lightweight mobile payment protocol using symmetric key techniques," 2012 Int. Conf. Comput. Commun. Informatics, ICCCI 2012, pp. 8–13, 2012.
[11] B. Pouralinazar, "The System for Secure Mobile Payment Transactions," 2013.
[12] G. Lowe, "An attack on the Needham-Schroeder public-key authentication protocol," Information Processing Letters, vol. 56, no. 3. pp. 131–133, 1995.