International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 06, June 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

SECURE MOBILE COMMERCE AND PROTOCOLS IN VOLATILE ENVIRONMENT

Narinder Bali[1], Raghav Mehra[2], Anita Gupta[3]

[1]*Department of Computer Sciences,, Bhagwant University. Ajmer, Rajasthan*

[2]*Department of Computer Sciences, Bhagwant University. Ajmer, Rajasthan*

[3]*Govt. College for Women, Parade Ground, Jammu, J&K*

ABSTRACT

Internet technology offers extensive range of services such as electronic mails, file transfers, etc., and one of the most popular services offered on the internet is "Electronic Commerce" (or e-commerce). Ecommerce is becoming bigger technological wave that has changed the way by which business is becoming being conducted. Systems with a focus on threats, vulnerabilities and risk. Mobile payments (m-payments) are increasingly being adopted by organizations as a new way of doing business in the 21st century. During the last few years, the use of m-payments as a new payment channel has resulted in an increase in the volume of literature dedicated to the topic. For this reason, this paper presents the findings of a review of literature aimed at identifying the key research themes and methodologies researched.

Keywords: E-commerce, cryptographic operations, m-payment, mobile devices, Internet technology

I INTRODUCTION

The rapid proliferation of portable devices and the world wide penetration of mobile cellular subscription. Using m-payment a person with a wireless device could pay for items in a store or settle a restaurant bill without interacting with any staff members. According to orange Mobile Payment (Danish Company) the entire transaction should take not more than 10 seconds. In order to provide a secure and comprehensive m-payment, the payment scenario should be designed so that it performs fast and simple for the end-use, but secure and comprehensive for the provider. An efficient payment scenario takes efficient steps in performance. With rising new smart phones available in markets, the facilities of smart mobile device could be exploited to develop an application to perform required m-commerce operations.

Table 1. Adoption of m-payments: drivers and barriers

Drivers	Barriers
Offering added value for consumers	Complex value-chain with lack of co-operation
merchants, mobile operators, financial	Financial regulation

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

institutions and other participants in the ecosystem	Security/Risk (perception of security/risk)
	Cost
User experience, easy-to-use	Unavailability of a broad range of mobile payment capable handset
	Lack of interoperability/ lack of Technology standards

II MOBILE PAYMENT

Although e-commerce is not all about fund transfer, electronic payment (or e-payment), such as credit-card payment over the Internet, is still one of the most popular e-commerce applications. In other words, e-payment is one of the crucial parts of an e-commerce transaction in that the e-commerce transaction cannot complete without it. For example, an online book store which provides both electronic and physical books to its customers must have a supporting payment system available for its customers to transfer money to it. Therefore, each customer can complete the purchase which includes goods delivery (or commitment of goods delivery) and payment with the store in one transaction. Without the payment system provided, the customers are required to perform two sessions separately: one for the goods purchase and the other for the payment transaction. In particular, the payment transaction has to be performed by transferring money to the store's bank account directly.

Credit-card payment seems to be a simple method to make a payment for goods or services on the Internet because many people have credit cards and regularly use them to purchase goods or services in physical stores.

Alternatively, a payment method that is suitable for low-valued transactions is called *Micropayment"*. Most micropayment systems deploy low computational cryptographic operations and simple message passing in order to reduce operational costs. The examples of micropayment systems are Milli-cent [GMAG95], PayWord [RS96], and PayFair [Yen01].

Electronic payment in wireless environments introduces the term *\Mobile Payment"* which is defined as interactions among engaging parties in a payment system regarding a payment transaction where at least one engaging party is a mobile user.

III LIMITATIONS OF WIRELESS ENVIRONMENTS

Performing payment transactions in wireless environments mainly suffers from resource limitations of mobile devices and characteristics of wireless networks [RdS98, KSL03a, and WC01].

3.1. Resource Limitations of Mobile Devices

Mobile devices have the following limitations:

Computational capability of their processors is comparatively lower than that of personal computer (PCs).

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

They are operated using battery power compared to electric power in PCs. Therefore, they can stay operated for shorter period than PCs.

They have limited storage which affects available cryptographic algorithms applied to them.

A mobile device with the above limitations is not capable of performing high computational cryptographic operations such as public-key operations. Due to the low computational capability of mobile devices, completing a payment transaction on a mobile device takes longer period of time than that on a PC which has higher processing capability. Moreover, public key operations are required to have certificate verification processes which require storage on each mobile device to store public-key certificates.

3.2. Transaction Performance of Mobile Payment Systems

Performing electronic payment transactions over wireless networks raises

Concerns about security of the underlying payment systems. Ideally, both Traditional and wireless Internet should serve all applications, including making payment, with the same level of security. Moreover, mobile payment applications should be compatible with existing infrastructure of traditional electronic

IV MOBILE COMMERCE

Internet technology offers extensive ranges of services such as electronic mails, and one of the most popular services offered on the Internet is *Electronic Commerce"* (*or e-commerce*). E-commerce is becoming bigger technological wave that has changed the way by which business is being conducted.

Two main areas in which e-commerce grew significantly in recent years are Internet banking and conducting business on the Internet [Gho98]. With Internet banking, the way customers make use of banking services has changed. They do not have to go to ATM (Automatic Teller Machine) terminals or stay in-line at a bank branch to withdraw or transfer money between accounts, but simply log on to a bank's website which provides Internet banking services including withdrawing money from the customers' accounts. Although the customers cannot get physical cash in their hands, they are able to transfer money to electronic cards and bring them to purchase goods or services at stores. Customers are able to pay bills or schedule monthly bill payments by using the Internet banking services.

V MOBILE PAYMENT

Although e-commerce is not all about fund transfer, electronic payment (or e-payment), such as credit-card payment over the Internet, is still one of the most popular e-commerce applications. In other words, e-payment is one of the crucial parts of an e-commerce transaction in that the e-commerce transaction cannot complete without it. For example, an online book store which provides both electronic and physical books to its customers must have a supporting payment system available for its customers to transfer money to it. Therefore, each customer can complete the purchase which includes goods delivery (or commitment of goods delivery) and payment with the store in one transaction. Without the payment system provided, the customers are required to perform two sessions separately: one for the goods purchase and the other for the payment transaction. In particular, the payment transaction has to be performed by transferring money to the store's bank account directly.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

5.1. Mobile devices have the following limitations:

Computational capability of their processors is comparatively lower than that of personal computer (PCs).

They are operated using battery power compared to electric power in PCs. Therefore, they can stay operated for shorter period than PCs.

They have limited storage which affects available cryptographic algorithms applied to them.

VI CHARACTERISTICS OF WIRELESS NETWORKS

Wireless networks have the following characteristics:

- Wireless networks have lower bandwidth than fixed networks.
- Connections over wireless networks are less reliable since packet losses occur more frequently than that of fixed networks. Packets need to be retransmitted which may result in high latency.
- Connection cost of wireless networks is higher compared to that of fixed networks.
- Data transmitted over wireless networks is easily eavesdropped.

From the above limitations, mainly due to poor performance, performing payment transactions over wireless networks is time-consuming. Moreover, performing payment transactions on low computational capability mobile devices will spend longer time to complete each transaction. As the connection cost of the communications over wireless networks is much higher than that over fixed networks, performing payment transactions over wireless networks using such mobile devices will charge users a large amount of money on their bills. In addition, due to the fact that the data transmitted over the wireless networks is easily eavesdropped, this can be prevented by applying highly secure cryptographic techniques such as public-key operations. However, such operations require high computational capability devices and high-speed wire-less networks that may incur high cost for users.

Performing electronic payment transactions over wireless networks raises Concerns about security of the underlying payment systems. Ideally, both Traditional and wireless Internet should serve all applications, including making payment, with the same level of security. Moreover, mobile payment applications should be compatible with existing infrastructure of traditional electronic

Figure 6.2 demonstrates the directions of payment token transfer. *Payment Ordering* represents payment token transfer from *C* to *M*, even though, in fact, the actual transfer of payment token is processed from *I* to *A* in *Payment Clearing*. *Debit* represents the deduction of the value of the payment token from *C* to *I*, although, in fact, this action is performed at *I* itself because *C*'s account has been established with *I*. *Credit* represents money deposit from *A* to *M* even though, actually, this action is performed at *A* itself because *M* has an account established with *A*.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 06, June 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

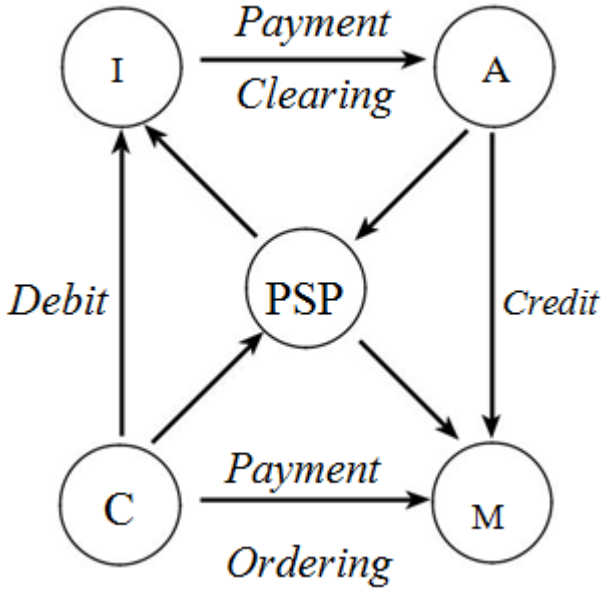

Figure 6.2: Payment transaction

Note that, from Figure 6.2, the arrows represent the directions of actual transactions. As *P SP* acts as a medium between *C-M* and *I-A*, all actual transactions relevant to *Debit* and *Credit* are performed through *PSP*. The broken arrows represent the directions of actions performed by originators of the actions to their intended recipients.

DETAILS OF THE PROPOSED FRAMEWORK

The proposed framework is composed of three main components:

Payment Protocol: the payment functionality of our framework can be performed by any kind of payment protocol, or even a fixed-network payment protocol. However, to achieve high transaction performance, a non proxy-based mobile payment protocol is preferred because it is designed to perform lightweight transactions.

Mobile Agent: the mobile agent in our framework performs the same task as the mobile agent in agent-based framework. That is, it performs transactions on the client's behalf. It contains payment-related information and travels to a foreign environment to generate the client's request for the particular payment protocol.

Proxy Server: to solve the problem of performing transactions in a hostile environment of agent-based framework, we set up a proxy server pro-viding a trusted environment where the client's mobile agent can use its processing capability to perform high computational tasks. However, following the trust relationships among engaging parties of the formal model, only *partial* trust relationships among parties need to be established between the client and the proxy server. In particular, the issuer is trusted by the client to store the client's information in order to reduce the storage requirement on the client's device, but the information stored at the issuer must not be suffcient for the issuer to impersonate as the client and to generate the client's request without any authorization from the client.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

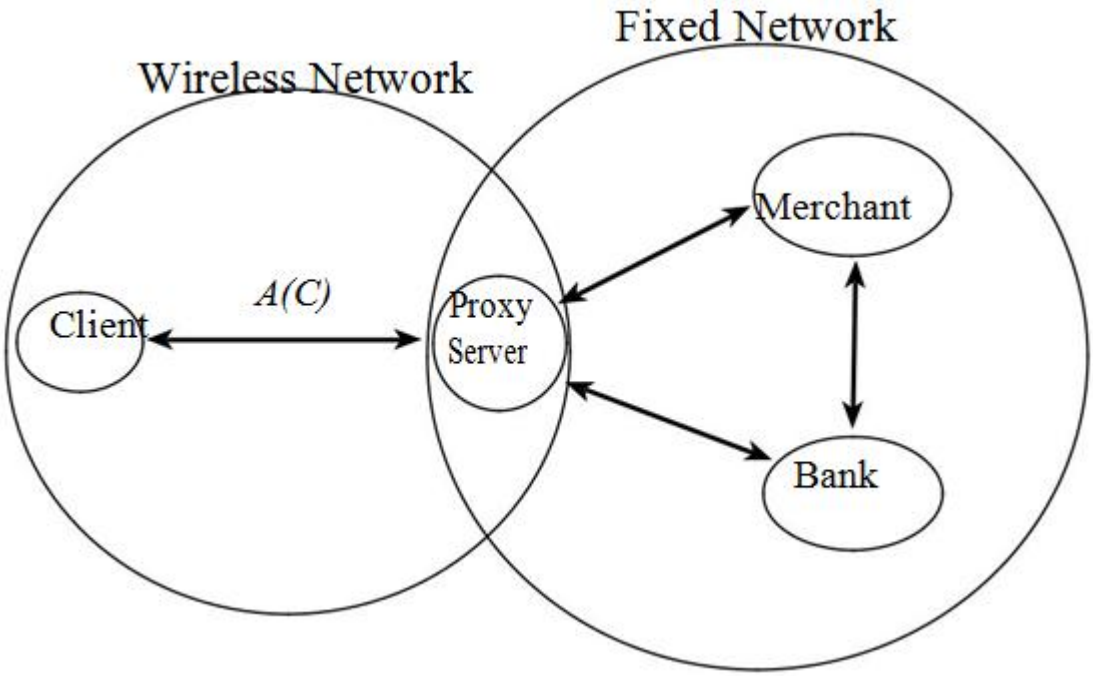

Figure 6.3: The proposed framework

The proposed framework is depicted in Figure 6.3. Note that *A*(*C*) stands for the agent *A* owned by the client *C*. From Figure 6.3, the client sends the mobile agent *A*(*C*), which contains the client's payment information, over a wireless network to the proxy server, where *A*(*C*) generates the client's payment request, located in a fixed network. After the request has been generated,

A(*C*) travels away from the issuer to perform the payment transaction following the particular payment protocol. At the end of the transaction, *A*(*C*) returns to the client with the result of her request.

VII CRYPTOGRAPHY CONCEPT

Cryptography is a technique used to secure data protection from the hacker, which can be classified into the following three groups:

- Symmetric Key Cryptography—It is the encryption methods in which both the sender and receiver share the same key. The algorithms, in general, consist of DES (Data Encryption Standard), 3DES (Triple DES) and AES (Advance Encryption Standard)
- Asymmetric Key Cryptography—It is also known as public key cryptography, a class of cryptographic algorithms which requires two separate keys. One key is secret and the other key is public. The algorithms are RSA (Rivets, Shamir and Adelman) and ECC (Elliptic Curve Cryptography).
- Hash Function—It is a public one-way function that maps a message of any length into a fixed-length, which serves as the authenticator. A variety of ways of a hash code can be used to provide message authentication.

VIII CONCLUSION

This paper gives an overview of mobile payments and analyzes the existing secure mobile payment protocol over the past 11 years. All protocol schemes focus on reducing the use of resources in the mobile process by

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

cryptographic concept. All protocols provided four main security properties: con-fidentiality, integrity, authentication, and non-repudiation. As a conclusion, to discover the best secure mobile payment protocol, the protocol standard must be the same all over the world and the communities and industries must be adopting the standard. In this paper we proposed a secure payment protocol, considering the restrictions of mobile networks in developing countries. The proposed protocol not only satisfies the convenience and ease of use that is generally required for mobile users in small payments, it also provides the transaction security level and non repudiation property that is necessary for macro payments. Although the proposed technique has been optimized for the current GSM network, but its modular design enables it to accept future improvements of the mobile network technology and infrastructure, such as EMS and MMS, with minimum change in the protocol structure

REFERENCES

1. McKitterick D, Dowlin J State of the art review of mobile payment technology. https://www.scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf
2. Fun TS, Beng LY, Razali MN (2013) Review of mobile macro-payments schemes. J Adv Comput Netw 1(4)
3. Singh A, Shahazad KS (2012) A review: secure payment system for electronic transaction. Int J Adv Res Comput Sci Softw Eng 2(3)
4. Ahamad SS, Udgata SK, Nair M (2014) A secure lightweight and scalable mobile payment framework. In: FICTA 2013. Advances in intelligent system and computing, vol 247. Springer International Publishing, Switzerland
5. Gowal, J., & Gowal, D. (2014). Design of Improved Algorithm for Mobile Payments Using Biometrics. *International Journal of Research in Engineering & Advanced Technology* (IJREAT), 1(6), 1-6.
6. Li Y, Wang Y Secure electronic transaction. http://people.dsv.su.se/*matei/courses/ IK2001SJE/li-wang_SET.pdf
7. Ally, A. (2014). The prospects and legal challenges posed by M-Payments and M-banking services in Tanzania. *Open University Law Journal*, 5(1), 49-57.
8. Isaac JT, Zeadally S (2012) An anonymous secure payment protocol in a payment gateway centric model. In: The 9th international conference on mobile web information system (MobiWIS). Elsevier
9. Sekhar VC, Sarvabhatla M (2012) Secure lightweight mobile payment protocol using symmetric key techniques. In: International conference on computer communication and informatics (ICCCI), pp 1–6, 10–12 Jan 2012
10. Tripathi DM, Ojha A (2012) LPMP: an efficient lightweight protocol for mobile payment. In: 3rd national conference on emerging trends and applications in computer science (NCETACS)
11. "certicom," [Online]. Available: http://www.certicom.com/index.php/an-introduction-to-the-uses-of-eccbased-certificates. [Accessed 01 01 2013].
12. "RSA Laboratories," RSA, [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2129. [Accessed 10 12 2012].