ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 2, No.8 , March 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Study of secure m-commerce, challenges and solutions

Ali Mirarab[1], AbdolReza Rasouli kenari[2]

[1] Qom, Iran
alimirarab@isca.ac.ir

[2] Electrical and Computer Department, Qom University of Technology
Qom, Iran
rasouli@qut.ac.ir

Abstract

With the development of mobile technology and the extensive use of intellectual mobile terminal, the mobile E-commerce has become a brand new method for the business activity for both individuals and enterprises. However, as the mobile E-commerce is in its infancy, its commercial environment is still not perfect and exist transaction security problems become a barrier in the rapid growth of mobile commerce subscriber. In order to make a way to select an appropriate solution to address M-commerce security problems, this survey completely focus on security issues in M-commerce and analyze the security requirements and important vulnerable of mobile e-commerce, existing security solutions are investigated in detail, the survey highlights important parameters and discusses the impact of the parameters on security, the survey identifies the open research issues regarding security and privacy in mobile e-commerce, and finally, state of the art taxonomy is presented.

Keywords: *Mobile E-Commerce, WPKI, WAP, e-Key, Double Layer Encryption, Double Encryption Model.*

1. Introduction

Mobile E-commerce is the B2B, B2C or C2C E-commerce which carries on mobile phones, PDA, handheld computers and other wireless terminals. It combines the Internet, mobile communication technology and other related technologies, so user's on-line activities will not be limited by time and space, thus, it will greatly facilitate user's life. With the development of mobile technology and the extensive use of intellectual mobile terminal, the mobile E-commerce has become a brand new method for the business activity for both individuals and enterprises. By combining the wireless network and E-commerce, suppliers can provide a more convenient and quicker service on a human scale for their customers. With the coming of the 3rd Generation mobile communication (3G) age and the progressive popularization of smart phones, M-commerce, M-banking, M-wallet and other mobile business is accelerating development.

The broadcast nature of the wireless communication and increased popularity of wireless devices introduce serious security vulnerabilities. Mobile users and providers must be assured of the correct identity of the communicating party; user and signaling data must be protected with confidentiality and integrity mechanisms. Mobile security architecture was divided into four levels: Network access security, Provider domain security, User domain security and Application security, as shown in Fig 1 [2].

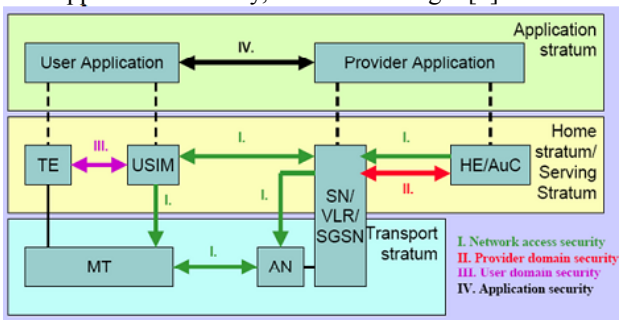


Fig. 1 Mobile Security Architecture [2].

Obviously, the mobile E-commerce which takes mobile phone as the major carrier has good prospects for development, and it becomes the research hot spot gradually. Mobile commerce still doesn't develop as people expected because the security is a key problem of different mobile commerce. However, as the mobile E-commerce is in its infancy, its commercial environment is still not perfect and exist transaction security problems need to be solved [4].

In this article we have tried to study the challenges and vulnerabilities of mobile E-commerce and analyze provided solutions to facilitate selecting appropriate solution for M-commerce Security. The rest of the paper is organized as follows. Section2 presents the Vulnerability Analysis of Mobile E-commerce Transaction System. Section 3 reviews M-commerce Security requirements. Section 4 deals with actual survey

of different security solutions that have been presented and published. Section 5 presents the parameters used to evaluate different security solutions for M-Commerce. The positive and negative aspects of security frameworks are illustrated in Section 6. Finally, Section 7 concludes our survey.

2. The vulnerability analysis of mobile E-commerce transaction system

In the whole transaction process of mobile E-commerce transaction system, there are three main unsafe factors which come from the mobile terminals, the mobile radio interface and the network-side [4].

2.1 Mobile terminal s unsafe factors

Mobile terminal's unsafe factors are mainly manifested in the user's identity, account information and authentication key and so on. For example, other people who get the user's mobile terminal are likely to fake the user's identity to do some illegal activities [4].

2.2 Radio interface's unsafe factors

As communication between mobile terminals and fixed network in wireless transmission relies on an open wireless interface to transmit, any people who have appropriate wireless device will have the opportunity to get the information through intercepting it over wireless channel, and even can modify, delete or re-transmit the information, which pose a threat to the trading activities [4].

2.3 The network's unsafe factors

The network mainly refers to wireless networks, gateways and cable lines. If the information is not protected when being transmitted in wireless networks, wired networks and converted by gateways, it is likely to be exposed causing a threat to the trading activities [4].

3. Security requirements analysis

When people use mobile commerce, their information must be transmitted through mobile Internet, including the customers' private information, the order information, and the payment information and so on. All these information should be kept secret for other people. Therefore the security transmission of the data and information is the important guarantee of safe mobile commerce. Security requirements in mobile commerce generally should include the following several aspects, each of these feature groups meets certain threats and accomplishes certain security objectives [5]:

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signaling data, and protect against attacks on the wire line network;
- **User domain security (III):** the set of security features that secure access to mobile stations;
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages;
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use.

4. Survey of M-commerce Security solutions

In this section, we present counter measure solutions that have been proposed to securing M-Commerce. A comparison and critical discussion on the proposed ideas will be detailed in section 6.

4.1 Mobile commerce security solution based on WPKI with Bluetooth

Pan Tiejun et al.[1] expressed that A WAP browser provides all of the basic services of a computer-based web browser but simplified to operate within the restrictions of a mobile phone, such as its smaller view screen. Users can connect to WAP sites: websites written in, or dynamically converted to, WML (Wireless Markup Language) and accessed via the WAP browser. By WAP, service providers had extremely rich opportunities to offer interactive data services such as: Email by mobile phone, tracking of stock-market prices, Sports results, News headlines and Music downloads. WAP adopts Wireless Public Key Infrastructure (WPKI) as security solution. WPKI is a two-factor authentication scheme using mainly the mobile phone and a laptop. It is mainly promoted by banks, mobile operators, and mobile network manufacturers. WIM (WAP Identity Module or Wireless Identification Module) is based on the WAP 1.2 specification enabling secure transactions and non-repudiation based on a digital signature, which has been support by some Smartphone with WIM slot. It is the core component to the mobile commerce security solution. But

WIM is not ordinary accepted by the Mobile operator in China, additional it is not compatible with the current a large mass of mobile phone. In order to solving this problem, we transform the WIM function into the Bluetooth earphone which can be widely accepted by the people.

Paper authors proposed a mobile commerce security solution based on WPKI with Bluetooth earphone that can be divided into following roles:

- Registration Authority - manages the user registration and customer care, usually acts on behalf of a Certification Authority;
- Certification Authority - manages activation, suspension and revoking of certificates;
- Trust Service Provider - acts as a central interface in WPKI infrastructure; main tasks include accepting authentication and signing transactions from Service Providers, passing requests to Mobile Operators and certificate and signature validity check;
- Service Provider - third party that is interested in authentication and/or digital signature of the user.

These roles in the above solution include:

- WIM Bluetooth (subroutines related to cryptographic functionality);
- Mobile phone (compatibility with GSM/UMTS standards);
- SMSC;
- OTA server;
- Mobile phone user interface (UI);
- Transaction interface (TI).

This solution has considered that only qualified certificates are used in WPKI implementations, therefore CA's are in charge of supervising RA's registration services conformance to local legal requirements [6]. Our mobile commerce security architecture model consists of WTLS (Wireless Transport Layer Security), WMLScript (Wireless Markup Language Script), WIM (Wireless Personal Identity Module), and WPKI (Wireless Public Key Infrastructure) as shown in Fig. 2. The core security component of WIM Bluetooth earphone is ESAM (Embedded Secure Access Module) connect Bluetooth chip via ISO-7816 protocol supporting WPKI security function which communicate to Smartphone by Bluetooth wireless connection.

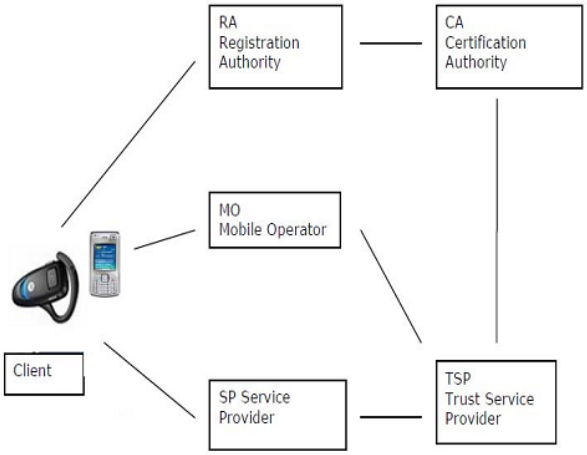


Fig. 2 Mobile commerce security solution based on WPKI with Bluetooth earphone [1].

The Bluetooth earphone plays the cryptographic token role in WPKI architecture considered by our solution because more and more Smartphone has the Bluetooth earphone which can be access by the application on J2ME, UIQ etc. platform. Additional Bluetooth standard give its own complete security solution which can be reuse by mobile commerce. The Bluetooth earphone contains a set of cryptographic primitives that allows producing some WPKI functionality. The minimum set of requirements for a WPKI Bluetooth earphone is to produce functionality which is similar to that of the "conventional" PKI smart-card:

- encryption of binary data with some low value cryptographic key Key-S
- encryption of binary data with some high value cryptographic key Key-N (used for non-repudiation signatures)

The first encryption function (that uses low-value Key-S) may be used in authentication applications and to create signatures that have no legal implications for the signer.
The second encryption function (that uses high-value Key-N) may be used in non-repudiation signing applications that produce artifacts with potentially legal implications for the signer. The Key-N may be routinely associated to the qualified certificate; the usage of this key has to be (obligatory) protected by some signing PIN code inside the Bluetooth earphone (no technical possibilities to invoke the usage of this key without making the user to input the signing PIN).

4.2 An advanced mobile security solution based on distribute key without changing hardware configuration of the mobile devices

Pan Tiejun et al.[2] present an approach in which the mobile security is enhanced by an isolated external

electronic security key (eKey) with a security enhancement mechanism. They propose an advanced mobile security solution and related security methodology based on distribute key without changing hardware configuration of the mobile devices. The solution consists of the UE (User Equipment), an electronic security key (eKey) which is connected to the mobile device by adaptable interface for enhancing the UE security ability and storing private data, CA with digital certification and web server which provides the M-commerce services. UE communicates with web server and CA via wireless mobile net and Internet. UE communicates with eKey via adapted interface (e.g., COMM, USB and Bluetooth). We provides M-commerce security procedure for application layer, which implements all kinds of mobile security services for the sake of convenience: User identification and administration (IMSI/ISDN/EID), AKA (Authority and Key Agreement), DI (Data Integrity), DC (Data Confidentiality), authentication information translation between eKey and web server etc. It is based on OOD technology, which provides compatible API with 3GPP security protocol, user can flexible configure the security service and main algorithms library according to different requirements. At the same time, it provides the concrete realization of the core algorithms clear defined of 3GPP. All algorithms are realized based on two core encryption modules: KASUMI and AES.

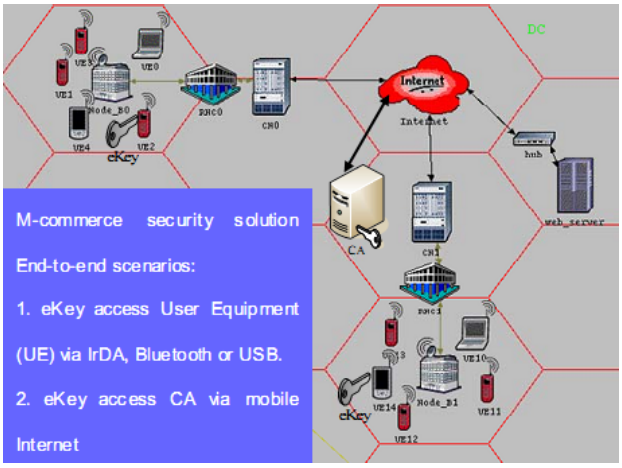
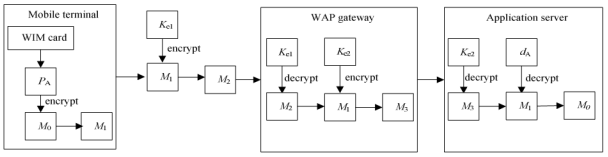


Fig. 3 Advanced mobile security solution based on distribute key without changing hardware configuration architecture [2].

In this mobile information security solution, the eKey has played a very important role. We have developed a practical project of the eKey to explore the technology feasibility of the solution. The eKey hardware design is mainly to solve the hardware encryption and anti-attack problems. As an external security device used for mobile phone, eKey should support Public Key Infrastructures (PKI) mechanism with Single DES, Triple DES, SHA-1, RSA arithmetic and X.509v3 certificates storage. Further, eKey should have high performance with low cost, power saving and tiny.

4.3 A double layer encryption scheme based on WAP for M-Commerce

Feng TIAN et al.[3] proposed a double layer encryption schemes based on WAP, in order to solve the problem of security gap in the transmission of mobile E-commerce information through WAP gateway, which combines with WAP security architecture and mobile E-commerce security architecture. The data is encrypted with the public key of application server on the mobile terminal firstly, and then the encrypted data is encrypted again with WTLS in the wireless network and TLS/SSL in wired networks, which realizes the double layer encryption transmission. The digital signature and verification based on elliptic curve cryptography are adopted in this system, which can fast verify the identity of both parties. This mobile E-commerce security system adopts a double layer encryption schemes in its data transmission and provides a safe transmission for its data. The security transmission process is as shown in figure 4.



P_A: the public key of application server; K_{e1}: the key between mobile terminal and WAP gateway; K_{e2}: the key between WAP gateway and application server ; M_0: the message sent by the mobile terminal send; M_1: the message encrypted with P_A ; M_2: the message encrypted with K_{e1}; M_3: the message encrypted with K_{e2}.

Fig. 4 Security transmission process in double layer encryption scheme based on WAP [3].

1) The terminal encrypts data message M0 to get M1 with the public key PA of application server, then encrypts M1 with the key Ke1, and gets M2, then sends M2 to WAP gateway.
2) WAP gateway decrypts the message M2 with Ke1 and gets the encrypted file M1.
3) WAP gateway encrypts M1 by TLS/SSL's key Ke2 and gets M3, then sends it to the application server.
4) The application server will decrypts M3 with Ke2 and get M1, then decrypts M1 with its own private key dA and gets the cleartext M0.

4.4 Improved double encryption model

Suzhen Wang et al.[4] proposed the solution of security vulnerability in mobile E-commerce based on the "double encryption model". In this model, each symmetric encryption algorithm, public key encryption algorithm

and message digest algorithm owned by mobile terminals and content servers has a priority, the most widely used algorithm has the highest priority; the second widely used algorithm has a second priority, and so on. First, mobile terminal sends a group of algorithms which have the highest priority to content server (rather than sent all of its algorithms to the server); the content server compares the algorithms sent by mobile terminal with its own algorithms by priority from high to low. As the high priority algorithm is the most widely used algorithm, the process of selecting matching algorithm between mobile terminal and server is easier than "double encryption model".

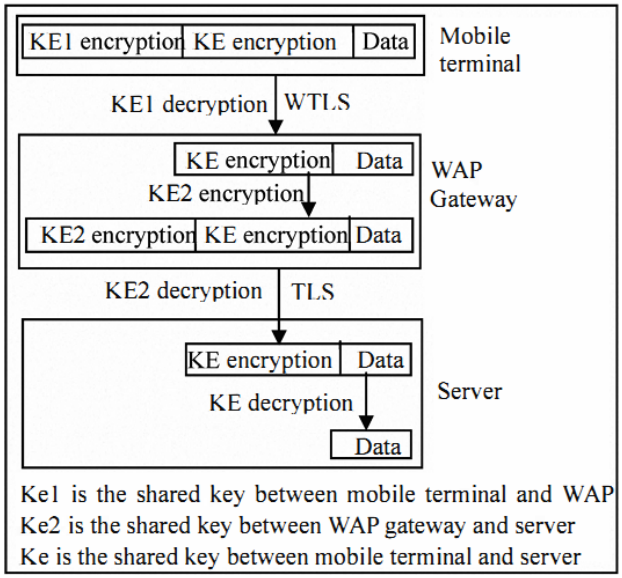


Fig. 5 Double encryption model diagram [4].

The transfer process is the same as that of double encryption model. The specific steps are as follows:

- Mobile terminal uses the security session key Ke to encrypt information, then encrypts the encrypted information with a shared WTLS key WKe1 between mobile terminal and WAP gateway, and then sends it to the W AP gateway.
- WAP Gateway uses Ke 1 to decrypt the information received. Because before data encrypted by Ke 1, it is also encrypted by Ke which shared by mobile terminal and content server, after the W AP gateway has decrypted the data, it's also cipher text, so that important information will not be exposed.
- WAP gateway uses the SSL / TLS key Ke2 to encrypt the information decrypted by W AP gateway with Kel, and then sends it to the content server.
- Content server receives information that WAP gateway has sent. The content server uses Ke2 to decrypt the received information first, and then use secure session key Ke to re-decrypt the information. Thus, the data which mobile device has sent is received.

Similarly, the content server can also use the same method to send encrypted information to the mobile device.

5. Evaluation criteria for M-commerce Security solutions

M-commerce Security solutions evaluation criteria will be described in this section. The analysis of mentioned automated requirements tools was necessary to define their common characteristics and way how they measure tools. Besides that the result of this comparison is a set of criteria that we believe are necessary for M-commerce Security By considering the importance of the aforementioned parameters (Section3) in M-Commerce. The criteria listed below are most common criteria that discussed in articles and researches [1][2][3][4] with considering all M-commerce security aspects:

5.1 Basic theory

The basic theory parameter specifies the basic building blocks of the discussed security solutions for M-Commerce. The basic building blocks may be mathematical or cryptographic principles. The basic theory parameter is included to identify the computational requirements of the discussed security framework solutions.

5.2 Uniform look and feel for users

No or minimal need to change the hardware and software configuration (in order to simplify user education and support).

5.3 User confidentiality

Inability to identify the recipient and the sender of the message by an Eve.

5.4 Mutual authentication

Also called two-way authentication, is a process or technology in which two parties authenticating each other suitably.

5.5 Data integrity

Maintaining and assuring the accuracy and consistency of sent and received data. The data integrity parameter identifies the consideration of the integrity verification issue in discussed security solutions.

5.6 Data confidentiality

Preventing the disclosure of data to unauthorized individuals or systems.

5.7 Easy implementation

No need to add any devices in WAP gateway, application server or system reconfiguration and change the configuration of the hardware.

5.8 High efficiency

The ability to function better and faster under the same sources, especially fit for the low calculating mobile terminal.

5.9 Small storing space

Small storing size for storing the key and parameters used in the solution.

5.10 High channel utilization

The ability to support high channel utilization by increasing the nodes.

5.11 Fast operation velocity

Velocity of both parts authentication, connectivity and encryption and decryption operations.

5.12 Cost reduction

Reduce the cost of encryption and decryption operations and consultations between mobile terminals and servers.

5.13 Authentication

Process of determining whether someone or something is, in fact, who or what it is declared to be.

5.14 Authorization

The process of validation user permission and privilege to M-commerce Services.

5.15 Anti-repudiation

The ability to ensure non-repudiation of information exchange (Non repudiation protects a sender against the false assertion of the receiver that the message has not been received, and a receiver against the false assertion of the sender that the message has been sent.).

6. Evaluation

All the solutions discussed under the category of Survey of M-commerce Security solutions have been presented in Table 1 chronologically. Each security solution has been evaluated with reference to evaluation criteria discussed in Section 5.

Table 1: Comparison of evaluated M-Commerce security solutions

	Mobile commerce security solution based on WPKI with Bluetooth[1]	**An advanced mobile security solution based on distribute key without changing hardware configuration of the mobile devices[2]**	**A double layer encryption scheme based on WAP for M-Commerce[3]**	**Improved double encryption model[4]**
Basic theory	WIM function with Bluetooth earphone	Distributed e-key	double layer encryption scheme	double encryption model
Uniform look and feel for users	Yes	Yes	-	-
User confidentiality	Yes	Yes	Yes	Yes
Mutual authentication	-	Yes	-	-
Data integrity	Yes	Yes	-	Yes
Data confidentiality	Yes	Yes	Yes	Yes
Easy implementation	-	Yes	Yes	Yes
High efficiency	-	Yes	Yes	-
Small storing space	-	Yes	Yes	Yes
High channel utilization	-	-	Yes	-
Fast operation velocity	Yes	-	Yes	Yes
Cost reduction	Yes	-	Yes	Yes
Authentication	Yes	Yes	Yes	Yes
Authorization	Yes	Yes	Yes	Yes
Anti-repudiation	Yes	Yes	Yes	Yes

Pan Tiejun et al.[1] proposed a secure solution which is based on WPKI with Bluetooth earphone. The user is generally responsible for managing his user names and PINS or passphrases When a PIN and passphrases identifies individuals, which could possibly vary from service to service. This requirement places too much of a burden on users who have multiple sets of user names with PINS or passphrases using all kinds of mobile commerce. In this security solution, the user accesses a certificate with a passphrase stored on a Bluetooth earphone. The certificate represents the individual as his or her personal identity throughout the session. Because users must remember only a passphrase, this approach is less of a burden for them than having to remember both a PIN and a passphrase; moreover, the safe solution based on the WPKI is much safer than PINS.

The aim of this security solution for WPKI transactions implementation is to ensure:

- Adequate security level (in order to achieve interoperability among applications);
- Uniform look and feel for users (in order to simplify user education and support);
- Flawless operation.

This security solution design using WIM Bluetooth earphone which can protect the message at the application layer, avoid the Security Gap problem to ensure end to end security. WIM Bluetooth earphone adopts hardware encryption techniques which is safer than software encryption and cheaper than Biometric Identification Technology.

Pan Tiejun et al.[2] proposed an advanced mobile security solution based on distribute key without changing hardware configuration of the mobile devices. The solution consists of the UE (User Equipment), an electronic security key (eKey) which is connected to the mobile device by adaptable interface for enhancing the UE security ability and storing private data, CA with digital certification and web server which provides the M-commerce services. UE communicates with web server and CA via wireless mobile net and Internet. UE communicates with eKey via adapted interface (e.g., COMM, USB and Bluetooth). M-commerce security is enhanced by using external security key and specified policies including user confidentiality, mutual authentication, data integrity and confidentiality. Furthermore, the design of eKey is given which put emphasis on the hardware security solution and the communication mechanism between main controller and security module. In this way, the M-commerce security problem is solved to a certain extent.

Feng TIAN et al.[3] We adopt the encryption schemes based on the double layer which has realized the safety transmission in mobile E-commerce. The connection between smart card and encryption calculation on elliptic curve cryptography makes up for the defects of low calculation on mobile terminal, quick to produce the key pair and achieve the data encryption, decryption, digital signature and the verification. System performance analysis show that this solution satisfy following characteristics:

- High security: The adoption of double layer encryption schemes, on one hand, solves the security problem thoroughly exposed in the WAP gateway data information decrypting and the encrypting process; on the other hand, the ECC public key system is obviously superior to RAS&DSA.
- Easier implement for the system: This plan does not need to add any devices in WAP gateway, application server or system reconfiguration, but only a WIM card.
- High operating efficiency: ECC is much faster than RSA and DSA for its application of elliptic curve crypto under the same resources, especially fit for the low calculating mobile terminal.
- Small storing space: The storing size for ECC's key and system parameter is much smaller than RSA and DSA. 160 bits' ECC has the same security extension with 1024 bits' RSA and DSA, and 210 bits' ECC the same with 2048 bits' RSA and DSA, which is specially designed for relatively small storing devices, such as WIM.
- High channel utilization factor: Utilization factor of data acceptance in WAP gateway's wireless channel shows the obvious increase in utilization factor with the increase of nodes.

This system has characteristics of high security, fast calculation speed, high channel utilization factor etc., which can meet the safety need of WAP mobile E-commerce.

Suzhen Wang et al.[4] proposed an improved security solution on the WAP gateway based on the "double encryption model". This solution can reduce the communication cost of the encryption consultations between mobile terminals and servers, shorten the time internal of consultations, and increase the connection speed and security degree in mobile E-commerce transaction. This solution has built a secure channel between mobile terminal and content server because the data is protected in the whole process of transmitting, so the solution has solved the weak point that the WAP gateway be able to see clearly of the message. This solution only needs add encryption/decryption functions at the application layer, does not require hardware-level changes, so it is easy to implement. Security analysis of

the Improved Double encryption Model shows that this solutions includes:

- Data integrity. To transfer data, we use the WTLS protocol between mobile terminal and WAP gateway, and TLS / SSL protocol between W AP gateway and content server; both protocols use a message authentication code mechanism to ensure data integrity.
- Data confidentiality. In the program only mobile terminals and the content server can see the message clearly, so it can ensure the confidentiality of the data.
- Status authenticity. The program uses authentication technology to ensure the authenticity of the identity of the transaction parties.
- Anti-repudiation. The program uses digital signature in the exchange of information to ensure non-repudiation of information exchange.

7. Conclusions

The survey critically investigates different security solutions proposed for the M-Commerce. Most of the discussed security solutions tried to fix security flaws in WPKI and WAP gateway and also reduce the burden on the user and mobile devices.

The combination of e-commerce and mobile devices, providing anytime and anywhere access. Despite of benefits that provided in e-commerce by mobile devices, due to broadcast nature of the wireless communication, it is required to deal with new security threats.

The most challenging aspects in M-commerce are the security transmission of the data and information and providing E-commerce transactions security that uses mobile terminal. To provide a secure M-commerce environment, service providers need to address issues pertaining to data security, network security, data integrity, application security, data access, authentication, authorization, data confidentiality, data breach issues, and various other factors. To achieve a secure M-commerce environment, security threats need to be studied and addressed accordingly.

References

[1] P. Tiejun, Zh. Leina, "New Mobile Commerce Security Solution Based on WPKI," 2012 International Conference on Communication Systems and Network Technologies, Rajkot, pp. 485-488, May 2012.

[2] P. Tiejun, Zh. Leina, F. Chengbin, H. Wenji, F. Leilei, "M-commerce Security Solution Based on the 3rd Generation Mobile Communication," 2008 International Symposium on Computer Science and Computational Technology, Shanghai, pp. 364-367, Dec. 2008.

[3] F. Tian, H. Xiao-bing, Y. Wei, " Study of WAP Mobile E-commerce Security on WPKI," 2009 Second International Symposium on Electronic Commerce and Security, Nanchang, pp. 3-6, May 2009.

[4] S. Wang, L. Fan, "A solution of mobile E-commerce security problems," 2010 2nd International Conference on Education Technology and Computer (ICETC), Shanghai, pp. 188-192, June 2010.

[5] 3G TS 33.102:"3rd Generation Partners Project; Technical Specification Group Services and System Aspects; 3G Security; 3G Security Architecture".

[6] WAP Forum. WAP 2.0 technical white paper [EB/OLJ. http: //www.wapforum.org/what/technical.htm. 2002- 01.

Ali Mirarab received the M.C.S. degrees of Information Technology. He passed BA has in Tehran University in field of IT engineering. His research interests are in various aspects of IT fields especially security and cloud computing.

AbdolReza Rasouli Kenari received the Ph.D. from UTM in 2011 and M.C.S. degrees from the Islamic Azad University in 2006 in Computer Engineering. He is currently Head of Graduate Studies at Qom University of technology. His research interests are in various aspects of data mining and security.