Analysis of Enhanced Encryption and Pin Distribution in Online Mobile Transactions

[1]Ms. Rajarajeswari, [2]Mr. K.Shanmugam[3]N.Singaravelan
[1]Assistant professor, [2]Assistant professor, [3]
Department of CSE, Arulmiu Meenakshi Amman College of Engineering, kancheepuram, India

Abstract- **Mobile E-commerce had seen drastic development in the last few years. But till now it raises a number of security and privacy challenges. This paper proposes an advanced mobile security system and methodology to provide a secure m-commerce transaction. This can be achieved by using a more secure WAP gateway which employs "double encryption model". Further the use of verification by adopting the distributed PIN technology will make it more secure and reliable one. WTLS and SSL/TLS protocols use a message authentication code (MAC) technique to provide the data integrity. In our proposed work two different session keys K1 and K2 are generated using the M-AES 256 bit algorithm. Even though all these technologies have been separately implemented, the use of all these together will strengthen the security in M-Commerce on a much larger scale.**

Index Terms— Mobile e-commerce, Distributed Pin, "double encryption model", WAP gateway, M-AES 256 bit encryption.

III. INTRODUCTION

M-Commerce is defined as any electronic transaction, information; interaction conducted using a mobile device and networks that leads to transfer the real or perceived value that is exchanged for goods, service or information. Airline ticket booking, purchasing movie tickets, gold and ornaments etc.Thus mobile e-commerce which takes mobile phone as major carrier has good prospects for development and it becomes the research hot spot gradually. However the limited resources of a mobile device like small memory and lower computational load should be use effectively, the mobility of devices amplifies the chances of losing the device and data. So, user prefers m-commerce applications which do not require strong and processing of sensitive data on mobile devices. Network centric aspects like channel threats and radio interface risks are to be considered. For all these key issues of interoperability, visibility security and privacy still need to be addressed. The three basic security components are:
1. Customer Data: Protecting valuable and sensitive information about customers i.e., their personal data.
2. Architecture: The network architecture and the mechanism of communication should be protected from being attacked.
3. Transaction: Most important the parties involved in the transaction, their data, identity, authentication etc. should be maintained confidentially thereby providing acceptance level of security.

A. Need for M.COMMERCE – Applications Mobile commerce is growing faster than expected, with the growth in technology; people are getting adopted easily to the mobile world. Important fields of M-Commerce Applications

1. Inventory Management
2. Advertisements
3. Financial Transactions
4. Location and search of a product
5. Entertainment
6. Auction or Reverse Auction etc.

B. For a best M-Commerce Application:

Every M-Commerce application should meet the basic requirement which includes minimalism and manageability with a strong security and single sign on. All these will make even the common people become more familiar with M-Commerce.

Thus this paper deals with wireless link threats in commerce transactions, it analysis the mobile e-commerce transaction system's vulnerability and proposes the improved security solution on gateway using technologies like distributed pin and double encryption model..

II. LITERATURE SURVEY

There are many techniques and algorithms used for secured transactions in mobile commerce. Algorithms like Rivest-Shamir -Adlemen (RSA) algorithm, Advanced Encryption Standard algorithm (AES), Data Encryption Standard (DES) algorithm.Steamcipher algorithm (RC4) is better than Block Cipher algorithm (DES, AES, and RSA).
There are many techniques available in literature. A few techniques are listed below

A) 2D-barcode techniques:

Existing techniques of the 2D-barcode [4] increases the security in mobile payment transaction and ordering of the goods in secure way. Another advantage of the 2D-barcode is customers and mobile users can easily extract all related product information from 2D-barcode and reducing the user inputs. The limitations in this technique are Merchant authentication is not provided. The customer details, pin and account number, and payment information are stored in customer mobile phone. So in the case of mobile theft it can be easily identified by the intruder.

B) Biometrics technique:

Existing biometric techniques used for user authentication is unique [5]. User authentication is achieved by mobile device. The main advantages of this technique are as both users and service provider recognizes without an additional device. By merits of using (ECC) for encryption method are, the process is small, efficient and requires low power. The Limitations in biometric techniques are, as it uses only encryption method for user and payment details for secure transfer of the data. By not using a security conversation mechanism such as WAP gateway data are not more secured. No Merchant authentication is available in this technique. The limitations of using ECC consists of, difficulty in counting the number of points on the curve and generating suitable curves. ECC is not yet fully understood and relatively has slow signature verification.

C) SET technique:

The Secure Electronic Transaction (SET) [7-8] is an open protocol specification developed for credit card transactions over internet. Some Limitations of this technique are attacks can be made over wireless network by means of sniffing. The entire PIN can be obtained if the external network is cracked. Problem in managing limited resources.

II. EXISTING SYSTEM:

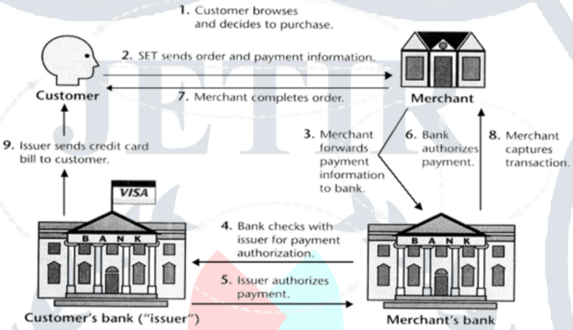
1. Customer browses and decides to purchase.
2. SET sends order and payment information.
Customer
7. Merchant completes order.
Merchant
9. Issuer sends credit card bill to customer.
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
VISA
BANK
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
BANK
Customer's bank ("issuer")
Merchant's bank

Figure 1. Existing System

A. Problems in Existing System:

1. Attacks can be made over wireless network by means of sniffing
2. Manageability problems due to limited resources.
3. The entire PIN can be obtained if the external network is cracked**.**

III. PROPOSED WORK

A) Double encryption model:

Mostly for secure data transfer, only encryption is done for user and payment details and no secure conversation mechanism was used. This leads to the proposed model. In the proposed model re encrypt the data in the Application-level, so that data exposure to WAP gateway is still being encrypted and protected [11].

The proposed architecture is as shown in Fig. 2.

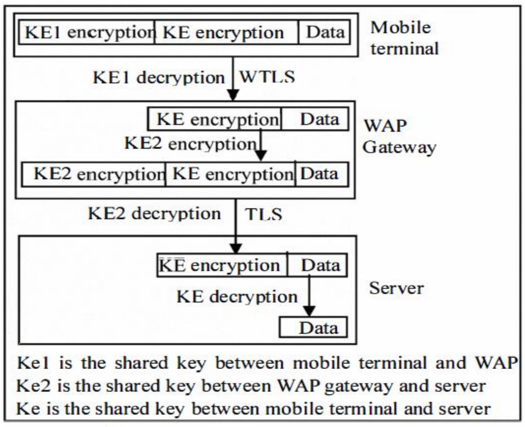

Fig. 2 Proposed Architecture (Double Encryption Model).

B) Double encryption model:

Reference [8]. The idea of this model is: re-encrypt the data in the Application-level, so that data exposure to WAP gateway is still being encrypted and protected. When the mobile terminal and content server are connected, a number of mutual authentication are processed to produce the session key and other parameters which only mobile terminal and content server know. Then use key to ensure end to end security between mobile terminal and content server, and the integrity of the other parameters.

This also encounters the following problems [6].

1. It ignores consultation of the encryption algorithms and digests algorithms between content server and mobile terminals, in the process of producing session key, so it is difficult to ensure the session key is generated by the same algorithm.

2. Transmitting data between mobile terminal and content server need digital signature every time, it is a heavy burden to mobile terminal since its computing power is not high.
However the advantage here is that transmitting data between mobile terminal and content server need digital signature every time, it is a heavy burden to mobile terminal since its computing power is not high. The short comings are as follows.

(1) It needs mobile terminal distribute all the symmetric encryption algorithms, public key encryption algorithms and message digest algorithms to content server in the process which mobile terminal and the content server consult the encryption algorithm and digest algorithm,

(2) Server compares each algorithm with its own algorithms one by one after receiving the variety of algorithm which the mobile terminal has sent. which also requires a large volume of work,

(3) It is necessary to increase a selection process, if the compatible algorithm between server and mobile terminals isn't unique, which also increases the workload. The improvements made for the problems are [6]-First, consulting the encryption algorithms and digest algorithms between content server and mobile terminal, then consult session password, and then use this session key to encrypt communication data. The consultation process of the encryption algorithms and digest algorithms is: mobile terminal distributes all of its encryption algorithms and digest algorithms to content server, the server compares each algorithm with its own to select a group of compatible encryption algorithms and digest algorithm and distributes them to mobile terminal and store them for its own use.

C) WAP server-Transparent gateway model:

The idea of this model is to make W AP gateway receive the encrypted WTLS information flow, and it directly sent it to the content server without decrypting it [7]. As a result, W AP gateway cannot see the raw information, so the gateway will not disclose the sensitive data. To solve the vulnerabilities of mobile e-commerce with this model, WAP gateway is still needed to solve the wireless access problem. But updating the server so that it can resolve the WTLS protocol, hardware-level changes are still needed on the server.

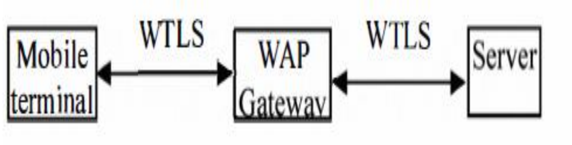

Figure 2. Transparent Gateway Model

IV. PROPOSED SYSTEM:

1. The customer navigates the merchant’s site.
2. Customer chooses the product and places the order to the merchant.
3. (A) Merchant authenticates himself to the third party.
(b) Third party approves merchant authentication.
(c) Third party informs the customer that this merchant is authenticated.
4. (a) Customer sends the payment details along with his pin (one half of the pin) which is encrypted and is sent to authentication server through WAP gateway.
(b) Customer sends the payment details and other half of the pin (encrypted through WAP gateway)

5. (a) The encrypted PIN travels through the WAP Gate where double encryption is done to save the PIN from intruders to the authentication server.
   (b) The other half of the distributed PIN is sent to the external serve through the WAP server where again double encryption is done.
6. After the PIN reaches both the server, each of it is checked and once it is authenticated by both the server, an OK signal is sent from the external server to the authentication server.
7. Then the required details are sent to the third party.
8. (a) The third party connects to the corresponding bank for authorizing payment.
   (b) The acquiring bank treats the demand and respondents to third party.
9. The response and all details about transactions are stored by the third party.
10. (a) Third party now sends the payment reference and other details to the customer.
   (b) Third party sends the response to the merchant.
11. The third part makes all the payment transaction.
12. The merchant receives the payment from the acquiring bank.
13. The merchant delivers the order.

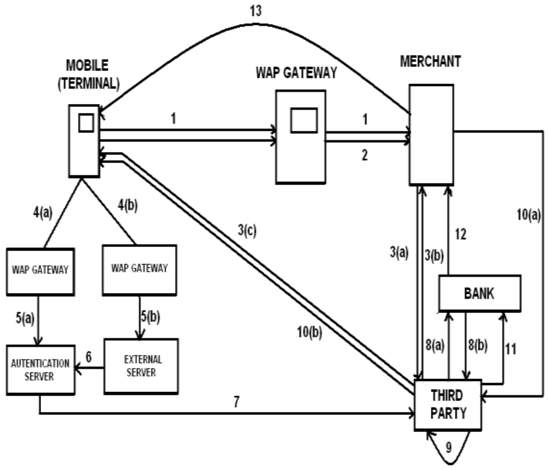

Figure 3. Proposed System.

A. DPIN verification:

The PIN given by the customer is divided into two halves (P1 and P2). Two different session keys K1 and K2 are generated using the AES algorithm. P1 is encrypted using the key K1 and P2 is encrypted using key K2. The mobile application then obtains the public keys of the two servers which are to authenticate the customer – the Authentication server and the External Server. The encrypted PIN half P1, key K1 and the Credit-card number are all double encrypted together with the public key of the Authentication server through the WAP gateway. Similarly, the encrypted PIN half P2, key K2 and the Credit-card number are all double encrypted together with the public key of the External server through the WAP gateway. These encrypted data are then sent to the respective servers for verification. The Authentication server checks its half of the PIN and obtains the result. It waits for a response from the External server. The External server verifies its half of the PIN and sends the response to the Authentication server. The Authentication server, only on assessing the results of both the verifications will approve the authenticity of the customer.

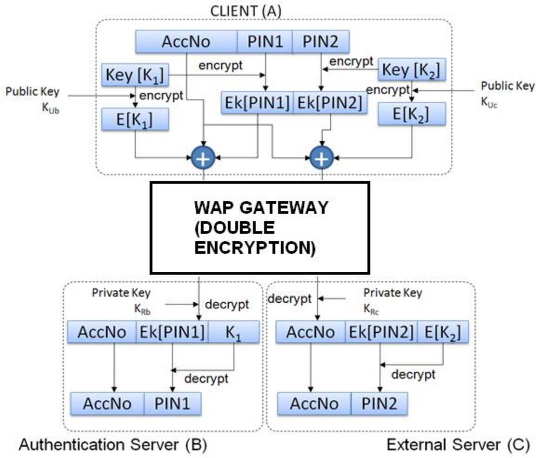

Figure 4. DPIN Verification Process

B. *Authentication of merchant and customer to third party:*

When the transaction merchant authenticates himself to the third party. The authentication takes place as below.
1. The customer sends his ID and timestamp value to the merchant.
2. The timestamp value and ID is forwarded by the merchant.
3. After generating the key Kab third party finds the A’s profile and sends the other information to the consumer.
4. Consumer extracts the key and calculates the hash code after receiving the information.
5. Consumer completes the authentication process once the calculated hash code is correct.

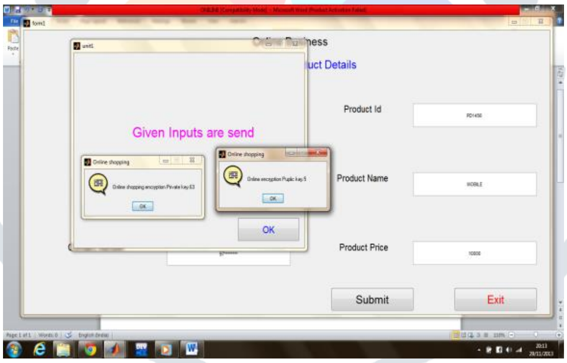
Online Business
Product Details
Given Inputs are send
Online shopping encryption Private key 63
Online encryption Puplic key 5
Product Id: P01456
Product Name: MOBILE
Product Price: 10000

Figure 5. Merchant Authentication (simulated output).

SHA hash function is computationally infeasible to find a message corresponding to the given message or to find two messages that produce same message digest, thus providing more security to the authentication process. Any change to the message will result in a different message digest. This results in a failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm.

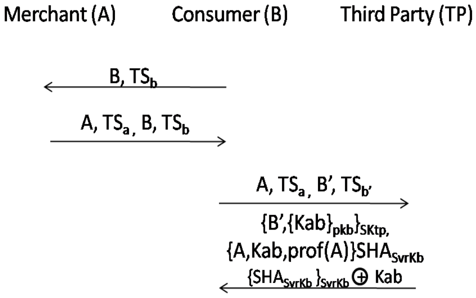

Figure7, Merchant Authentication

C. *Benefits of the proposed model:*

1. The use of double encryption helps to build a more secure channel between mobile terminal and content server. This solution has solved the weak point that the WAP gateway to be able to see clearly of the message.
2. The encryption PIN is not stored in the mobile, this will ensure that even in the case of mobile theft, the PIN is not identified by the intruder.
3. Here is no need of any special hardware to be added to the mobile, since there is priority communication cost of the encryption consultations between mobile terminals and servers increases connection speed and security degree in mobile commerce transactions.
4. Data Integrity is ensured due to WILS protocols between mobile terminal and WAP gateway, TLS/SSL protocol between WAP gateway and content server. In these two message authentication code mechanism is employed.
5. Dated confidentiality due to distributed PIN is ensured. The PIN is divided into two parts and sent Even if the intruder with the succeeds to trap one half of the PIN, it becomes copious to crack the other half of the PIN simultaneously. The cracking of the entire PIN becomes extremely difficult and a tedious process providing enhanced security to this system. Further only the terminals and content server. Can see the message clearly.

6. Merchant authentication: This process gives full satisfaction to the customer. It is simple since it uses SHA to calculate message digest. Thus it is highly efficient and effective.

VI. CONCLUSION:

With all the limitations of mobile device, the usage of distributed PIN for the purpose of verification and merchant’s authentication makes the communication highly effective and provides immense security, thereby assuring the customer that the transaction is carried out with the right person. To add on with this the introduction of a more secure WAP Gateway which involves the “double encryption model” to another key point to ensure the safety and reliability of the mobile e-commerce transactions? When compared to the previously proposed architecture, it serves to provide a high level security because at each stage a more enhanced mechanism is introduced to ensure a complete reliable and secure transaction.

VII. REFERENCES

[1] T. Karygiannis, NIST, Computer Security Division, karygiannis, Wireless Network Security802.11, Bluetooth™, and Handheld Devices March 25, HPCC, 2003.

[2] LI Xi, HU Han-ping “A secure mobile payment system” Institute of Pattern Recognition and Artificial Intelligence, Hashing University of Science and Technology, Wuhan 430074, China.

[3] Scarlet Schwiderski-Grosche, Heiko Knospe SECURE M-COMMERCE.

[4] Suresh Chari, Parviz Kermani, Sean Smith, Leandros Tassiulas. Security Issues in M-Commerce: A Usage-Based Taxonomy 2001.

[5] Jianqi Cui, DanLin Yao,” a new security solutions on WAP-based mobile e-business, computer application research”, September 2007, pp. 99-lOl

[6] Xiangdong Hu, Qinfang Wei, Jiqing Xian, Ping Wang, “WAP security implementation of the new type of cryptographic algorithm, computer application research”, 2002, pp.19-22

[7] Dongmei Wu, based on wireless application protocol, “a new end to end security model”, Chang'an University: Natural Science Edition,2005, pp.117-120

[8] T.D.B Weerasinghe, Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms, International Journal of Information & Network Security (IJINS) Vol.1, No.2, June 2012, pp. 77~87.

[9] Neetesh Saxena, Narendra S.Choudhari, “EasySMS: A Protocol for End-to-End Secure Transmission of SMS”, IEEE TRANSACTIONS ON INFORMATION FORESENICS AND SECURITY, VOL. 9, NO. 7 JULY 2014.

[10] JESUS TELLEZ, SHERALI ZEADALLY, “SECURE MOBILE PAYMENT SYSTEMS”. IT PRO IEEE Computer society, 2014.