Anita Maheshwari / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue4, July-August 2012, pp.2003-2007

Two Way Authentication Protocol For Mobile Payment System

Anita Maheshwari

Abstract

In Two Way authentication technique use a best approach for secure web transaction. It uses a TIC code it is called transaction identification code and SMS it is called short message service both provide the higher security level. TIC is a OTP (one time password) technique and issued by bank or other financial institution to the user or person who is access to the web services. In this technique uses a encryption / decryption method. It is a very complicated algorithm. . This method keeps the TIC as a secret code on cell phone. Bank provides the TIC list to the user cell phone .The user can easily pick up the TIC form the stored list of TIC. . To keep the TICs secret we store our TICs list in an encrypted manner and decrypt it at the time of requirement. This code is used to initiate secure web transaction using cell phones. Then after two ways authentication technique is involved that authenticate both the user who involved in transaction.

I. INTRODUCTION

Set is secure electronic transaction .it design to protect credit card transaction through internet It provide the security and authentication by registration. Set protocol permit user or customer who wants to make credit card payment to any of the web based services. It is a useful protocol for message exchanging between three parties: cardholder, merchant, payment gateway.
.

Some pseudo –code is used in this protocol-

C ⟶ M : initiate request

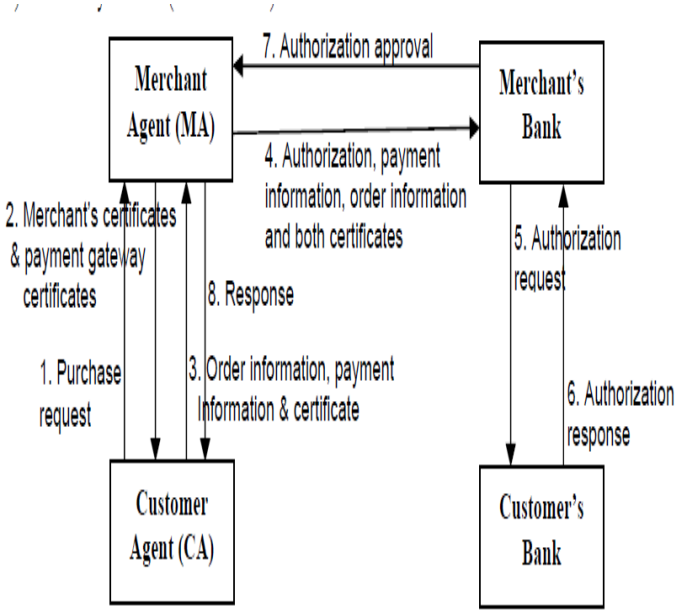
M ⟶ C : initiate response

C ⟶ M: purchase request

M ⟶ p: Authorization and capture request

P ⟶ M: Authorization and capture response

M ⟶ C: purchase response



SET Based Transaction Protocol

This diagram define working of the set protocol.-

1) Purchase request:-According to the diagram In this step customer Agent visit the Merchant website and select various items for purchasing and get total cost according to the selected items.
2) Merchant certificates & payment gateway certificates:-in this step merchant ask for payment method & customer choose credit card through set protocol.
3) In this step digital wallet is invoke and give list of credit card to customer for choosing card. and customer select one credit card,
4) Customer selects the one credit card from the list of credit card. After that merchant sends all payment information to the merchant bank for customer
5) Merchant bank send all information to the customer bank for authentication purpose. After that customer bank check all the information to own database. And also check it is a valid user or not.
6) After completed all checking process customer bank send authorization response
7) Merchant bank send the message of authorization approval to the merchant Agent.
8) After that confirmation message received to the customer your order has been processed.

Some disadvantage of set protocol is:-

1) Set is only design for wired network. It not support fully wireless network.
2) Set is end to end security mechanism which means it requiring traditional flow between customer and merchant.
3) All the transaction is flow from the customer to merchant so that it increases the risk of middle attacker. So that at the middle all information can be copied.
4) No one notification received from the customer bank to the customer after successful transaction
5) Set protocol is only for card based not support account based payment system.

So that we use a two way authentication protocol

TWO WAY AUTHENTICATION APPROACH

Introduction:- secure electronic transaction is a one way authentication technique so it increase lots of risk that way use one more approach is called multifactor authentication technique .it is a secure wed transaction it also include the cell phone in this transaction.

Multifactor Authentication Technique:- This process use the two authentication techniques

a) TIC (Transaction Identification code)

b) SMS

TIC Authentication Technique

It is a Transaction Identification Code used to identify both the user which is involve in this transaction. It is identify the transaction has been initiated by the valid user or right person.

- TIC codes are issued by the bank .
- It is combination of numeric or alphanumeric characters.
- It is randomly generated number. it is 8 bit or 16 bit number which is assign to user or customer.
- It is like a one time password which means one TIC code used only one time during transaction
- It is unique code.

In this process we are assuming bank are responsible to store TIC generation logic and they are also responsible the complexity of TIC code .bank are responsible for keep TIC as a secret. Bank also provide the list of TIC code to the customer or user. The Bank or Financial institution will keep a record of issued TIC codes to its customers and match the same code during the online web transaction. A TIC code is cancelled after each successful transaction.

2. SMS Authentication

Bank stores the customer phone number to provide sms confirmation to user during transaction. We assume that user will carry his cell phone or receive sms. After getting sms user also send the response (YES or NO) . when user send YES which means he is a valid user and he want to access the information & when user send NO or does not send any response to web server which means it is not a valid user and transaction will be terminated.[1]

Architecture for secure web transaction

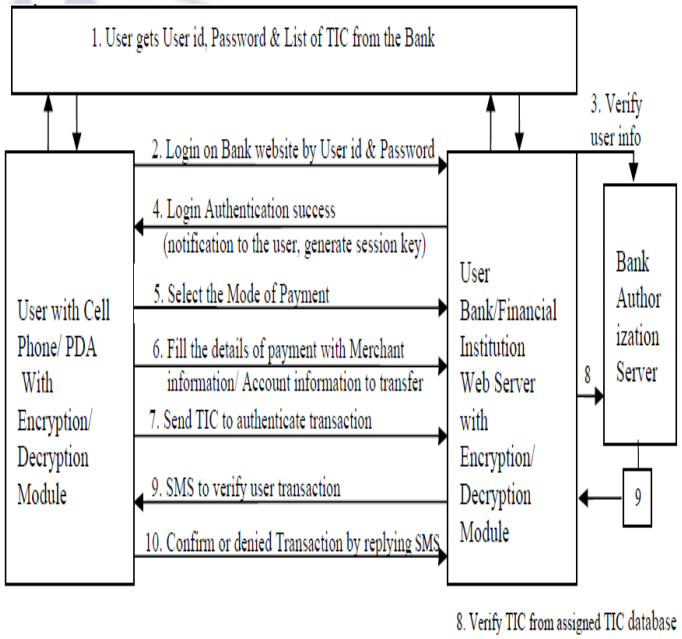


Figure describes the protocol which is start with the money transaction by the user. We assume that all the information which is related to user is store in the wed server database like user cell number, account information etc.

According to this diagram many steps are done during transaction:-

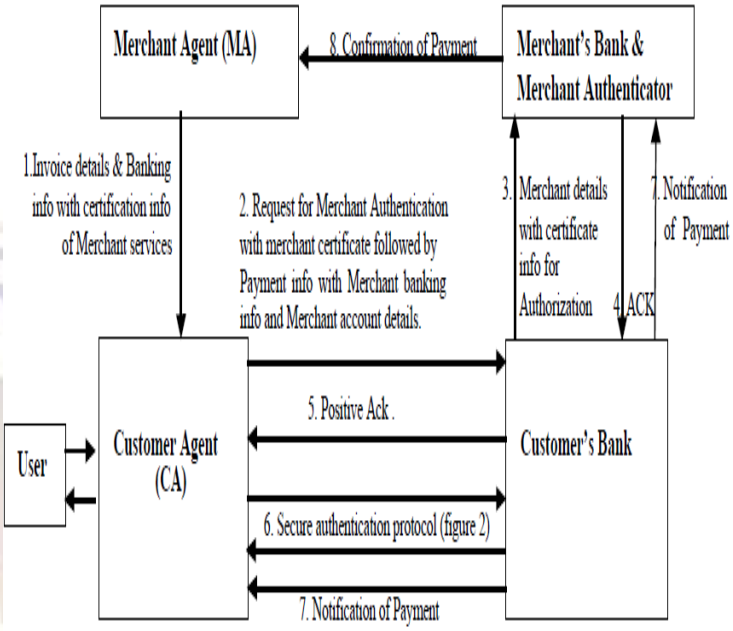
1) Firstly User gets the username, Id, list of TIC from the bank. Each user has one account which is receive from the bank authority and receive TIC list from the bank authority. This list is encrypted through proper encryption algorithm. After that user select one TIC code from this list. This TIC code is unique in each transaction.
2) User gives username and password to bank website for authentication. It is a login process
3) User information sends to the bank authorization server for verification. When user is a valid user then he receives the message from the server side.
4) User receive the login authentication success message from web server and web server also generate the session key and send to the user

5) The user will select mode of payment. We have consider two modes of payment: Credit Card based system & Account based Electronic transfer.
6) User will insert the details of payment by filling in a simple form with details such as merchant's bank and branch code information, invoice number and account number to which an amount has to be transferred. .
7) The user will insert a TIC code by choosing a TIC code from the stored list of TICs. This TIC are stored with encrypted manner after that user will decrypt and send the TIC to the bank through the transaction after that this TIC code send to the bank authentication server. This TIC match to the list of TIC which is issued TIC the user/customer. AES encryption method is used in TIC encryption process.
8) Bank authentication server decrypt the message and receive the TIC code and match to the list of TIC which is issued to the user when both TICs match bank cancel the user TIC from database. If no TIC matches then send error message to the user.
9) Bank server generates an acknowledgement to the user, which makes use free to logout from the web portal and wait for a confirmation SMS or to initiate another financial web transaction.
10) After complete this process the authentication server will send an SMS to the user's cell phone to verify the transaction
11) The user would confirm their initiated transaction by choosing "YES" or deny it by choosing "NO" by replying confirmation SMS[1]
12) The server will notify the user by a Message to acknowledge the successful completion of transaction or declination of the transaction.

TWO WAY AUTHENTICATION SYSTEMS

It is a system for two way authentication it describes the five major components:-

1) User : user is a valid account holding customer of the bank
2) Customer Agent (CA): it is software which is installed into user mobile device.
3) Merchant Agent (MA): it is a online service provider so that user can perform online transaction and purchasing through merchant agent.
4) Customer bank : this is the bank at which the user has a valid account
5) Merchant bank : this is the bank at which merchant has valid account [1]

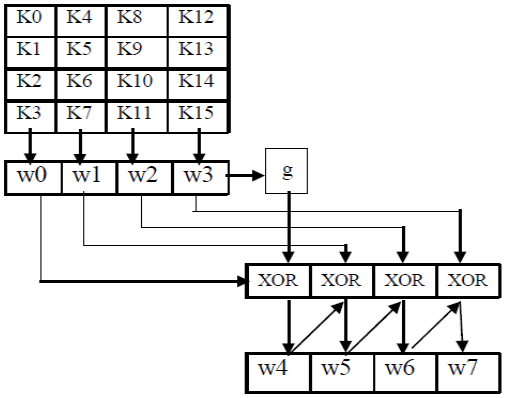


CRYPTOGRAPHY AND KEY AND SESSION MANAGEMENT

Encryption is the process for translating plaintext into codable form which is called cipher text to make it unreadable form to anyone. So that it is used to provide secret information. Cryptography is very essential aspect for secure communication.

ENCRYPTION ALGORITHM

we use AES algorithm it is a advanced encryption standard. It is used for encryption of electronic data. It supports variable-length block using variable-length keys. A key size of 128, 192, or 256-bit can be used in encryption of data blocks that are 128, 192, or 256 bits. The main advantage of this algorithm is block length and/or key bits can easily be expanded. We have considered a simple example which shows the AES key expansion technique. In this technique 16 keys are used randomly and four words are used initially. Each new word depends on the previous word. And one special type of function is used in this process so that key is randomly changed through this complex function.[4]



According to the diagram 4 keys are provided to the 4 word w0 word is very first word it XOR with complex function and generate w4 word then after this word is XOR with the w1 word and w5 word is generated this process is running till w7 word is not generated .through this process TIC code is generated .

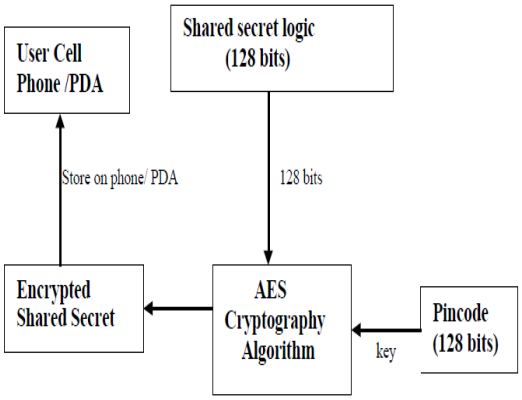
The following are the sub-functions of function g:

One byte left shift is done by this algorithm. By this operation input is [a0,a1,a2,a3] is transformed into [a1,a2,a3,a0].

For each byte of input words, the Byte substitution is done by SubWord,using the S-box.

The output of the above two steps (i.e.,step 1 and 2) is XORed

Cipher Key Management:-our main objective is provide the secure transaction between client and server. So that produce a secret key and this key is used for encryption and decryption of information. So that when start the transaction from the user side server generate the secret key and also generate the shared secret logic for encrypt the secret key and send to the user side user decrypt the key and use in the later stage .this same secret key is also store in the server side which decrypt the detail and TIC code and match this TIC with the store TIC which is issue to the user when it is match then transaction is start



According to this diagram key is generated from the server side and one shared secret key is also generate for encrypt this key and apply the AES algorithm and encrypt shared secret key is generated and it is send to the user cell phone. This key is a 128 bits. Whenever user cell phone is lost then no one can use this key because this key is store in the encrypt format so this key is very useful and this key is only decrypt when valid user login the bank website.

One TIC list is send to the user cell phone. List is stored into encrypted manner user select the one TIC from the list he use the local password for this selection when TIC is selected it authomatically decrypt . and the selected TIC will also remove from the TIC list. So that encryption and decryption of TIC is also based on the AES key algorithm which is define to upper portion. So that this TIC is used by the user for the use of one time password mechanism.

Authentication protocol over the internet;-

1) Firstly mobile device start the protocol through sending its ID to the server .
2) Server create a session for this client and generate a random request it is a matrix request
3) Client generate a challenge with his ID ENCRYPTED with the combination of the matrix key or internal key
4) Server send a challenge received with the previous message and randomly generate session key
5) Client decrypt the message through the session key when this challenge match the previous challenge which is send to the server then client consider it is a Valid server[4]

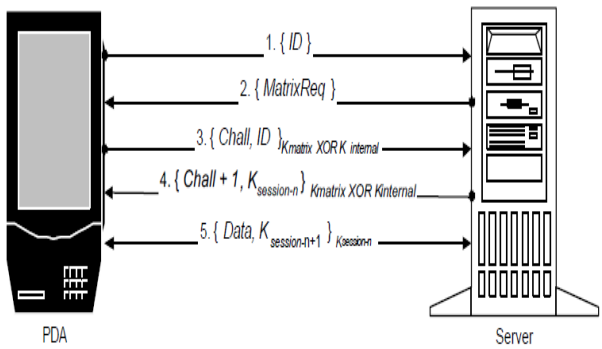
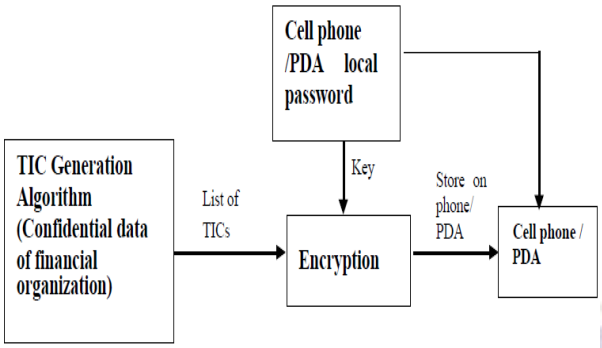


Figure 2 – The authentication protocol over the Internet.

Factors of authentication:-

Online banking fraud- The Internet is a medium which allows large number of people or organizations to communicate with each others in a few seconds, without much efforts and charges. .



Now online fraud is very popular all over the world, it has become a major source of revenue for criminals. The banks or financial institutions are very attentive in detecting and preventing online frauds

Key types of online fraud-

The Online fraud has been categorized broadly into two categories as mentioned in

User identity theft:-

- ✓ Phishing attacks which trick the user into providing access information.
- ✓ Key-loggers and "spyware" which clearly capture access information.

User Session Hijacking

Attacker gets control over the active user session and monitors all user activities.

- ✓ Local malware session hijacking attack performs host file redirection.
- ✓ Remote malware session hijacking attacks performs //

Authentication Methodologies :-

Existing authentication methodologies have basic three "factors

- ✓ Know: The user knows (password, PIN);
- ✓ Has: The user has (ATM card, smart card); and
- ✓ Is: The user is (biometric characteristic such as a fingerprint). [2]

Conclution And Future Work:-

In online payment security is a major part. There are many internet threats that affect the security system of internet. single factor authentication increases risk in communication because it require only username and password so that any attacker hank this information and treat as a valid user that's way use the multifactor authentication like a two way authentication technique is used for this purpose so that it reduce fraud and provide strong security application for online transaction.

The implementation of this protocol will not increase expenses of users significantly. This protocol can be easily implemented and executed on the current expenses charged by financial institution from the users to perform online payments or with very less addition to the current charge of online payment. Basically, the cost model of the proposed protocol depends mostly on the policies that financial institutions adopt for implementing this protocol

Future work will focus on developing a new and efficient way for TIC code generation at the financial institutions. TIC code installation on the user's cell phone must also be an easy task to avoid repeated visits by the customers to the bank or financial institution. Server side TIC maintenance, management mechanism and distribution to satisfy the demand from a large number of users are also part of future work

Referances:-

1) Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Sugata Sanyal and Svein Knapskog, "A Multifactor Security Protocol For Wireless Payment-Secure Web Authentication using Mobile Devices", IADIS International Conference, Applied Computing 2007, Salamanca, Spain, pp. 160-167, February 2007.

2) Lawton G., "Moving Java into Mobile Phones", IEEE Computer, Volume 35 Issue 6, pp. 17- 20, June 2002

3) M. Debbabi, M. Saleh, C. Talhi and S. Zhioua, " Security Evaluation of J2ME CLDC Embedded Java Platform ", In Journal of Object Technology, volume.5, Issue 2, pages 125-154, March-April 2006. (http://www.jot.fm/issues/issues 2006 3/article2)

4) Jablon David P., Integrity, Sciences, Inc. Westboro, MA, ACM SIGCOMM, "Strong Password -Only Authenticated Keyexchange",Computer Communication Review, Vol. 26, pp. 5 - 26, September 2005.

5) J. Daemen and V. Rijmen, "Rijndael, the advanced encryption standard," In Dr. Dobb's Journal, Volume 26 Issue 3, pp. 137-139, March 2001.

6) Pointcheval D. and Zimmer S., "Multi-Factor Authenticated Key Exchange," in Proceedings of Applied Cryptography and Network Security, pp.277-295, 2011

Author:-

Anita Maheshwari- she has completed her B.Tech.(I.T.) form Rajasthan University and M.Tech.(CSE) from Mewar University Chittorgrah **(**Raj.). Areas of interest is- Two way authentication protocol for Mobile payment system