A Multifactor Security Protocol for Wireless Payment
Secure Web Authentication Using Biometric Characteristics

Pawandeep Singh, Harneet Arora
Dept. of CSE, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

Abstract
This authentication technique uses a best approach for secure web transaction. It uses a Biometric property of user for authentication and SMS (Short Message Service) to enforce an extra security level along with the traditional Login/password system. Biometric properties are needed when a user wants a transaction then the user gives their fingerprint information. In this technique uses an encryption/decryption method. It is a very complicated algorithm. This method keeps the biometric properties as a secret code. A user creates the biometric properties on their Mobile device with the help of fingerprint scanners. Then the pre-installed application creates an image of the fingerprint and encrypt with the help of public key cryptography. This technique is not a one time password technique, it can be used as more as user’s want. This code is used to initiate secure web transaction using cell phones. Finally we extend the system for two way authentication which authenticates both parties (user and e-service provider).

Keywords
Biometric Characteristics, Multifactor Security Protocol, Wireless Payment

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-------MB: Authorization and capture request
MB------CB: Authorization request
CB------MB: Authorization response
MB-------M: Payment Ack.
M---------C: purchase response

Fig. 1: Transaction Flow in SET

Some disadvantage of set protocol is:-
• Set is only design for wired network. It not support fully wireless network.
• Set is end to end security mechanism which means it requiring traditional flow between customer and merchant.
• 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.
• No one notification received from the customer bank to the customer after successful transaction.
• Set protocol is only for card based not support account based payment system. So that we use a two way authentication protocol.

II. Related Work

A. Multifactor Authentication
Single-factor authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. To provide secure web transactions using cell phones multi factor authentication techniques have to be used.

B. Biometric Authentication
Biometric Authentication is the technique which is used to identify both the user and the ongoing transaction. It certifies that the current transaction has been initiated by the right person and it is a valid user who is trying to access his/her account.

Biometric Identification is :-
• Image of finger-print is created by user itself.
• Image is generated with the help of inbuilt finger-print scanners on the devices which are used by users.
• This image is encrypted using public key cryptography before sending through the wireless media.

The Bank or Financial institution will keep a record of users finger-print and match the same during the online web transaction.

C. SMS Authentication

Another method to validate user transaction is an SMS confirmation. The Bank or financial institution stores user cell phone number to provide multifactor authentication. We believe that users will carry their cell phone and can receive and send the short message. As a result, only valid users who have account will receive confirmation SMS from the authentication server.

After getting an SMS the user can acknowledge the choices. When authentication server receives “YES” it knows that the user is valid and the user has approved their initiated transaction. On the other hand, if the user sends a “NO” or the user does not send any response within a specified time period then the transaction will be rolled back and terminated [1]

D. Secure Web Authentication Protocol

This shows the Protocol for secure web authentication using Mobile devices. This protocol starts with the action of money transfer decided by user. Here we assume that the user information is available at server which includes user’s cell phone number. A separate authentication server is recommended to maintain strong security to authenticate users and their transactions with regular web and database servers of user information.

![Multifactor Secure Web Authentication Protocol Using Mobile](image)

Below we describe each step of the above protocol.

1. User gets username & password from the Bank. Each user has only one username/password to their account.
2. A Web-based username/password basic authentication is used to identify the user to the Web server.
3. The username and password will be verified by the Bank Authentication Server. After user recognition the user will get option screen to proceed further.
4. The user will get a notification of a successful logging with welcome message. This step also generates a session key.
5. The user will select mode of payment. We have considered two modes of payment: Credit Card based system & Account based Electronic transfer. It is straightforward to add other modes to our system.
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 generate a image of finger-print using finger-print scanners which is inbuilt in the mobile device. All details of the transaction, with attached image, will be further encrypted by AES encryption technique and submitted to the bank web server. The bank web server would pass it on to the authentication server where it would be decrypted and matched with the finger-print image which is stored in the users information on server side.
8. The bank authorization server decrypts the received message. It then verifies the image received from the user by comparing it with the stored image in the user account information at server database. If both images match then it goes to the next step. If no image matched with those in database then the authentication server will deny the user transaction and display appropriate error message to the user.
9. Bank server generates an acknowledgement to the user, which makes user free to logout from the web portal and wait for a confirmation SMS or to initiate another financial web transaction.[1]
10. After completing the database updation with respect to the ongoing transaction, the authentication server will send an SMS to the user’s cell phone to verify the initiated web transaction. The cell phone number of the user is available on authentication server.
11. The user would confirm their initiated transaction by choosing “YES” or deny it by choosing “NO” by replying confirmation SMS.
12. The server will notify the user by a Message to acknowledge the successful completion of transaction or declination of the transaction.

III. 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.

A. Encryption Algorithm

we use AES algorithm it is an 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 the 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 image 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 \([a_0,a_1,a_2,a_3]\) is transformed into \([a_1,a_2,a_3,a_0]\).

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.

**B. Cipher Key Management**

Our main objective is providing the secure transaction between client and server. So that produce a secret key and this key is used for encryption and decryption of information.

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.

**IV. 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.

**A. 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).

V. Conclusion
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 hack 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.

VI. Future Work
Future work will focus on developing a new and efficient way of using biometrics characteristics using cell phones/PDA. Fingerprint scanning is efficient on the user’s device with the help of appropriate scanner so that user send correct information to the bank or financial institution. Server side maintenance, management mechanism and distribution to satisfy the demand from a large number of users are also part of future work.

References