A Multifactor Secure Authentication System For Wireless Payment

Sugata Sanyal, Ayu Tiwari and Sudip Sanyal

Abstract Organizations are deploying wireless based online payment applications to expand their business globally, it increases the growing need of regulatory requirements for the protection of confidential data, and especially in internet based financial areas. Existing internet based authentication systems often use either the Web or the Mobile channel individually to confirm the claimed identity of the remote user. The vulnerability is that access is based on only single factor authentication which is not secure to protect user data, there is a need of multifactor authentication. This paper proposes a new protocol based on multifactor authentication system that is both secure and highly usable. It uses a novel approach based on Transaction Identification Code and SMS to enforce another security level with the traditional Login/password system. The system provides a highly secure environment that is simple to use and deploy with in a limited resources that does not require any change in infrastructure or underline protocol of wireless network. This Protocol for Wireless Payment is extended as a two way authentications system to satisfy the emerging market need of mutual authentication and also supports secure B2B communication which increases faith of the user and business organizations on wireless financial transaction using mobile devices.

Sugata Sanyal
School of Technology and Computer Science, Tata Institute of Fundamental Research, (TIFR), Mumbai, India, e-mail: sanyal@tifr.res.in

Ayu Tiwari
Indian Institute of Information Technology (IIIT), Allahabad (UP), India
e-mail: ayu.tiwari@gmail.com

Sudip Sanyal
Indian Institute of Information Technology (IIIT), Allahabad (UP), India
e-mail: ssanyal@iiita.ac.in

1 Introduction

Online banking, one of the fastest growing internet based activity which increases flexibility to the users to make their utility payments world wide and also increases the business of the organizations universally. It is so popular that the criminals are well aware of it and it is major revenue making source for criminals. The fundamental requirement of any online banking applications is a security to protect users confidential data. Financial institutions providing online services and offering Internet-based products should use secure and efficient methods of authentication to protect data of their customers. Accessing today's web-based services always requires a username and password to authenticate the user identity. This is a significant vulnerability since the password can be captured by the man in the middle attack and later used for making illegal access to the users account. The user authentication method used by current online payment systems is not adequate and secure. Thus it is possible for an unscrupulous user to use credit card number or account details stolen from valid user. Financial agencies considered single-factor authentication is not sufficient for user authentication and insecure for high-risk financial transactions which involve access to customer information or the online fund transfer to other parties using web browsers or cell phones/PDA [1, 2].

The single factor authentication does not support all the security requirements, major drawbacks of single factor authentication are:

1. System relies on password authentication only.

2. Easily deducible with public domain cracking software utilities.

3. Weakness of the system: Password is encrypted and Needs to traverse insecure medium (Interception and decryption).

4. This makes it vulnerable to passive attacks.

5. Rigid and strict password requirements, so difficult to remember passwords and this leads to storing of an e-copy of the password on the computer at easily accessible locations.

In order to support our claim single factor authentication is vulnerable to various attacks. We would like to highlight the key points of the published guidelines of FFIEC (Federal Financial Institutions Examination Council).The FFIEC Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. They introduced a various points related to need of stronger authentication for Internet banking services as mentioned in [3]:

- Financial institutions must use the guidance by FFIEC for evaluating and implementing authentication systems and practices

- Financial institutions thus offering internet based products must have reliable and secure methods to authenticate users

- Risk assessment must be conducted to identify types and levels of risk associated with their particular internet finance related product

So, we need Multifactor Authentication technique to secure our web transactions and to increase faith of users on mobile financial transactions. In this proposed work we are introducing new authentication system which is secure and highly usable, based on multifactor authentication approach. It uses a novel approach to create an authentication system based on TICs (Transaction Identification code) and SMS to enforce an extra security level over the traditional login in a username/password context. Al-Qayedi et al.[4] have also proposed the use of SMS to implement secure login session but have not used TICs in their protocol. TICs are user specific unique transaction identification codes which are issued by banks or financial institutions to their users. This code is similar to One Time Password (OTP) but provide more secure authentication to the transactions and one TIC code is used only once. This work also suggests an encryption/decryption technique that would be used to keep TICs as secret codes on cell phones/PDA. The user can easily pick up a TIC (from the stored list of TICs) to initiate secure web transaction using cell phones/PDAs, instead of remembering and typing a complicated TIC code in each transaction. This protocol is extended to introduce mutual authentication by two way authentication system i.e. the company or service provider is authenticated to the user along with the authentication of user to the financial institution. In two way authentication business organizations can also adopt this proposed system for their B2B mutual communication. The proposed protocol can also implemented in B2B communication with very slight modification to it. It enforces the strong security over the existing system to protect the business communication over the insecure networks.

The paper is structured as follows: Section two reviews the related work on e-payment systems. Section three introduces the Multifactor authentication approach. Section four presents our protocol for Wireless Payment including the system design and architecture for secure web authentication. Section five presents the architecture of the two way authentication scheme and its functional components. In Section six, we discuss some implementation issues. In section seven, security analysis demonstrates the resistance of the protocol against various internet threats. Section eight shows various advantages of this new system followed by some conclusion in section nine.

2 Background and Related Work

According to Gao et al.[5], mobile payment refers to wireless-based electronic payment for m-commerce to support point-of-sale/point-of-service (POS) payment transactions using mobile devices. In general, m-payment systems can be used by wireless-based merchants, content vendors and information and service providers to process and support payment transactions driven by wireless-based commerce applications. As discussed in [2], the existing m-payment systems can be classified into three major types. The first type is account-based payment systems which can be mobile phone-based, smart card or credit-card m-payment systems [6, 7, 8, 9, 24]. Second type of m-payment system refers to the mobile POS payment systems by which customers can purchase products on vending machines or at retail stores with their mobile devices. The third type is E-wallets or E-cash which stores digital cash, which has been transferred from a credit card, debit card or virtual check inside their e-wallets. This payment system is designed to complement existing credit and debit card systems for mobile users and can be either automated POS payments or attended POS payments [7, 9].An example of mobile POS payment system is Ultras M-Pay (http://www.ultra.si/).

2.1 Secure Electronic Transaction (SET)

The Secure Electronic Transaction is an open protocol specification developed for credit card transactions over internet. Although SET has been designed to operate in a wired infrastructure [10, 11, 12] its transaction flow and implementation of security are of interest to us since it can also be employed in a wireless scenario [10]. As referred to [10] basic transaction flow under SET protocol is:

1. The consumer accesses the merchant's web site, browses the goods on display and selects what he or she wants and gets the total cost of all chosen items including taxes and shipping costs.

2. The system asks for payment method and the consumer chooses to pay through a credit card using SET.

3. Digital Wallet is special software used to enter credit card information.

4. After getting details of customer payment the merchant contacts the merchants Bank for customer authorization and payment.

5. Merchant Bank will contact the customers Bank for the same and get approval of payment.

6. Merchant will notify, if transaction is successful.

7. A few seconds later, there is a confirmation to the customer that this order has been processed.

SET is a good example of a protocol which does not provide secure user authentication. Generally, implementation of SET uses SSL-based methods, which is not completely secure [13].
Some disadvantages of SET are:

1. SET is designed for wired networks and does not meet all the challenges of wireless network.

2. SET protocol worked in the traditional model of payment data , so an end-to-end security mechanism was required.

3. Direction of transaction flow in SET. In SET transactions are carried out between Customer Agent and Merchant. It is vulnerable to attacks like transaction/balance modification by Merchant.

4. The transaction flow is from Customer to Merchant so all the details of the users credit cards/debit cards must flow via the merchants side. It increases the users risk, since data can be copied and used later to access a customer account without authorization.

5. There is no notification to the Customer from the customers Bank after the successful transfer. The user has to logon to their Bank online portal in order to get transaction and payment detail.

6. SET is only for card (credit or debit) based transactions. Account based transactions are not included.

3 Multifactor Authentication Approach

Multifactor Authentication is a technique for users to authenticate themselves using two or more authentication, generally this method has been implemented for large devices which are more capable in terms of power and processing capabilities, some commonly available systems uses combination of something the user possesses such as a security token (e.g., USB dongle or security smart card), and something the user knows (e.g., password). Another very popular multifactor authentication technique is Biometrics. The major draw back of Biometric approaches is that it requires large systems to implement with very high power and processing capability with high implementation and deployment cost.

The proposed work suggests that Multifactor Authentication technique can be implemented in secure web transactions using cell phones. The best way to implement the multifactor authentication approach without any extra hardware and extra cost is to use two separate communication channels to confirm the identity of the user.

3.1 Multifactor Authentication Techniques

In the present work, we propose a multifactor authentication technique based on TICs and SMS confirmation.

3.1.1 TIC Authentication

TIC code authenticates the wireless transaction to allow server access. It is a technique which verifys both the user and the ongoing transaction. A TIC code certifies that the current transaction has been initiated by the right person and that its a valid user who is trying to access his/her account.
TIC codes are:

- Issued by the Bank or Financial Institution to its customers.

- A 32 bit or 64 bit Pseudo Randomly generated code which are assigned to the customers.

- May be a complicated digit sequence or combination of numeric and alpha numeric characters.

- One time code, each transaction will use unique TIC code for authentication.

The TIC codes are most sensitive data for any financial transactions, so we are storing TICs in encrypted format on users cell phone. The key to decrypt the TIC before making any online web transaction is a local password on cell phone and only valid cell phone owner will know the password. This password is a local password and user can change it easily time to time to keep protection. The Bank or Financial institutions are responsible for TIC generation and distribution to their customers. The TIC generation logic is strictly confidential and limited to the only responsible authorized staff of the organization. The financial organizations will also maintain the authentication server to record the issued TICs to the users and matches the same code for each receive transaction and cancel the used TIC after successful transaction, so that each TIC will be used only once, [14] also recommended that financial institutions should decide the validity time period for TICs according to its standard

organizational issuing policies, this method decrease the risk of fraud with the very old TICs.

3.1.2 SMS Authentication

The Bank or Financial institution stores user cell number to send SMS to their customers for their transaction confirmation. Cellular network uses separate channel to send and receive SMS over wireless medium [4]. Here we assume that users carry their cell phone with them regularly and therefore can receive the short message and reply SMS to confirm or deny their financial transaction. As a result, only valid users will receive SMS from the authentication server. After getting the SMS, a user can acknowledge the choices. When the authentication server receives "YES" it knows that the user is valid and that the user has approved their initiated transaction.
So, Multifactor Authentication is used to verify the user and the transaction by using following steps as referred to [14]:

1. Web-Based Basic Authentication: Firstly, the user will access web server using their assigned web-based username/password for basic authentication.

2. TIC Authentication: After successful authentication of the user using username/password, the web server will demand for a TIC code from the web user as a second authentication when user will initiate any financial transaction. Now user will decrypt and insert one time TIC code to uniquely identify his/her transaction and prove his/her identity to the web Authentication server.

3. SMS Confirmation: After the successful TIC code authentication, the third authentication will take place, a SMS confirmation is a final approval to their initiated online transactions.

The security of the system also depends on the security of the messages sent by SMS and WAP, which are encrypted and protected with A5/3 Algorithm [15]. The user will get a SMS with the required details which are essential to identify and recognize the users initiated transaction. By this SMS, a user will confirm their transaction by "YES" or "NO". Transaction will be committed on server only if the user chooses "YES" and Rollback in case of "NO". As refer to [14], in next section we are focusing on proposed protocol based on above recommended authentication techniques.

4 Secure Web Authentication Protocol

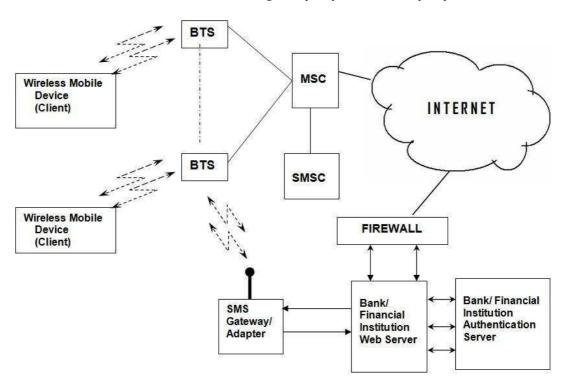The data flow and architecture, based on Multifactor Authentication techniques, is described in this section.

Fig. 1 Architecture of Multifactor secure Web Authentication Protocol using Mobile Devices
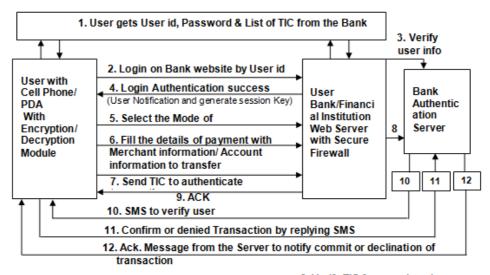
4.1 Architecture of Secure Web Authentication Protocol

Figure 1 shows high level architecture of protocol for a secure web authentication using small wireless mobile devices like cell phone/PDA. Figure 2 shows more detailed pictorial representation of transactions of protocol.

The basic function of this protocol starts when user initiates payment or fund transfer process using their cell phone/ PDA. It is highly recommended to use separate authentication server to implement the protocol and increase security. Step by step processes of using the proposed system are given below:

BTS - Base Transceiver Station, MSC - Mobile Switching Centre, SMSC - Short Message Service Centre

1. User will get their secure login/password details from bank or financial institution when they make contract with financial institution to open their account.

Fig. 2 Multifactor secure Web Authentication Protocol- Transaction Flow

Financial Institution is also responsible to distribute the TICs to their customers, authorized person will make initial setup to their customers cell phones/PDA and install TIC codes with internal encryption.

2. The user will login using a Username/Password on Bank web server through GPRS connection and web-based username/password is a basic authentication used to identify the user to the web server.

3. After successful basic authentication the user will get an option to initiate transaction with a welcome message and secure session id. We have considered three modes of payment: Credit Card, Electronic transfer and Debit Card.

4. The user will select mode of payment. In case of credit card based payment protocol demand valid credit card number.

5. The user will insert the details of payment by filling in a simple form with details such as the merchants account number, invoice number or account number to which an amount has to be transferred.

6. User can not submit online transaction without TIC code. As we have already mentioned in Sect. 3.1, TIC is a one time code and user will insert a TIC code from the stored list of TIC codes. Note that TICs are password protected on the cell phone and this password will be used to open the list of TIC codes and de-

crypt the selected one before using it in ongoing transaction.

7. Complete transaction with an attached TIC will be further encrypted and submitted to the server for processing. Here we are suggesting hybrid encryption technique to encrypt the transaction details, more details on cryptography implemented in the proposed system are mentioned in Sect. 4.2.

8. On the server side, banks authentication server decrypts the received transaction and extracts a TIC code. The server verifies the TIC sent by the user by comparing it to its stored list of TICs in the user account information at the server database. If both TICs matched, it cancels the used TIC from its database and goes to the next step. If no TIC matched with the database then the authentication server will deny any further user transaction and transmit an appropriate error message to the user.

9. If TIC authentication is successful, a authorization server will generate a text SMS and send to the SMS Gateway/Adapter to transmit it over the cellular network. Cellular network uses SMSC as a backbone device of the network to deliver a SMS to the user cell phone. The user will acknowledge to the server to verify his/her web transaction.

10. The user will confirm his/her initiated transaction by replying a SMS with "YES", or deny it by choosing "NO", by sending a confirmation SMS.

In the above module all the transactions from client to server or vice versa are strictly in an encrypted format. An Encryption and decryption module is installed on the users cell phone/PDA and on server side environment. Moreover, unlike SET, at no stage does the user have to supply personal information to the merchant. The cryptography module is discussed in more detail in next sub section.

4.2 Cryptography and Key Management

The most effective solution for secure communication over wireless networks is to employ an end-to-end security approach. End to end security can be achieved with the help of strong cryptography techniques. Public key encryption techniques is very popular encryption method and used in many application areas like application data security, operating systems security, network security and Digital Rights Management (DRM) are some examples. Internet Engineering Task Force (IETF) is an organization formed to decide standards for Internet and mobile platforms for cellular network environment. Public Key Infrastructure (PKI) is also widely accepted in cellular network environment to make secure communication in wireless networks. As mentioned in [17] public-key encryption needs more computation and processing time in comparison of symmetric-key encryption. Therefore, public-key

encryption is not always suitable in large amount of data communication. However, public-key encryption is used to exchange a symmetric key, which can be later used for further encryption of data. This approach uses combination of above two techniques in encryption and adopted by various security protocols and it is called hybrid encryption schemes [16, 17, 18].

AES Rijndael Encryption Algorithm has been referred in the proposed system [30, 31]. AES Rijndael algorithm uses iterated block cipher, it produces output after multiple transformation of input block and cipher key. It supports variable-length block using variable-length keys; a 128, 192, or 256-bit key which can be used to encrypt data blocks that are 128, 192, or 256 bits long. All nine combinations of key and block lengths are possible[30, 31]. AES Rijndael algorithm was designed to have the following characteristics:

- Algorithm is secure against all known attacks

- It perform operations at good speed over huge platforms, code is also small

- Design is simple

The AES Rijandael implementation was taken from the Legion of the Bouncy Castle cryptographic package [28] which provides a Java implementation for the algorithm.We have used block size of 16 bytes processed with 128-bit keys: this proved to be the best combination for operation on J2ME devices due to the speed and memory limitation of such devices [19].

4.2.1 Cipher Key Management

Securing the communication between client and server is our primary concern. For this reason we have implemented a hybrid encryption scheme over wireless medium. As referred to [19], we have used a session-key management mechanism where the encryption / decryption keys are randomly generated for every client session. This mechanism works as follows: the server uses a 128-bit key. At the start of user session the server randomly generates one secret key (128 bits) and stores it in the users specific entry in the database. The server then encrypts the session key using the client's 128 bit shared secret logic known to the client and the server. Session key is transmitted to the client after encryption.

A TIC code is used to encrypt all the transaction details of the customer before submission to the server, and then the TIC code itself is encrypted with a secret key which is generated by the server and transmitted to the user after a successful login.The client decrypts this secret key and uses this further to encrypt the TIC code before transmission to the server. On server side same secret key is stored which
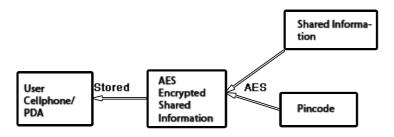
Fig. 3 Storing of Shared Information on Client Environment

decrypts the TIC code, then matches the TIC code with the issued TICs to the customer If this TIC matches with the database then it will be next used to decrypt the other transaction details which were encrypted by an identical TIC at the user end otherwise transaction would be denied.

Another important issue that must be addressed is securing the storage of the shared secret on the client and server. On the server, this shared secret is stored in the database, which we have assumed to be secured by the database management system, operating system with secure firewalls and other computer security policies. Reference [19], also explain that securing the shared secret on the client machine involves big risk since these are small devices that can even be stolen. We used the following mechanism to protect the shared secret on the client environment:The shared secret key is stored in an encrypted format on the cell phone/PDA, in the Keys Java class in the application's JAR file. As shown in Fig. 3, the shared secret is encrypted by the client's 128 bits pin code, since AES requires that the key length is 128 bits [19].

In case of the banking application, at the time of subscription to the mobile banking service, it is the responsibility of the service manager to encrypt the shared secret with the client's pin code when the application is distributed, and to store the shared secret on the mobile phone/PDA.Furthermore, to enhance the security of code on the client, the Java classes in the MIDlet JAR file are obfuscated to protect the code from byte code de-compilers. The obfuscator we used is the Retroguard obfuscator v1.1 [29].

In proposed protocol TIC codes are most sensitive data which are stored on cell phone/ PDA. To maintain the security we have proposed that TICs are stored on the cell phone/PDA in an encrypted format and password protected as shown in Fig. 4. The user will insert local password of TICs to open the list of TICs and can select any TIC from the list to initiate financial transaction. This selection of TIC automat-
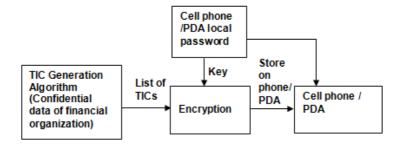
Fig. 4 TIC Protection at Client Environment

ically decrypts the selected TIC and displays it on the users screen. This selection will also remove the selected TIC from the list of TICs at client environment. Local password of TIC is the key for decryption of TIC and known to the user only. Even the server at the financial institution is unaware of this key. It can be changed at any moment according to the convenience of the user. The local Encryption and decryption of TIC is also based on the AES symmetric key algorithm. AES cryptographic algorithm is best suited for the small devices; it enhanced the performance of cryptographic processing speed over small hand held devices instead of degrading the device performance.

However, there are several instances when we require a two-way authentication. In the following section we present the protocol for mutual authentication [14].

5 System for Two Way Authentication

After having analyzed the Secure Electronic Transaction (SET), on-line payments [9, 10, 13] and having taken into consideration the constraints of the wireless infrastructure, we developed the secure protocol for Wireless Payment, supportive of one-way authentication in the previous section. In reference to [10], we extend the protocol to support two-way authentication in the present section. In this architecture (Fig. 5) we have considered five major components with certain roles:

1. User: A user is a valid account holding customer of the bank,
2. Customer Agent (CA): A CA is a software module which is running on the customers mobile device,
3. Merchant Agent (MA): An MA is an online service provider and merchant website by which users do online purchasing,
4. Customers Bank: This is the bank at which the user has a valid account, it also contains the authentication server necessary to authenticate the user,
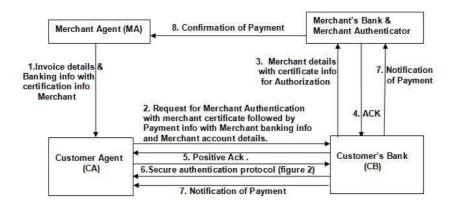
Fig. 5 Protocol for Wireless Payment: Two Way Authentication System

5. Merchant Bank: This is the bank in which the merchant has a valid account, the merchant Bank is also responsible for authenticating the merchant.

As referred to [10, 14] the two way Authentication protocol functions when the Merchant and Customer perform some commerce and Merchant generates an invoice statement for Customer to settle payment and it performs all authentication process for the other party. To implement the present scenario we have assumed all the participating financial institutions has business contract and bound with legal terms and conditions to give services to their customers. Figure 5, demonstrates the step by step flow of the payment transactions.

1. The MA generates an invoice and sends the Merchants encrypted banking information and authentication certificate with the invoice details to the CA.

2. The CA requests for authentication of Merchant to its Bank with the Merchant bank details, the merchant account details and a Merchant authentication certificate provided by the MA.

3. The Customer Bank forwards the Merchant details with the authentication certificate to the Merchant bank for authentication of the merchant.

4. The Merchant Bank sends a positive or a negative acknowledgement to the Customer Bank which confirms the validity of the Merchant or invalidates the Merchant.

5. In case of validation, the Customers bank sends a Positive ACK to the CA and goes to step 6. If the Merchant certificate is not valid, the Customer Bank will

notify the CA with that information. If Customer Bank receives a negative or suspicious acknowledgement of the Merchant it simply rejects the user transaction with valid security reason.

6. To initiate a payment process, secure web authentication protocol will be used to authenticate the customer. As mentioned in Sect. 4.1, secure web authentication protocol includes TIC validation and SMS confirmation as a part of secure customer authentication.

7. After getting a successful SMS confirmation from the customer, the Customer Bank will start transferring of amount to the Merchant Bank and after successful transfer also generate a payment notification for the Merchant Bank as well as to the customer with the required transaction detail.

8. As a final step Merchant bank will send a confirmation of the received payment from the customer to the MA with relevant details, such as invoice number, customer id and amount received. So that, the Merchant can shipped the purchased goods to the customer.

Protocol for secure web authentication secures the financial transactions between customer and customers Bank and preserves customers confidential data from the third party. As referred to [10] we also do not route payment transaction data via the MA. As a result, the security of the system is less susceptible to attack. Customer payment information and personal data are no longer available to the merchant directly and thus those details cannot be altered by the merchant.

In the next sub section we have presented complete transaction flow of the protocol, which is presented in the form of sequence diagrams. These details are required in order to perform a complete threat analysis of the proposed system.

5.1 Transaction Flow of Protocol

There are four sequence diagrams to demonstrate the step by step transaction flow of the proposed system. We have considered five major components in describing transaction flow of proposed system:

1. Customer Agent (CA)
2. Customer Bank (CB)
3. Customer Bank Authentication Server (CBAS)
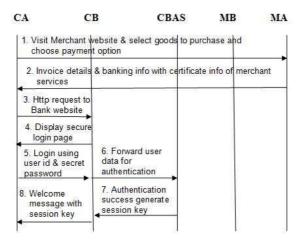4. Merchant Bank (MB)
5. Merchant Agent (MA)

Fig. 6 First Authentication of User to the Bank

5.1.1 First Authentication of User to the Bank Authentication Server

1. The user (CA) visits the website of the merchant to purchase goods online and chooses a payment option from the website.

2. The merchant web server (MA) generates invoice details and the merchant bank information with the merchant authorization certificate and sends to the CA in an encrypted format. We have discussed an encryption/decryption technique in Sect. 4.2. The same technique is useful to transmit merchant certificate information in an encrypted manner so that no one but CA can use it for merchant authentication. Note that cell phone has standard encryption/decryption capabilities to access and transfer data over the wireless cellular networks.

3. The user (CA) generates http request to their bank web server to initiate payment transaction.

4. The CB web server displays secure login page to logon on the web server.

5. The user can login using their user id and secret password known to them. Before transmitting users login details from client to server they will be encrypted using public key cryptography which is implemented on bank server by standard security mechanism. For more information on the public key cryptography refer to [16, 14].

6. The user details will be forwarded to the bank authentication server. Note that to maintain strong security mechanism we have recommended that the bank should
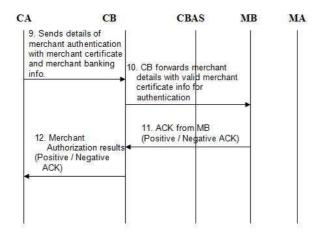
Fig. 7 Two Way Authentication

maintain separate authentication server.

7. At authentication server users login data will be decrypted and matched with the secure database records of the customer. On success it generates random session key which will be encrypted by shared secret logic as mentioned in Sect. 4.2.

8. The customer bank (CB) will send general textual welcome message and session id to track the user session with the secret session key received from CBAS to the user (CA). If the user authentication fails then it sends invalid login message to the user.
After successful login two way authentications take place as mentioned in Sect. 5.1.2.

5.1.2 Two Way Authentication - Authentication of Merchant to the Customer

9. The user (CA) will send the request to the users bank for merchant authentication before making payment to MB. The CA will forward received merchant details to authenticate the merchant.

10. Here we have assumed that the customer banks (CBs) and the merchant banks (MBs) have business model and they are linked to each other with the legal terms and conditions with standard policies decided by their business organizations. So, the CB will make a request to the merchant's bank to authenticate the merchant. Each merchant has legal authorization certificate which has been issued by
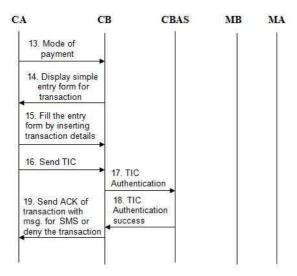
Fig. 8 Second Authentication of User to the Bank

their banks or some centralized financial institutions to authenticate the merchant services.

11. The MB will acknowledge a request for the merchant authentication after matching details of merchant provided by the CB. Acknowledgement may be positive or negative depending on the validity of the merchant certificate.

12. The CB will forward the received acknowledgement of the merchant authentication to the user (CA). Note that if MB would provide negative acknowledgement then the CB simply terminates the user transaction with valid security reason and if CB receives positive acknowledge from the MB then it is assumed that the merchant is valid and user can go forward to make payment.

   To initiate payment it will run multifactor secure web authentication protocol as mentioned in Fig. 1 and Fig. 2. Detailed explanation of the transaction flows of this protocol is mentioned in Sect. 5.1.3.

5.1.3 Second Authentication of User to the Bank Authentication Server

13. The user (CA) will select the mode of payment to make payment. Here we have considered three basic modes of payment: Electronic Transfer, Credit Card or Debit Card.

14. Selection of payment method generates an entry form with appropriate fields.

15. The user will fill the details of transaction by filling simple entries like amount, account number to which amount has to be transferred, if there is a merchant payment it automatically selects invoice number and other merchant details which was given by the merchant.

16. The user (CA) will insert the TIC code by opening the list of TICs stored at client environment. Note that:

    - The TICs are stored on the cell phone/PDA in an encrypted format and password protected.

    - The user will insert local password of TICs to open the list of TICs and can select any TIC from the list.

    - This selection of TIC automatically decrypts the selected TIC and displays it on the user's screen. This selection will also remove the selected TIC from the list of TICs at client environment.

    - Local password of TICs is a key for decryption of TIC and known to the user only, even server at financial institution is unaware of this key.

    - Transmission of TIC from CA to CB is strictly in an encrypted format as referred to Sect. 4.2.

17. The bank server will forward the received TIC to the CBAS for TIC authentication and CBAS decrypts the received encrypted TIC to match with its database.

18. The CBAS server will match the received TIC with the assigned list of TICs to the user. If the match succeeds it delete the used TIC from its database and send message to the CB server. On unsuccessful match it sends denial message to the bank server.

19. If a received TIC matches with the assigned list of TICs to the user, the bank server generates acknowledgement to the user with message to wait for a SMS. If TIC does not match with the users assigned list of TICs then it denies the current transaction and sends a message to the user that transaction is cancelled because of invalid TIC.
    After successful match of the TIC the user is free to close the current user session or make new financial transaction. The next step is SMS confirmation, the authentication server will generate a SMS destined to the user, as discussed in Sect. 5.1.4.
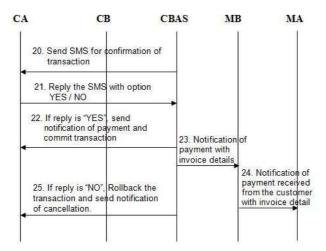
Fig. 9 Third Authentication of User to the Bank by SMS Confirmation

5.1.4 Third Authentication of the user and transaction by SMS confirmation to the Bank Authentication Server

20. The CBAS will send a SMS with transaction details for the confirmation of transaction by the user.

21. The user will reply to SMS by choosing "YES" or "NO". A SMS reply "YES" means user is valid and confirming their transaction. A SMS reply "NO" means user is denying their transaction.

22. If the bank authentication server receives "YES" from the user's SMS confirmation, it generates a notification of payment to the user and commits the users transaction.

23. The bank server will also send a notification of payment to the MB with invoice number and other required customer information.

24. The MB is responsible for sending notification of payment received from the customer to the merchant. Notification includes details of payment like invoice number and other required customer information.

25. If the CBAS receives "NO" from user's SMS, it immediately rolls back the current user transaction and sends a notification of cancellation of transaction to the CA.

Communication between the Customer Bank and the Merchant Bank is also online exchange of data which involves risk of many types on internet based attacks.

In order to make secure communication between the two business entities we must maintain secure channel with strong security credentials. Although in present scenario organizations are actively participating in implementation of security to protect their B2B communication, also organizations are very much aware of time to time improvement of their security system to protect their confidentiality. A suggested protocol in Sect. 4.1 can also be implemented in B2B communication but without SMS confirmation module. If the business units use TIC codes as a special one-time token to uniquely authenticate their every mutual transaction, they will get more secure financial transaction over the existing one. Bank servers have strong processing unit and large storage capabilities, so there is no restriction to maintain TICs in their database. It is recommended that banks should use separate TIC format to authenticate their B2B transactions. When bank initiate fund transfer to other bank it will insert TIC code as a one time token in their transactions and encrypt the complete financial details and transmit it to the server of other banking unit. At the server side it decrypts the received transaction and compares the TIC with the stored TICs in their database corresponding to bank branch who initiated the transaction. On each successful transaction both the business unit will cancel the used TIC from their database. Business organizations can easily implement this protocol with their existing infrastructure without replacing any of their existing security models and use existing encryption/decryption techniques which they have been using so far in their mutual communication, only addition of one field for TIC code is required to implement the proposed system. There is no SMS confirmation required because it is not feasible to implement in B2B communication, as well as there are very less chances of fraud or unauthorized access to the business data. Business units are generally trusted parties and bound in legal terms and conditions of association of financial authority.

The two-way authentication protocol addresses several shortcomings of the SET :

- Data that is vital for the user is never available to the merchant in an unencrypted manner and merchant will not have access to any customers confidential information.

- Secure Credit Card based transaction supported over SET. Only Credit Card owner can initiate transaction, if any unauthorized person gains access to your Credit Card information and try to initiate transaction with your Credit Card number then this protocol will deny this transaction because TIC authentication and SMS confirmation would not be present in fraudulent transaction.

- Set supports only card based financial transactions but using this protocol users are free to make direct account based fund transfer using Electronic Transfer.

Protocol is secure from various internet based attacks and also protects users from unauthorized access if they lost their cell phone or their phone is stolen. The detail

security analysis of the system is mentioned in Sect. 7.

The actual implementation requires elaboration of some specific technologies which are discussed in the next section.

6 Implementation Issues

J2ME is the preferred development platform the portability of Java code, the Java phone can process data locally which reduces the network traffic, and the capability to establish a new security policy on the client that will encrypted only sensitive data rather than encrypting complete transaction data. It also makes effective power utilization in limited power devices [23]. Also, J2ME mobile information device applications (MIDlets) can make use of, the WAP to perform HTTP network connection, without requiring TCP/IP [19]. J2ME provides a feasible solution to the traditional security gap in the WAP gateway. The security gap is due to the security protocol conversion mechanism ; the security gap is between WAP gateway with the secure sockets layer (SSL) encryption and the WAP wireless transport layer security (WTLS) encryption protocols. Due to this protocol conversion data would be available in an unencrypted format during the switching process of protocols, which increases the risks to the confidentiality of data in the gateway [19, 14, 22].

6.1 J2ME Overview

J2ME provides the ability of servers to accept a new set of clients: cell phones, two-way pagers, and palmtops. These devices can be programmed using the mobile information device profile (MIDP), a set of Java APIs which, together with the connected limited device configuration (CLDC) provide a complete Java runtime environment [23, 33]. The J2ME supports many powerful features of the Java programming language as a light-weight virtual machine (KVM) , it also provides a secure and easy execution environment for mobile devices [23].

6.2 Simulation

Our simulation of client applications have used Sun J2ME Wireless Toolkit consisting of build tools, utilities and a device emulator. It also includes the standard APIs like Limited Device Configuration (CLDC), Mobile Information Device Profile (MIDP), Wireless Messaging API (WMA), PDA Optional Packages for the J2ME Platform, J2ME Web Services Specification etc. The authentication server

is based on J2EE technology with web server Apache Tomcat and database Oracle 9i with Jserver capabilities.

6.2.1 Session Management

Various strategies have been developed to track client sessions on HTTP,a stateless protocol; the most popular of these are the use of cookies and URL rewriting [19]. The Java Servlet API are used to create the HttpSession object, which maintain session for each user at web server. We have used cookies to keep track on user sessions. To group HTTP request or response in a current active sessions cookie interchange mechanism is used. Each MIDlet client request to the web server explicitly contains a session cookie back. Server creates a new session using the HttpSession object, it sends the JSESSIONID cookie in the "SET-COOKIE" response header. The MIDlet client uses getHeaderField method on the HttpConnection object to extract the coookie, and use it further with the every HTTP request to keep track on session [19].

The initial setup of the cell phone/ PDA to connect with the bank financial server includes the Customer Agent (CA) installation with shared secret key. Once a phone is active to connect to the server user can store the TIC codes. The bank authority is responsible for TIC codes generation at the financial institution server and distribution of TICs to the customer and encryption of TICs before storing them on the client environment. TIC codes are pseudo random codes and can be generated with pseudo random number generation algorithm as mentioned in [20, 21, 14]. TIC generation logic is strictly confidential at the web authentication server and we are assuming that the banks will update TIC generation data regularly and time to time improve TIC generation algorithms to maintain confidentiality. Users demand for TICs as per their requirement as suggested in Sects. 3.1 and 4.1. The authorized person of the financial institution is responsible for the distribution of TICs to the user cell phone via simple data cable and distribution process includes the encryption of TICs for security reasons. At server side, we have assumed that TICs are stored in database and there is a strong security of Database management system (supported by Oracle 9i) and operating system with secure firewalls to protect server side data.

The small cost analysis of the proposed system shows that 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 to the users to perform online payments or with very less addition to the current charge of online payment. Basically, cost model of the suggested protocol depends mostly on the policies that financial institutions adopt for implementing this protocol. Implementation does not require many infrastructure change or wireless protocol modifications so it will not put extra cost to the financial institutions or wireless network service providers.

7 Analysis of Various Internet Threats

The proposed protocol is capable of handling various internet threats like phishing, loss of cell phone etc. In this section we present a detailed analysis of our system under various threats. In each case we analyze the information that an attacker may have and the specific points in the protocol where the attacker would fail to proceed with a fraudulent transaction.

7.1 Security against Phishing

Phishing fraud has become a popular technique for user identity theft. Phishers fraudulently acquire sensitive information of users such as passwords and credit card details to gain unauthorized access to the user's confidential financial data and perform illegal transfer of funds. Phishing is generally carried out using email or an instant message or via phone contact.Once this information is acquired, the phishers may use a person's details to create fake accounts in a victim's name, ruin a victim's credit, or even prevent victims from accessing their own accounts.

The protocol proposed in this paper is secure against phishing attacks. A multi-factor secure protocol for user authentication has capability to secure the user data and maintain integrity, confidentiality and access control from malware access. To understand the origin of this security we have considered below scenarios.

7.1.1 If Phishers fraudulently acquires user id and secret password

This is a general scenario of phishing attacks by which the attacker gets secret password of the user account and falsely accesses the user account to perform illegal transfer of fund. The proposed protocol shows that in the present case our protocol protects the users account and private data. The attacker would not be able to perform any illegal action, because of:

1. Figure 6 shows the first authentication of the user. As mentioned in step 5 of Fig. 6, the user has to produce login id and secret password to logon on bank server. If phisher fraudulently acquires the users account password then he successfully achieves the authentication of step 5 and subsequently step 6, step 7 and step 8 of Fig. 6. If organizations would rely on only user name and password authentication then any unauthorized person can easily acquires the control of user financial account by means of some phishing attack. To avoid this situation we have proposed additional authentication system - The TIC verification and authentication to protect users accounts from various phishing attacks.

2. In reference to Fig. 8 which shows the Second authentication of the user, any transaction trying to access user account has to produce one time valid TIC code to the web authentication server according to steps 16 and 17 of Fig. 4. At step 17 the authentication server would deny the falsely going transaction if it does not find a valid TIC code from the user.

3. TIC codes are secret codes issued to valid account holders and TICs are not publicly accessible. It is a one time code for each online transaction and it is randomly generated in nature so any phisher can not guess the next TIC code of user account.

7.1.2 Transmission of TICs over insecure channel

In Fig. 8, step 16 shows that a TIC code transmission from the users cell phone/PDA to the web authentication server is strongly in encrypted format. So, it would not be easy for phishing attackers to decrypt a TIC code to access the users private information. Encryption techniques are discussed in more detail in Sect. 4.2. Moreover, one TIC is used only once and then discarded.

7.1.3 If Phisher fraudulently acquire users secret password and also one TIC code by some Phishing technique

This is an extreme scenario of phishing attack in the present system by which attacker gets the secret password of the user account with one TIC code and falsely accesses user account to perform illegal transfer of fund. This protocol is safe in this extreme situation and protects users confidentiality.

1. There is another major security factor of the presented protocol to protect users from this extremely vulnerable condition. The system is secure in this condition by multifactor authentication technique as mentioned in step 20 of Fig. 9.

2. In Fig. 9 of Sect. 5 shows third authentication of the user to the bank by SMS confirmation. A SMS confirmation is a next factor which saves the user information from malicious access of unauthorized users in this extreme situation. At step 21 in Fig. 9 by replying "NO" to SMS confirmation the user can deny unauthorized access of account and take necessary action of changing of passwords and secure their confidential information from attackers.

3. The TIC codes are pseudo random in nature so, if phishing attacker gets one TIC code sample by some phishing technique, the phisher can not generate next TIC code because TIC generation logic is strictly confidential at web authentication server and we have assumed that banks and financial institutions are responsible for time to time updating of TIC generation data and upgrading of TIC genera-

tion algorithms.

4. If the user is getting continuous SMSs for web transaction confirmations which have not been initiated by them, the user can notify to the bank or financial institution and get replacement of all previously issued TIC codes to the user.

7.2 Security against virus attack on cell phones and PDAs

Mobile wireless devices, like cell phones and PDAs, are also vulnerable to hackers and viruses. Popular viruses "Cabir" and "CommWarrior.A," could scan users address book and phone numbers and transmit from mobile phones and BlackBerrys by using Bluetooth or via messages services without the knowledge of user [25, 26, 27].

The proposed system is secure against mobile device virus attacks on the users cell phone. The system is secure from the various virus attacks by the following points:

1. The users always carry their cell phone with them so a SMS confirmation will not be present in case of malicious transaction raised by any unauthorized user, who has gained access to the users confidential data through virus attacks.

2. The TICs are stored in an encrypted format and password protected, so the person who has gained information illegally will still be unable to decrypt the TICs and virus attacks would not be able to disturb the users data.

3. It is always recommended that to prevent inadvertently downloading a mobile device virus through a Bluetooth connection, check the access permissions on your Bluetooth settings and turn off user devices Bluetooth connection when they are not using it. The users can also use antivirus software on some mobile platforms to protect themselves from viruses.

7.3 User Session Hijacking

An attack in which all users activities or operations are closely monitored by using malicious software ("malware") is known as user session hijacking. Session hijacking malware can be reside users local computer, or remote as part of a "man-in-the-middle" attack. To overcome this threat proposed secure protocol provides security at the following steps:

1. In Fig. 6 first authentication of the user to the bank, after successful completion of step 5 and 6 authentication server creates a session id as mentioned in step 7 and 8 of Fig. 6. This session key would be transferred to the user in an encrypted manner to create a secure session. Further Http requests from user should use session id to make request to the server. If the server receives unauthorized Http request which does not contain the session id generated by it, then the service would be rejected.

2. The TIC codes are pseudo randomly generated by confidential algorithm; it is a complicated code which can not be easily predicted by any person. The TIC codes, which are one time code for each transaction, are cancelled by the web authentication server from the database after each successful transaction. So, if a man in the middle attacks on the user session to monitor user activities then he will get a TIC that has already been cancelled.

3. Sensitive and confidential transaction information would be encrypted before transmission over the channel. As mentioned at step 16 in Fig. 8, TIC transmission over the user session is also in strongly encrypted format and secret encryption key is uniquely generated by the web authentication server as shown at step 7 and 8 of Fig. 6.

4. We have used 128-bit shared secret logic between server and client to transmit unique secret key to the client on every login. So, there is no need to transmit this shared logic over the insecure medium since it is known at both ends.

5. Another factor of security is a SMS confirmation as mentioned in Fig. 9. A SMS does not route on the same channel which has been used in online web transaction. A SMS uses control channels over cellular networks. Security of the system also depends on the security of the messages sent by SMS, which are encrypted with A5/3 Algorithm [15].

7.4 Cell phone/PDA theft

A major drawback of handheld devices is that they can be lost or stolen. If user's phone is lost or stolen, the user can suspend their wireless service to protect themselves against unauthorized access and charges. However, it is entirely possible that an unauthorized person may try to initiate a transaction with lost/stolen cell phone. This protocol protects the user from this contingency due to the following reasons.

1. Due to above reason we assume people lose their mobile phones, they are typically reported lost and deactivated. Once deactivated, the user will no longer be able to receive SMS messages destined for user.

2. Another important issue of security is that if some person has stolen users cell phone/PDA then that thief does not know the local password of stored TICs of users cell phone/PDA. If the users bank account password is known to thief still he/she can not misuse the users account because thief has no access to the TIC codes which are stored in an encrypted format with password protection.

3. If the users cell phone/PDA is lost or stolen it is strongly recommended that the user should take necessary action of deactivation and make immediate request to the bank for cancellation of the entire issued TICs to the user.

In addition to the above scenarios we have also considered some cases which should be addressed in real implementations to maintain the reliability of the system.

7.5 Issues

We have considered below scenarios to address the various issues of real implementation of the system:

7.5.1 If merchant has generated invoice details and customer did not transfer the payment or merchant bank did not receive the payment

Our background study shows that SET protocol is a popular protocol for online payment. Our proposed work also shows that this protocol can be extended for the wireless networks and mobile devices. We referred SET strategy which is also applicable to this proposed system.
The bank confirms the successful completion of the transaction by sending them a reference/transaction number for audit purposes. At the end of the day, it also sends each merchant a database of the transactions which had transpired during the day [10, 12]. The merchant would verify a received payment from the customers everyday and dispatch the purchased goods after transfer of full payment from the customer including taxes and shipping costs.

7.5.2 If Customer has transferred the payment and customer did not receive the purchased goods

Another important issue is after transfer of payment if customer did not receive the purchased goods. To avoid the possible of this case we have used the two way authentication protocol as mentioned in Fig. 7, which authenticates the merchant and their services. Merchant authentication shows that merchant is valid and bound in legal terms and conditions of association to banking authority and it is secure for customer to do commerce with authorized merchant.

7.5.3 If cell phone has been stolen, how stored passwords are secured on hand held devices

If the cell phone has been stolen and the thief tries to break the security password of TICs then the thief would not be able to easily break the security password because it is restricted by J2ME security model. The class loader in CLDC is a built-in "bootstrap" , we can not replace or override or change configuration of class loader. The user define class loaders can be eliminated by "Sandbox" security model restrictions [32].

When a MIDlet needs to store persistent information, it can use new record store. All the persistent storages are shared by all Midlets installed on the device, the TIC's are stored in an encrypted format with the secret key known to the user which is the password of TIC's. A secret shared logic is also stored after encryption as mentioned in Sect. 4.2. This secret logic is stored in MIDlet after encryption with pin code which is protected by the MIDlet security features. In MIDP 2.0 a MIDlet suite can save data in a persistent storage area. The storage unit in J2ME CLDC is the record store. Each MIDlet suite can have one or more record stores; these are stored on the persistent storage of the device. A MIDlet is restricted by one protection domain defined by AMS (Application Management Software) to authenticate the origin of a MIDlet: The authenticated MIDlet is qualified as trusted, otherwise, it will be qualified as mistrusted. So, un-trusted applications require that sensitive APIs can only be accessed through user permission.

7.5.4 If SMS is delayed or destroyed due to network congestion

While it is expected that to implement a functional m-commerce system it is a fundamental requirement that we have a fast and congestion free connectivity of wireless cellular network, we still consider the scenario of a SMS being lost. In order to address this extreme situation we have implemented user session life time till TIC verification and successful ACK from the bank.

The user session starts after successful login using user id/password and user can logout to terminate the session after TIC validation and after getting an ACK from the bank. A SMS uses a different channel of cellular network, so there is no need to maintain the user session till the SMS confirmation. The bank authentication server notifies the user via SMS regarding the confirmation of payment transfer. If SMS is delayed and bank authentication server did not receive any SMS confirmation response in the pre-decided time interval, then the bank authentication server will resend a SMS to the customer for the confirmation of the pending transaction. It is entirely possible that the bank will receive more than one acknowledgement for the same transaction. In this case it simply rejects the duplicate one. If the acknowledgement does not come through after a specified length of time, or after a specified number of SMS has been sent, then the authentication server would assume that the

user is not interested in the transaction and would roll back the actions taken with respect to that transaction.

8 Advantages

Major advantages of the proposed protocols are:

1. It implements Multifactor Authentication in existing available infrastructure and wireless protocols.

2. Privacy at every point over the insecure network. System maintains end to end security in communication.

3. It supports mutual authentication to authenticate both the parties.

4. No need of any customization or modification to the existing network protocols.

5. Hybrid Encryption is used to protect data over insecure channel.

6. Protection against lost or stolen devices.

7. System is secure against unauthorized use of Credit Cards. Provides safeguard over the existing card based payment system.

8. Protocol is secure against the man-in-the-middle attack.

9. Business units can also adopt this protocol to secure their B2B communication with very slight modification to this protocol.

10. Application layer security solution for wireless payment system, with the existing network and physical layer security.

9 Conclusion

Enterprises are increasingly taking advantage of wireless networks to expand their business and make mode of payment easy and reachable to every user. However, financial transactions over these networks are vulnerable to various type of frauds and attacks which introduce significant security concerns, especially as enterprises must not only authenticate their customers and transactions, but must also implement a mechanism for authentication of merchant or business organization. To address this requirement we have introduced the application level security solution, secure web authentication protocol is a multifactor authentication protocol. Protocol is extended

as a Two Way Authentication to support mutual authentication and also suggested that same solution can also be implemented to secure B2B communication with very small modification to the protocol. Proposed system is secure against internet based attacks. It is also secure in case of lost or theft of mobiles devices. The protocol can be implemented within limited resources of a Java MIDP device, without any modification to the existing communication protocols or wireless network infrastructure.

References

1. White paper: AEP Smartgate Security, Strong Multi Factor User Authentication for secure information sharing, white paper, AEP Networks, December 1998, http://www.aepnetworks.com/products/downloads

2. White paper: Enhanced Online Banking Security, Zero Touch Multi-Factor Authentication, November 2006, http://www.entrust.com/resources/download.cfm/22600/EfraudWhitePaper.pdf

3. Guidelines: Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council, Arlington, October 2005, http://www.ffiec.gov

4. W. Adi, A. Mabrouk, A. Al-Qayedi, A. Zahro: (2004), Combined Web/Mobile Authentication for Secure Web Access Control, Wireless communications and Networking conference, IEEE Communications Society, pp. 677- 681. March 2004.

5. J. Gao, J. Cai, K. Patel, and S.Shim: (2005), Wireless Payment, Proceedings of the Second International Conference on Embedded Software and Systems (ICESS05), China, pp. 367-374, .December 2005.

6. S. Kungpisdan, B. Srinivasan and P.D. Le: (2004), A Secure Account-Based Mobile Payment Protocol, Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE CS press, Las Vegas USA, volume 1, pp. 35-39. April 2004.

7. Y.B. Lin, M.F. Chang, H. C.H. Rao: (2000), Mobile prepaid phone services, IEEE Personal Communications, vol. 7, pp. 6-14, June 2000.

8. A. Fourati, H.K.B. Ayed, F. Kamoun, A. Benzekri: (2002), A SET Based Approach to Secure the Payment in Mobile Commerce, In Proceedings of 27th Annual IEEE Conference on Local Computer Networks, Florida, pp. 136 - 140, November 2002.

9. Huang Z., Chen K.: (2002), Electronic Payment in Mobile Environment, In Proceedings of 13th International Workshop on Database and Expert Systems Applications (DEXA'02), France, pp. 413 - 417, September 2002.

10. J. Hall, S. Kilbank, M. Barbeau, E. Kranakis: (2001), WPP: A Secure Payment Protocol for Supporting Credit- and Debit-Card Transactions over Wireless Networks, IEEE International Conference on Telecommunications (ICT), Bucharest, Romania, Volume 1, June 2001.

11. V. Pasupathinathan, J. Pieprzyk, H. Wang and J.Y. Cho: (2006), Formal Analysis of Card-based Payment Systems in Mobile devices, Fourth Australasian Information Security Workshop, Conferences in Research and Practice in Information Technology, Vol.54, pp. 213-220, January 2006.

12. MasterCard Inc.: (1997), SET Secure Electronic Transaction Specification, Book 1: Business Description, MasterCard Inc., May 1997, http://www.win.tue.nl

13. L. Albert, K. C. Kaya: (2001), CONSEPP: CONvenient and Secure Electronic Payment Protocol Based on X9.59, 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, IEEE press, pp. 286-295, December 2001.

14. Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Sugata Sanyal and Svein Knapskog: (2007) 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

15. GSM calls even more secure - thanks to new A5/3 Algorithm ETSI: (2002), http://www.cellular.co.za

16. Jablon David P.: Integrity, Sciences, Inc. Westboro, MA, ACM SIGCOMM, September, 2005, Strong Password - Only Authenticated Key exchange, Computer Communication Review, Vol. 26, pp. 5- 26, September 2005

17. E. Limor: (2002), Using Public Key Cryptography in Mobile Phones, white paper, VP Research, Discretix Technologies Ltd. 2002, http://www.discretix.com

18. Halevi Shai, Krawczyk Hugo: (1999), Public-key cryptography and password protocols, Proceedings of the 5th ACM conference on Computer and communications security, San Francisco, Vol. 2, Issue 3, pp. 230 - 268, November 1998.

19. Itani Wassim and Kayssi Ayman I.: (2004), J2ME End-to-End Security for M-Commerce, Journal of Network and Computer Applications, Volume 27 Issue 1, pp. 13-32, January 2004.

20. Mitzenmacher M., Upfal E.: (2005), Probability and Computing: Randomized Algorithms and Probabilistic Analysis, Cambridge University Press, New York, NY.,2005.

21. Motwani R., Raghavan P: (1995), Randomized Algorithms, Cambridge University Press, New York, 1995.

22. Soriano M. and Ponce D.: (2002), A Security and Usability Proposal for Mobile Electronic Commerce, IEEE Communication Magazines, Volume 40, Issue 8, pp. 62- 67, August 2002.

23. Lawton G.: (2002), Moving Java into Mobile Phones, IEEE Computer, Vol. 35, Issue 6 pp. 17- 20, June 2002.

24. Stephan Gro, Sabine Lein, Sandra Steinbrecher: (2005) A Multilateral Secure Payment System for Wireless LAN Hotspots, Trust, Privacy and Security in Digital Business: Second International Conference, TrustBus 2005, Copenhagen, Denmark, Book Title:TrustBus, Publisher Springer, pp. 80-89, August 2005.

25. Article: Helping Consumers Prepare to Avoid Potential Threats: (2006) http://www.educause.edu/ir/library/pdf/CSD4433.pdf

26. Article: Cybersecurity a private affair: (March 2007) http://searchsecurity.techtarget.com/qna

27. Article: http://news.zdnet.com

28. Article: Legion of the Bouncy Castle http://www.bouncycastle.org

29. Article: RetroGuard for Java Obfuscator http://www.retrologic.com

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

31. William Stallings: (2003) Cryptography and Network Security Third edition, Pearson Education, 2003

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

33. Vartan Proumian: (2002) Wireless J2ME Platform Programming, Sun Micro system press, Java Series, Prentice Hall PTR, April 2002