A Multifactor Security Protocol for Wireless Payment-Secure Web Authentication using Mobile Devices

A Thesis Submitted
In Partial Fulfillment of the Requirements
For the Degree of
Master of Technology
In
Information Technology (Wireless Communication and Computing)

by

Ayu Tiwari

(MW200505)

under

Dr.Sudip Sanyal
Indian Institute of Information Technology, Allahabad

Indian Institute of Information Technology, Allahabad

July 2007

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY

Allahabad

(Deemed University)

(A Centre of Excellence in Information Technology Established by Govt. of India)

Date :_____

I/We hereby recommend that this report prepared under my/our supervision by **Ayu Tiwari** entitled "***A Multifactor Security Protocol for Wireless payment-Secure Web Authentication using Mobile Devices*** "be presented in the partial fulfillment of the requirements for the degree of Master of Technology in Information Technology Specialization *"Wireless Communications & Computing"* for Examination.

COUNTERSIGNED

_____

Dr.Sudip Sanyal

(THESIS ADVISOR)

_____

Dr. U.S.Tiwary

DEAN (ACADEMIC)

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY
Allahabad
(Deemed University)
(A Centre of Excellence in Information Technology Established by Govt. of India)

CERTIFICATE OF APPROVAL*

The foregoing thesis is hereby approved as a creditable study in the area of Information Technology carried out and presented in a manner satisfactory to warrant its acceptance as a pre-requisite to the degree for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the thesis only for the purpose for which it is submitted.

COMMITTEE ON
FINAL EXAMINATION
FOR EVALUATION
OF THE THESIS

_____
_____
_____
_____

*Only in case the recommendation is concurred in

DECLARATION

This is to certify that this thesis work entitled "***A Multifactor Security Protocol for Wireless payment-Secure Web Authentication using Mobile Devices***" which is submitted by me in partial fulfillment of the requirement for the completion of M. Tech in Information Technology specialization in Wireless Communications and computing to Indian Institute of Information Technology, Allahabad comprises only my original work and due acknowledgement has been made in the text to all other material used.

Ayu Tiwari
M.Tech. IT (Wireless Communications and Computing)
MW200505

Abstract

The Cell phones have revolutionized the way we live. Cellular phones and PDA's have largely grown in popularity and as a result users have started online banking, purchasing of internet-based products and other online services. Previous web access authentication systems have used either the Internet or the wireless Mobile channel independently to authenticate the identity of remote user.

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 hacked by the man in the middle attack and later used for making illegal access to the user's account.

Our goal is to create an authentication system that is both 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 (Short Message Service) to enforce an extra security level with the traditional Login/password system.

We have also used an encryption/decryption technique which is based on symmetric key and an iterated block cipher concept. This concept has been used to keep TICs as secret code on cell phones/PDAs and is also used to initiate secure web transaction using cell phones/PDAs. Finally we extend the system for two way authentication which authenticates both parties (user and e- service provider).

A detailed threat analysis demonstrates that the proposed system is secure against various types of internet attacks like phishing, man-in-the-middle, viruses etc.

Objective

The main objective of the present work is to provide a highly secure wireless environment for financial web transactions that is simple to use and deploy, that does not require any change in existing wireless networks or protocol. This Protocol for Wireless Payment is used to achieve secure web transaction using cell phones / PDAs. The system is based on Multi-factor Authentication concept to provide secure wireless environment to the users to increase faith of the users in online financial web transactions using mobile devices.

Acknowledgements

Before, I get into thick of things; I would like to add a few heartfelt words for the people who were part of my thesis in numerous ways, people who gave unending support right from the beginning. During this period, the faculty members and my batch mates took keen interest and participated actively. They are very efficient and qualified in their respective disciplines.

I express my sincere gratitude to **Dr.Sudip Sanyal, Indian Institute of Information Technology-Allahabad** for all his affectionate encouragement and guidance during the entire Thesis. His views and inputs are very helpful throughout the process.

I would like to thank **Prof. Sugata Sanyal, Tata Institute of Fundamental Research, Mumbai,** who suggested many related points and is always very constructive and helpful

I would like to thank **Dr. M.D. Tiwari, Hon'ble Director, Indian Institute of Information Technology-Allahabad** for the facilities and environment for research.

Not the least I would like to appreciate the support and guidance of all my Teachers specially Dr.U.S.Tiwary, Mr.Vijay Kumar Chourasiya and Dr. Ranta Sanyal and my all M.Tech. friends without whose help and support the thesis could not have been a success.

Lastly I would like to thank my family for their love, support and encouragement that they have given me through the past months, helping me to persevere in my studies. In addition, I wish to thank specially **Maa & di**, for giving me the educational opportunity that allowed me to do my post graduation.

List of Figures

TABLE OF CONTENTS

Chapter 1
Introduction

1.1 Background & Introduction

This chapter describes the background for the work and explains the selection of subject with goals and scope of the work. It shows the basic requirements and conditions for this project. At then end it presents an outline of the complete work as categorized in the remainder of the chapters.

As computing becomes pervasive, people increasingly rely their business over the Internet by using e-commerce. Now, the Internet is a preferred source to access online e-services such as e-commerce, e-voting, e-banking, e-government, etc. Online applications require a strong security feature to protect user confidential data. Security is a major issue in internet based online payment system. There are various internet threats which affect the security system of internet and increase risk for electronic transaction. Most of the authentication system relies on passwords, personal identification numbers and keys to access their personal account information. This type of authentication system can not verify or authenticate the identity of the users who he or she claims to be.

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 hacked by the man in the middle attack and later used for making illegal access to the user's account.

Financial organizations offer online services and Internet-based commerce should use secure and efficient methods to authentication their customers. The current authentication technique for online payment system is not very secure to protect users from identity theft,

as a the result any attacker gain the access on confidential information of the user like credit card number or account password and make illegal transfer of funds which will be charged to the valid user's account.

Single factor authentication increases risks posed by phishing, identify theft, online fraud and loss of confidential customer information [19, 20]. So, financial institutions should implement an effective authentication to reduce fraud and increase security for applications. Strong customer authentication is necessary to enforce security and assist financial institutions to detect and decrease user identity thefts.

The above observation underlines the need of Multifactor Authentication techniques for secure financial web transactions and to increase faith of users on wireless financial transactions. To do so in the present work we suggest an authentication system that is both 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 (Short Message Service) to enforce an extra security level along with the traditional Login/password system [18]. A detailed analysis of the proposed protocol has shown it to be resistant to various internet threats.

In the proposed protocol TICs are user specific unique transaction identification codes which are issued by bank authorities or financial institution to the user. This code is similar to OTP (One time password) and one code is used only once. They form the basis for authentication of the transaction.

In the present work we have used suitable encryption/decryption techniques that would be used to keep TICs as secret codes on cell phones / PDAs. The user can easily pick up a TIC from the stored list of TICs to initiate secure web transaction, instead of typing complicated TIC code in each transaction. 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 / PDAs.

Finally we extend our system for two-way authentication which authenticates both parties involved in transactions. Under this we would authenticate the company or service provider to the user. The proposed technique authenticates the company or service provider to the user along with the authentication of user to the financial institutions [18].

1.2 Requirements and Conditions

In the proposed work, we take the following facts into consideration:

- The user has one cell phone with java enabled service.

- On a mobile connection user has activated General Packet Radio System (GPRS) connection. In GPRS connection, the charging amount depends solely on the amount of exchanged data and not on the duration of the connection.

- To make system less vulnerable authentication should not be dependent on the web server. Web server is generally vulnerable to several types of hacking attacks. Thus, authentication is done by the separate Authentication Server offered by the financial service provider i.e. banks etc. This makes a system more secure to maintain confidentiality and privacy of customer's data.

- Cell phone should have capabilities to send and receive SMS.

1.3 Outline of Thesis

Chapter 2 describes the Factors of Authentications with some key types of online frauds. It also focuses on the guidelines issued by Federal Financial Institutions Examination Council (FFIEC) related to stronger authentication for Internet banking services which shows that effective authentication system is necessary for financial institutions.

Chapter 3 highlights some existing M-Payment and electronic payment systems with their importance and application areas. It also presents a detailed study of the SET protocols and points out some of the disadvantages of the system.

Chapter 4 provides a brief introduction to the various modes of electronic payment with the details of the proposed system specifications. It also shows the Multifactor authentication techniques used in the present work with detailed explanation on the proposed protocols for Secure Web Authentication and Two-Way Authentication.

Chapter 5 discusses the details of transaction flow of the proposed protocols, with various components involved in the system.

Chapter 6 talks about the Cryptography and Key Management of the system with the session tracking. It also briefly explains the concept of the key expansion cipher key management.

Chapter 7 provides a detailed analysis of the proposed system under various internet attacks. It talks about the system security features and demonstrates the system resistance to various internet threats.

Chapter 8 focuses on the various technologies that have been used to implement the system along with their advantages and features. This chapter also describes the tools used in implementation of the client and server of the system.

Some simulation results are discussed in chapter 9. The section provides the screenshots of the functionality provided by the developed system to make secure wireless payment. The screenshots helps to provide a closer look at the developed system.

Conclusion is given in the last chapter 10 and scope of future integration is also incorporated.

Appendix- A shows the database schema design used in simulation of the system with corresponding integrity constraints applied in the schema.

Appendix- B shows the list of server side servlets of the system with their brief functionality and purpose.

Appendix- C gives details of various commands and setting used throughout the system development process.

Appendix- D gives details of various terms and abbreviations used throughout the dissertation.

Materials (e.g. URLs, books and research papers) used & studied are given in Reference.

1.4 Summary

- The Financial organizations offer Internet based commerce and services should use an effective method to authentication their customers or users and their transaction.

- A single factor authentication such as user name and password is inadequate for user identity verification and vulnerable to various internet attacks.

- Financial Institutions should use Multi-factor Authentication techniques to increase the faith of the users on wireless financial transactions.

- The proposed system is based on multifactor authentication – TIC validation and SMS verification are the strong features of the system.

- The system also supports two way authentications to authenticate both the parties.

Chapter 2

Factors of Authentication

In this chapter we examine the necessity of having a secure technique for performing online financial transactions. The following reports and statistics, culled from various sources, clearly demonstrate the rise in online frauds.

2.1 Online Banking Fraud

2.1.1 The Rise in 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. Reuters reports shows that according to US Treasury advisor Valerie McNiven the cyber-crime raised big amount of money globally. The report shows that increasing number of attacks and the evolution of their techniques. The report from Anti-Phishing Working Group in November 2005 shows raise in number of Phishing attacks and their techniques [19, 20, 44]:

- More than 2000 companies, consisting of ISPs and banks, reported 16,882 unique phishing attacks.

- The report also shows that increase in the number of fake URLs hosting to steal user passwords.

2.1.2 Key Types of Online Fraud

The Online fraud has been categorized broadly into two categories as mentioned in [20]:

1. **User Identity Theft:** the user's secret information required to access the online systems is stolen through means that include:

❖ Phishing attacks which trick the user into providing access information.

❖ Key-loggers and "spyware" which clearly capture access information.

2. **User Session Hijacking** – Attacker gets control over the active user session and monitors all user activities. In this attack all user's online activities are monitored using malicious software ("malware"). Malware software for Session hijacking can run on a user's local computer, or remotely as a attack on "man-in-the-middle".

❖ Local malware session hijacking attack performs host file redirection.

❖ Remote malware session hijacking attacks performs DNS hijacking and Content Injection.

2.1.3 The Spirit of the FFIEC Guidelines

The FFIEC was established in March 1979 to recommend uniform principles, standards to promote consistency in the administration of financial agencies. The Council has five member agencies: the Board Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration and the Office of the Comptroller of the Currency. In a press release the Federal Financial Institutions Examination Council (FFIEC) issued guidelines on October 12th, 2005 related to stronger and secure user authentication for Internet

banking services it also recommend that financial institutions should use effective authentication system to reduce fraud [20].

Main highlights of the FFIEC Guidelines

- Financial organizations offering online services and Internet-based commerce should use secure and efficient methods of customer's authentication.

- Authentication techniques based on single-factor authentication may not provide sufficient protection for Internet-based financial services.

- The FFIEC agencies consider that financial institutions should implement multifactor authentication to reduce fraud and increase security for applications.

2.2 Factors of Authentication

2.2.1 Authentication Methodologies

Existing authentication methodologies have basic three "factors" [19, 45]:

- **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).

Authentication methods those are based on more than one factor are more difficult to break and secure than single-factor methods. Efficiently designed and implemented multifactor authentication methods are more reliable and secure to reduce online frauds.

2.2.2 Selection of an Authentication key

Selection of an appropriate authentication key is one important characteristic of securing online services [44].

1. Passwords

A password is a type of secret authentication data which grants access to only authorized users. The password is known to the only authorized users and unauthorized persons are unaware of this, and user wish to gain access must be tasted to verify the authnticity of the user by checking the password. The passwords are universally used to keep authorization. However, password systems are vulnerable to many attacks and attackers can recover the user password by some attack. Additional protections have been implemented to protect the data communication channel to make password confidential, but this is not completely secure against attacks. Many security experts now realized that passwords are not secure mechanism to protect user confidential data; passwords can be hacked easily by hacking attacks [44].

2. Hardware tokens

A hardware token is physical device, it is a hardware implementation of the authentication device attached to an authorized user's computer. Hardware token is a specialized physical device that protects secrets (cryptographic keys) and performs cryptographic operations. The cryptographic operations are used to secure the communication channel and authentication of parties [44].

Some of the major drawbacks of hardware tokens are:

- It Increases the implementation cost, and complex functionality required in implementation and deployment.

- Reduced ease of use for customers.

3. *Software tokens*

Software tokens are similar to hardware tokes. It is software implementations of hardware tokens. Software tokens run on the PC or on a separate multi-purpose device but hardware tokens are stored on an external device away from the PC. Software tokens support authentication of both parties and protect the used communication channel to transmit data for authentication [44].

The major issues with software tokens are:

- Software tokens can be copied easily

- They may be copied without knowledge of user.

This could be happen if the system is less secure in protecting the secret. The main advantage of software token is low cost.

4. One-time passwords

The one-time password (OTP) based system is more secure then ordinary password based system, it is diffcult break and secured from unauthorized users. In this type of system passwords get updated constantly, for each access user has new password so it reduced the risk. Special algorithms are used to generate a series of passwords. Each password of the succession is called a one-time password as it is different from the other passwords and each password is used only once. Many types of one time password generation system are available to protection against attacks [44].

Some advantages for one-time passwords systems are:

- They are very easy to use

- This type of systems has lower cost and complexity as compared to the cost of software and hardware tokens.

- One time password reduces the risk of attack against traditional passwords.

5. Biometrics

In Biometric authentication human physical and behavioural characteristics are used to verify the identity of the user. Biometrics is well suited to local access control rather than remotely access authentication. In case of remote access based on biometric authentication user's personal data are used for authentication, significant privacy issues arise with the collection, storage and use of such information. Special care must be taken in case of remote authentication because user's personal data travels on communication network for authentication [44].

The financial agencies consider that single-factor authentication is not appropriate for financial transactions or access to customer information or online transfer of funds [19, 20]. The tools used in single-factor authentication are passwords and PINs, have been widely used for online banking and in e-commerce, including account balance inquiry or online payment. However, financial institutions should assess the security of such authentication techniques and protect their customer's data from various online threats such as phishing, malware access and pharming. Where risk assessments signify that the use of single-factor authentication is not appropriate, financial institutions should implement multifactor authentication. Multifactor Authentication will increase the system security by providing an additional authentication "factor" further than the traditional login/password.

2.3 Summary

- Recent studies have shown that there is increase in online fraud or identity theft.

- Online frauds are widely categorized in two categories – User Identity theft and User Session hijacking.

- FFIEC has issued guidelines which show that single factor authentication is not secure and vulnerable to various online attacks, so financial institutions should implement multifactor authentication system.

- Selection of an authentication key is an important issue in multifactor in authentication.

Chapter 3

Introduction to existing Payment System

Mobile Payment (M-payment) is a wireless payment system that has raised the attention of researchers in the last few years. M-Commerce payment can be conducted in several ways and is based on "any–where, any-time" paradigm. M-payment is a critical component in M-commerce or E-commerce applications. According to the world wide forum, M-payment on a mobile device would be very popular and provide tremendous opportunities for M-commerce in the coming years.

Secure Wireless payment system has become an important research area in the last few years. There are various types of electronic payment solutions are available for internet based commerce. According to Gao et al. [2], mobile payment means wireless based electronic payment for M-commerce to support point-of-sale/point-of-service (POS) payment transactions using mobile devices such as cellular phones, smart phones and personal digital assistants (PDAs), or mobile terminals. In general, M-payment systems is widely used by merchant to make wireless based payment, content vendors, and information and service providers to process and support m-payment transactions based on wireless commerce applications. As discussed in [2], the existing m-payment systems can be classified into three major types.

The first type is known as account-based payment systems, in which each customer has a valid account maintained by a Trusted Third Party. The user can initiate pre-paid or post-paid financial transaction. There are three subdivisions of account-based M-payment systems:

1. The payment system based on mobile phone, which facilitates the customer to do commerce and make payment over mobile phones,

2. The Smart Card Payment systems, and

3. Credit-Card M-payment systems, the users can make payment via of credit cards using their mobile devices.

More details about different account-based payment systems are discussed in [3, 4, 5, 6].

The second type of m-payment system refers to the mobile POS payment systems by which customers can purchase products using vending machines or online website with their mobile devices. There are two types of POS payment systems:

1. An automated POS payments, which are frequently used in immobile terminals such as vending machines, parking meters, etc.;

2. Attended POS payments, in which mobile users can make payments with the assistance from a service party such as a taxi driver, a counter clerk, etc.

A typical example of mobile POS payment system is Ultra's M-Pay (http://www.ultra.si/).

The third type is E-wallets or E-cash. In this method customers stores digital cash in their E-wallet from a debit card, credit card or virtual check. Digital cash is like electronic cash in virtual savings account where the user can make payment for their purchases. E-wallets are frequently used in micro payments or small payments. Customers can obtain E-Wallets from their financial institution, specific merchants, or technology providers to make payments [2].

3.1 A SET Based Approach to Secure Wireless Payment

The objective of the present work was to develop a wireless payment protocol which supports credit card payments as well as debit card payments in a secure manner. Two existing protocols were taken into consideration: the SET protocol, On-line payments [7]. This section provides a brief overview of the protocols.

3.1.1 Secure Electronic Transaction (SET)

The Secure Electronic Transaction is an open encryption and security specification designed to protect credit card transactions on the Internet. Companies involved in the development of the SET are IBM, Microsoft, Netscape, RSA, Terisa and Verisign. It is supported by major corporations such as VISA Inc. and MasterCard. Although SET had been designed to operate in a wired infrastructure [7, 5, 34], its transaction flow and implementation of security are of interest to us since it can also be employed in a wireless scenario.

The SET protocol is basically used in existing credit-card based payment system and provides enhanced security to web based financial transactions as well as authentication of transaction and involve identities by registration and certification. SET is also an international standard with published protocol specifications.

In Figure 1 on next page we show the flow of messages in the SET protocol. In a typical scenario, the merchant's site will be accessed via the Internet by customers using their personal computers. While the SET protocol permits customers to make credit-card payments to any of the merchants offering a web-based service, customers also have the option of paying for other types of services using the on-line banking facilities (Internet) [7, 8, 34].

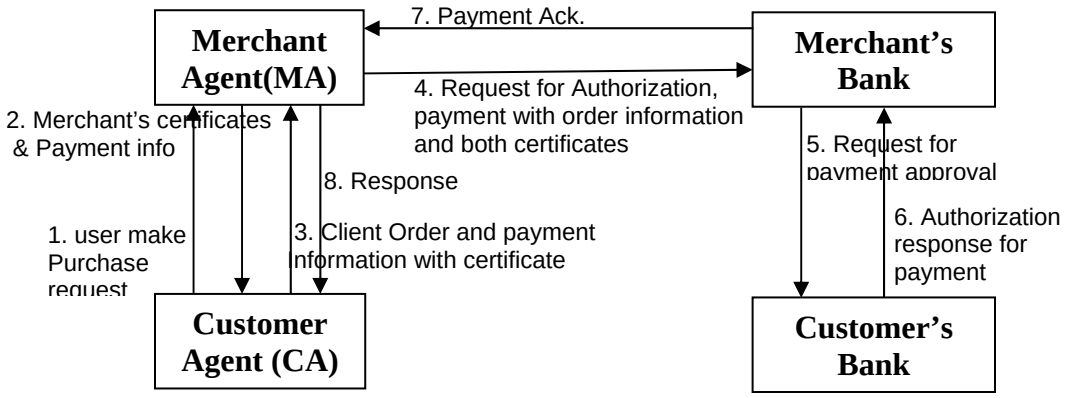


Figure 1: Transaction flow in Secure Electronic Transaction (SET)

A brief description of the SET protocol, as depicted Figure 1, is described below:

1. The customers visit the merchant's web site to select various goods for purchasing and get the total cost of all the selected goods, 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. Special software on the consumer's PC, called Digital Wallet, is invoked and it give choices to customer to select one credit card from the list of credit cards issued to customer.

4. The consumer selects the card to make payment, and the electronic transaction take place based on SET protocol.

5. After getting details of customer payment the merchant contacts the merchant's Bank for customer authorization and payment.

6. Merchant Bank will contact the customer's Bank for the same and get approval of payment.

7. Merchant will notify, if transaction is successful.

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

On-line Payment services provided by most of banks, allow customers to make payments online to various persons or organizations that have previously registered themselves with the banks. Customers making online payment provide account number and type (i.e. savings, cheque etc.) and the amount to be transferred to the institution website. The bank generates transaction/reference number to confirm the successful completion of the transaction. At the end of the day, it also sends details of all the transactions carried out in the favor of merchant during the day for audit purpose [7, 34].

3.1.2 Disadvantages of SET

SET is a good example of a protocol that is not completely secure in user authentication. SSL-based methods are ignoring essential "security" necessities [10]. Some disadvantages of SET are:

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

2. As the SET protocol was designed to maintain the traditional flow of payment data (CA – MA – Merchant's Bank), There is a need of an end-to-end security mechanism.

3. The third element is the direction of the transaction flow. In SET, transactions are carried out between the Customer Agent and the Merchant. So it is vulnerable to various attacks like merchant can modify transactions data by altering the balance.

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

5. There is no notification to the Customer from the customer's Bank after the successful transfer. The user has to check his/her balance after logging on bank website again.

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

3.2 E-wallet or Digital cash

Jan Ondrus in [41] has given details on Digital cash or E-cash which is a method of money transfer, this method of the payment is electronic transfer of fund using computers via internet or on mobile phones via GPRS connection to use internet or Blutooth.This method of money transfer is easy and flexible to the users. Digital cash is also frequently used in day to day life to make small payments.

Digital cash system has many advatages which makes customers life easy, it also has some disadvantages which include fraud, device failure, tracking of perticular person and reduction in human social interactions. According to the facts given in [40], fraud over digital cash has been a pressing issue in recent years. It includes illeagle access of customers bank account and unauthorized acces of user private banking information which has increased the information hacking and identity theft. Some popular types E-wallet and Digital cash are briefly explain from [42] in next sub sections :

3.2.1 Electronic Purse

Electronic purse is a system which facilitates customers not to carry cash with them for small payments. It is based on smart card technology which is similar to pre-paid financial card. Some advantages and disadvantages and example of existing system are given below for more detail on Electronic purse please refers [42].

Advantages

- Very easy in use.
- Capability to hold various currencies, simple payment based on P2P.
- Consumers and retails are free from cash handling.

Disadvantages

- Generally used in small payments.
- There is no global standard for this type of payment system.
- Electronic Purse is Bank dependent.

Existing Applications

Proton electronic purse developed by Banksys, Other smart card based electronic cash systems are- Mondex, Visa Cash, Manmont

3.2.2 Distributed Wallet

A distributed wallet is a payment system which initiates payment transaction via installed software on the consumer's computer which interacts via Internet to the wallet servers to make payments. The client machine first makes a connection to the server machine using a connecting protocol for the user authentication and to make payment. Some advantages

and disadvantages and example of existing system are given below for more detail on Distributed Wallet please refers [42].

Advantages

- It works on smart card and secret PINs.
- There is no need of Merchant subscription to make payment via distributed wallet service if the wallet client supports the payment system based on SET protocol.

Disadvantages

- The complexity of Distributed wallets is higher than remote wallets and it also require large messaging sequence to run on dissimilar environment.
- There is no any protocol which activates client side module of the distributed wallet to make interfacing with multiple wallet servers.

Existing Applications

Distributed wallet specification is available as a GlobalSET

3.2.3 Personal Wallet

A personal wallet is a software or hardware installed on user's machine. There is no need of server, because payment transaction does not require any wallet server. The user's credit information is stored locally on the user device. Some advantages and disadvantages and example of existing system are given below for more detail on Personal Wallet please refers [42].

Advantages

- Implementation cost is very less

- Ability of offline payment.
- Advanced and strong security feature.
- It can also works on smart card and secret PINs.
- All card information and user's confidential and personal data are in control of user.

Disadvantages

- Need large storage capability on user device.

Existing Applications

SET based system - IBM Consumer Wallet, Ilium Software launched eWallet

3.3 Combined Web/Mobile Authentication for Secure Web transactions.

The hybrid approach of authentication is proposed by Adi W. & Al-Qayedi A in [1] which enables strong authentication by combining two factors to authenticate the user. First authentication approach is a traditional Web-based username/password and second one is a Mobile-based challenge/response authentication. Results in [1] show that the combined system has resistance to eavesdropping attacks and provides security by maintaining secure remote authentication server. This system functions well in existing infrastructure and 3G mobile networks or pervasive computing environments.

3.3.1 Combined Web/Mobile Authentication

The above cited work, [1], proposed one of the combined Web/Mobile user authentication approach before making payment transaction. It uses browser based

system for online transactions with cellular network for user verification. Their approach mainly operates as follows:

1. The user can start transactions from computer using internet and complete it over cellular network based GSM network, in this approach Network Service Providers are also involve in completion of transaction.

2. The user can start transaction via making simple request on internet via their computer before making payment.

3. The customer will get invoice detail of purchased goods by which they can collect their purchased goods after making full payment.

The protocol relies on SMS messages, i.e., after validation of user password user will get SMS from the web server to authenticate their identity. Then the user will proof their identity to the authentication web server via sending an encrypted image from their mobile to the authentication server. The above described authentication must be done with in a pre-decided fixed time frame.

3.4 P2P (Point to Point) Payment System

P2P-Paid is a mobile based payment system, its development process is a part of research at San Jose State University in 2004. The main objective of this system is to develop wireless payment protocol which initiates wireless payment transactions over cell phones. As mentioned in [2], in the existing mobile payment system transactions are carried out on Internet. P2P protocol for wireless payment supports online financial transactions over internet as well as peer-to-peer mobile payment transactions on mobile phones to make small payment using a Bluetooth technology of cell phones over wireless network [17].

The basic purpose of the P2P-Paid payment protocol is to make secure and convenient payment using a lightweight protocol over Bluetooth communication. The user can make secure P2P financial transactions by using various options available to mobile users in this protocol. These options include device/service discovery for Bluetooth connection, make request for money, transfer money, management of all financial transactions, etc.

3.4.1 Components of P2P Payment Protocol

As referred to [2] the Payment protocol can be divided into two parts:

1. Mobile client to Server Communication Protocol.
2. Mobile Client to Mobile Client Protocol.

3.4.2 P2P-Paid system Client Functionality

As referred in [2, 17] mobile client interface supports the following functionalities in P2P-Paid system:

- **P2P party discovery:** It discovers the users Bluetooth devices over Bluetooth network to connect them each other before making payment.

- **P2P session management:** After making discovery and connection between Bluetooth devices, it generates P2P payment session for secure exchange of money and drop session after completion of transactions.

- **P2P payment management:** The users can make P2P mobile payment transaction over the Bluetooth network under secure session. The payment transactions in P2P payment protocol are based on 2-D payment transaction protocols.

- **Account management:** This option supports various operations of account management such as account balance enquiry and displaying an account summary.

- **Payment scheduling:** The user can update, delete and view their payment schedules using mobile phones.

- **Payee management:** By this function user can add new payee information or remove existing payee details or view existing payee information. Payee management is required before making payment.

3.4.3 P2P-Paid System Server Functionality

The server works with installed middleware by communicating with mobile client software to provide wireless payment. As referred in [2, 17] the functionality of Server in P2P-Paid protocol is as follows:

- **P2P communication:** A mobile client makes a connection to the server using a peer-to-peer 2-D payment protocol to start all mobile payment transactions.

- **User management:** It supports user registration system and maintains user information.

- **P2P- Paid account management:** It manages the user account information to maintain user account.

- **Bank Account Management:** It maintains account detail at server side with security, confidentiality and data consistency.

- **Schedule management:** It stores the user schedules of all mobile payment, including addition, updation or deletion of a payment schedule for mobile user.

- **Payment Management**: It maintains the records of all the mobile payment transactions with there status.

- **Session Management:** It generates a P2P payment session for secure exchange of money and control this session till completion of transactions.

- **Security management**: It maintains the various security controls such as access control authentication, security key management, encryption/decryption, etc.

3.5 Summary

- The Secure Wireless payment system has become an important research area in last few years. 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 such as cellular phones, smart phones, and personal digital assistants (PDAs). M-Payment is classified broadly in three categories :

  - Account-based payment systems,
  - Mobile POS Payment system,
  - E-wallets or E-cash.

- The Secure Electronic Transaction is a Card based payment protocol, SET is also an international standard with published protocol specifications. Many leading Companies like IBM, Microsoft, Netscape, RSA, Terisa and Verisign are involved in the development of SET. SET is designed for wired networks so do not meet the all the challenges of wireless networks.

- E-wallet Digital cash or E-cash is a method of money transfer, this method of the payment is electronic transfer of funds using computers via internet or on mobile

phones via GPRS connection to use internet or Blutooth. Many types of digital wallet systems are availables of which Electronic purse, Distributed Wallet and Personal Wallet are famous examples.

- The P2P-Paid payment protocol is a wireless payment protocol which initiates wireless payment transactions over cell phones to provide a convenient, secure money transfer over Bluetooth communication protocol. P2P Payment systems are frequently used for micro payments and it works for the payment between the mobile client to mobile client or mobile client to P2P web server.

Chapter 4

System Specification and Architecture

Various forms of existing electronic payments have been considered in the previous chapter where we also examined their advantages, disadvantages and domain of applicability. In the present chapter we develop the basic ideas of the present work. We first discuss the modes of payment and the role of multifactor authentication. This is followed by an overview of the protocol developed by us for client and transaction authentication. This is then extended to build a protocol for two way authentication.

4.1 Mode of Payment

Electronic payment systems are classified in three groups as mentioned in [43]:

1. Credit card based systems
2. Debit card based systems
3. Electronic checks and Account Transfers

4.1.1 Credit card based systems

Credit cards are a pre-agreement repayment system, credit card issuers and the acquirers are members of a card association, e.g. Visa or MasterCard. Issuers are bank authority. The merchants accept credit cards for payment they required necessary infrastructure, they have association with acquires who provide equipments for credit card payment. Credit card payments can be made both when being physically present or over telephone or Internet [43].

4.1.2 Debit card based systems

Debit cards have payments set against an account with a pre-agreed deposited scheme. It is similar to an ATM card. Both the Debit card issuers and the acquirers are members of a card association, e.g. SBI ATM Card, City Bank ATM Card etc. Normally all of them are banks. The merchants have association with the acquirer, who provides the necessary infrastructure to the merchant for accepting Debit card payments. Debit card payments can be made both when being physically present or over telephone or Internet [43].

4.1.3 Electronic Transfer systems

Electronic payment rely on the Internet to make money transfer which is based on centralized account model, generally association is required between both the payer and the merchant's financial institutions to make money transfer or both parties has account in the same financial institution. The transfer is simple from one account to another. In case of centralized account situation the major issues are ways for debiting the accounts and account holder authentication for funding [43].

4.2 Multifactor Authentication

As emphasized in the previous chapters, we need a strong authentication mechanism when using electronic transfer systems. Single factor authentication is considered to be inadequate for this purpose. Thus, we need multi factor authentication.

Multi Factor 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. In our system we are using multi factor authentication using two different modes. The implementation is performed using TIC and SMS. While SMS

has been used in previous approaches to the problem [1], we are introducing the new concept of TIC as a novel method of authenticating a transaction and the user.

1. TIC Authentication: TIC (Transaction Identification Code) Authentication is the technique which is used to identify both the user and the ongoing transaction. TIC code 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

TIC codes are:

- Issued by the Bank or Financial institution to its customer.
- 8 bit or 16 bit Pseudo randomly generated code which is assigned to the customers.
- May be complicated digit sequence or combination of numeric or alpha numeric characters.
- One TIC code is used only once, i.e. a unique TIC is used for each transaction.

Here we are assuming financial institutions are responsible to store TIC generation logic and algorithm confidentially and they have their specific parameters to decide the complexity of TICs format. Financial institutions are also responsible for upgrading from time to time the TIC generation logic and data and also to keep it absolutely secret. The user will get the list of TIC codes from the bank or financial institution according to its requirement.

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 (i.e. each TIC code is used only once). We can also decide a validity time period of TICs according to issuing organization policies, which provides an extra security feature in the system.

2. SMS Authentication: Another method to validate user transaction is an SMS confirmation. The Bank or financial institution stores user cell phone number to provide

multi factor 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.

We believe in above reasonable assumption given in [1] that when user lose their mobile phones, they make complain of lost phone and take necessary steps to deactivate their SIM. After deactivation of SIM, user would not be able to receive any SMS generated for them.

Our user authentication system attempts to resolve some of the issues associated with the previously mentioned systems.

So, multi factor authentication is used to verify user identity by using following steps:

4.2.1 Web-Based Basic Authentication

Firstly, the user has to prove their identity to the web authentication server using a web-based username/password basic authentication process.

4.2.2 TIC Authentication

After authenticating the user using username/password, the web authentication server demands a TIC code from the user. Now Cell phone/ PDA user will insert a one time TIC code to uniquely identify their transaction and prove his/her authentication to the web

authentication server. TIC code would be selected from the stored list of TICs which were issued by authorized financial institution and uniquely assigned to its customers.

4.2.3 SMS Confirmation

After the TIC code identification and validation the remainder of the transaction will proceed. At the end of the transaction the user will get an SMS from the web authentication server to confirm his/her financial transaction. By this SMS user can confirm their transaction by “YES” or “NO”. If user chooses yes then transaction would be committed on the server and if the user denied then transaction would be cancelled. The security of the proposed system also depends on the security of encrypted messages sent by SMS and WAP, A5/3 Algorithm is used for message encryption as mentioned in [23].

4.3 System Architecture

In this section we present the basic flow of messages for implementing the proposed protocol. This also allows us to identify different components of the system and their functionalities.

4.3.1 Secure Web Authentication Protocol

Figure 2 shows the Protocol for secure web authentication using Cell Phone/PDA. 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. As illustrated in Figure 2, following are the steps:

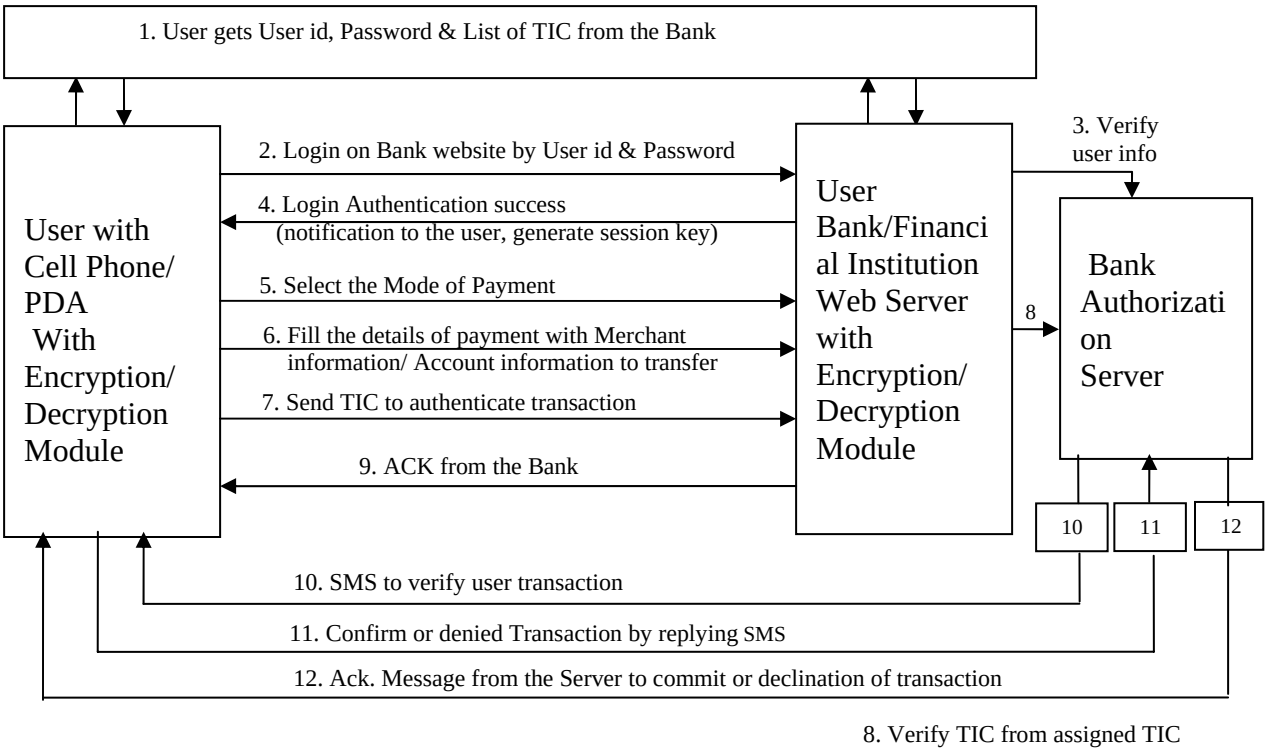


Figure 2: Protocol for wireless payment: Multifactor secure Web authentication protocol using mobile devices

Below we describe each step of the above protocol.

1. User gets username/password and Transaction Identification codes (TICs) from the Bank. Each user has only one username/password to their account, but TIC code is unique for each online transaction. So users will get list of TIC codes from the bank authority or authorized financial institution according to their requirement.

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 will insert a TIC code by simply choosing a TIC code from the stored list of TICs. Note that TICs are stored, with password protection, with a local encryption on the cell phone. The user will decrypt and insert the TIC in the financial transaction to give unique authentication to each web transaction. All details of the transaction, with attached TIC, 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 list of TICs that have been issued to the user. Discussions on the encryption/decryption technique used in the proposed system are given in chapter 6.

8. The bank authorization server decrypts the received message and extracts the TIC. It then verifies the TIC received from the user by comparing it with the stored list of TICs in the user account information at server database. If both TICs match then it cancels the used TIC from its database and goes to the next step. If no TIC 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.

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.

In the above module all the transactions from client to server or vice versa are strictly in encrypted format. Encryption and decryption module is installed on the cell phone/PDA of the user and on server side environment. Cryptography module discussed in more detail in chapter 6. From the above description we can see that after authenticating the user using the basic login/password mechanism, the user and transaction are authenticated again using the TIC mechanism and the transaction is again verified using SMS. Thus we have multifactor authentication and verification steps, using different media.

4.3.2 System for Two Way Authentication which authenticates both the parties

Mutual authentication is a process by which the web site (i.e. the service provider or merchant) is authenticated to the customer along with authenticating the customer identity. Currently most financial institutions do not authenticate their Web sites to the

customer before collecting sensitive information. One reason for the success of phishing attacks is that unsuspecting customers cannot determine that they are being directed to spoof web sites during the gathering stage of an attack. Financial institutions can provide authentication of their web site to the customer which helps customers in selection of legal web sites over spoofed site. After having analyzed the Secure Electronic Transaction (SET), on-line payments [6, 10] 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. We extend the protocol to support two-way authentication in the present section i.e. we would like to authenticate the merchant / vendor / service provider to the user in addition to authenticating the user and the transaction. This is a necessary addition since, in E-commerce and M-commerce applications, the user may not be aware of the authenticity of the merchant or service provider. In fact this is the main reason why phishing attacks are so popular and successful.

In order to develop a system providing two way authentication we have considered five major components with their certain roles as shown in Figure 3 below:

1. **User:** A user is a valid account holding customer of the bank,

2. **Customer Agent (CA):** CA is a software module which is installed on the user's mobile device.

3. **Merchant Agent (MA):** An MA is an online service provider and merchant website by which the users perform online purchasing / transactions.

4. **Customer's Bank:** This is the bank at which the user has a valid account, it also contains the authentication server necessary to authenticate the users and their transactions.

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 services.

The two way Authentication protocol starts when the MA sends an invoice detail to CA related to purchase goods with payment information and terminates when the MA receives acknowledgement of received payment from Merchant's bank [7] as shown in Figure 3, the flows for the payment transactions are as follows:

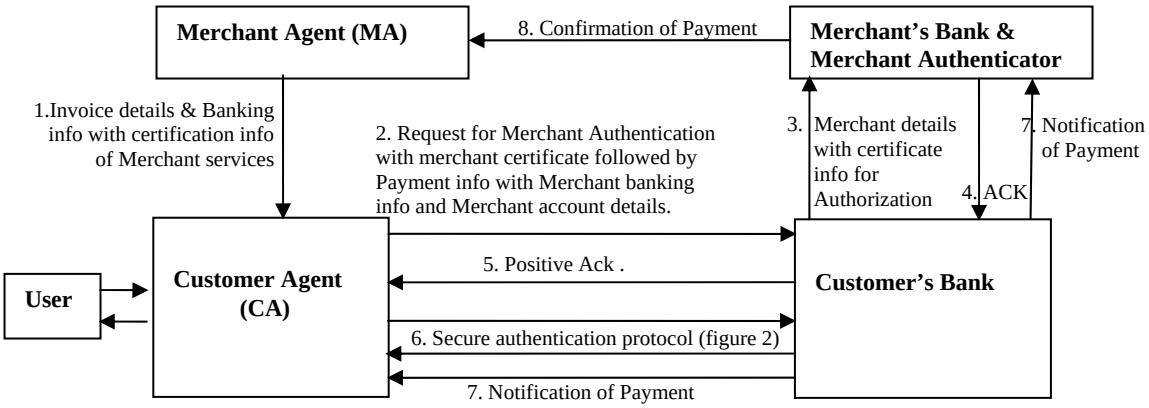


Figure 3 : Protocol for Wireless Payment : Two Way Authentication

1. The MA generates an invoice related to purchasing detail and sends the Merchant's encrypted banking information and authentication certificate with the invoice and payment 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 Merchant authentication certificate provided by the MA.

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

4. The Merchant Bank / Authentication party 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 Customer's bank sends positive ACK to the CA and goes to the next step or if merchant certificate is not valid, the Customer bank will notify the CA with that information. If Customer Bank received negative or suspicious ACK of the merchant authentication it simply rejects the user transaction with valid security reason.

6. After valid authentication of merchant, here secure web authentication protocol will run as shown in Figure 2, to authenticate customer before making payment. If the Customer Bank received positive acknowledgement of the Merchant it demands a TIC for Customer authentication. After a TIC validation it sends a confirmation SMS to the customer to verify their initiated transaction. For more details on Secure Web Authentication protocol (Figure 2) please refer to section 4.3.1.

7. After getting an SMS confirmation from the customer, the customer Bank will send payment notification to the Merchant bank as well as to the customer with the customer details and payment detail.

8. Merchant Bank will send confirmation of received payment from the customer to the MA with relevant details such as invoice number and customer id and amount received.

In this proposed architecture we do not route payment transaction data via the MA. As a result, the implementation of security is less onerous. We do not route the customer payment instructions from the merchant portal, so payment details cannot be modified by the merchant.

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

- Confidential and private data of user is never available to the merchant in an unencrypted manner because transaction flow is not from merchant site.

- Moreover, even if the cell phone is stolen and the user's login password is available to the thief, the system is still secure, because the TIC's are also encrypted and they can be accessible only by a key known to the valid user.

- The protocol is also secure against "man-in-the-middle" attacks since at no stage do we send unencrypted data over untrusted network.

- We have the benefits of OTP since each TIC is used for only one transaction.

The proposed system is secure from various internet attacks as described above. A complete threat analysis has been presented in chapter 7.

4.4 TIC Generation and Distribution

Another important module in the protocol is generation of TIC codes at the financial institution server, distribution of TIC's to the customer and encryption of TIC's before storing them on client environment. TIC codes are pseudo random codes and can be generated with pseudo random number generation algorithm as mentioned in [16,36,37]. TIC generation logic is strictly confedentential at the web authentication server and we are assuming that the banks will update TIC generation data and improve TIC generation algorithms. The authorized person of the financial institution is responsible for the distribution of TIC's to the user cell phone via simple data cable device and distribution process includes the encryption of TIC's to maintain security confidentiality. At server side, we have assumed TIC's are stored in database and there is strong security of Database management system (supported by Oracle 9i) and operating system with secure firewalls to protect server side data.

We have also implemented a module which generates TICs on the server and load them on the client environment in an encrypted format. It makes TIC distribution easy and reduces the repeated visit of the user to the bank or financial institution.
The user can make request to the bank server to generate TICs and user has to produce a valid secret code before TIC generation. This secret code may be the user's ATM debit card secret pin code or some other confidential four digit code. To make system less vulnerable users can generate limited number of TICs at a time.

Loading process includes the local encryption of TICs before storing them on client environment. An encryption/decryption techniques used are discusses in detail in chapter 6.

4.5 Summary

- Electronic Payment system, a very popular way to make online payment, is broadly classified in three types:
    1. Credit Card based Payment System
    2. Debit Card based Payment System
    3. Account based Electronic Transfer.

- As discussed in chapter 2, Single factor authentication is not secure for online financial transactions. So a new protocol is proposed which is based on multi factor authentication techniques.

- The Secure Web Authentication protocol is developed. It works on the following steps of authentication :
    1. Web based basic authentication (User name and Password)
    2. TIC (Transaction Identification Code) authentication.

3. SMS confirmation (by “YES” or “NO”).

- TICs are pseudo randomly generated codes assigned to the customers from financial institutions or banks. Note that the TIC is unique for each transaction.

- Proposed protocol is extended for two way authentication to authenticate both the parties (Merchant and User).

- In the proposed authentication protocols customer confidential information of payment is not routed via merchant site, so merchant can not alter or copy the confidential data of users. As a result implementation of security is less onerous.

Chapter 5

Transaction Flow of Protocol

In the previous chapter we presented an overview of the protocol proposed in the present work. In this chapter we look at the detailed message flow of our system. This is necessary in order to perform a detailed threat analysis. As mentioned in the previous chapter, we have considered five major components in describing transaction flow of the proposed system:

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

We explain the message flow in four parts with each representing one phase of the total process. The message flows are shown using sequence diagrams along with detailed explanations. The phases consist of:

1. The first authentication of the user by the bank authentication server i.e. the basic login and password based user authentication.
2. Two way authentication i.e. authentication of the merchant / vendor / service provider.
3. The second authentication of the user and the transaction using TIC.
4. The final authentication and confirmation of transaction by the user, using SMS.

5.1 Part I: First Authentication of User to the Bank Authentication Server

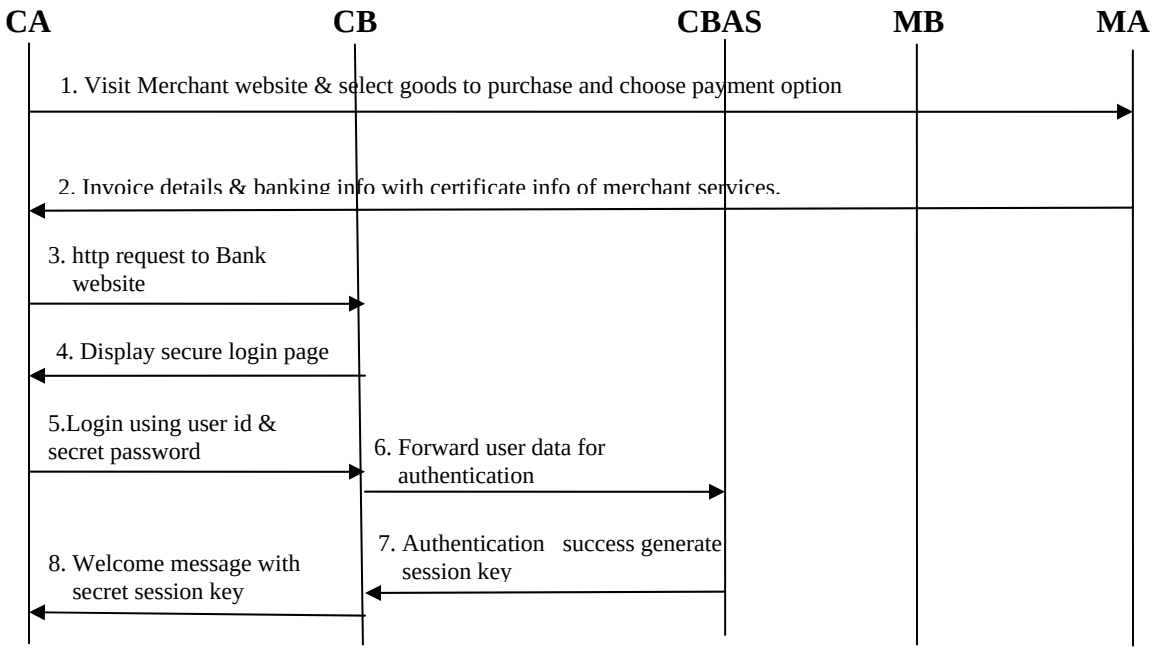


Figure 4: First authentication of User to the Bank

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

2. The merchant web server (MA) generates invoice details and the merchant banking information with the merchant authentication certificate and sends to the CA in an encrypted format. 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 his/her 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 logs in using user id and secret password known to user only. Before transmitting user's login details from client to server they will be encrypted using symmetric key cryptography which is implemented on bank server and on user cell phone by standard security mechanism.

6. The user details will be forwarded to the local bank authentication server. Note that to maintain strong security mechanism we have recommended to maintain separate authentication server at the bank or financial institution.

7. At authentication server user's login data will be decrypted and matched with its secure database records of customers. On success, it generates a random session key which will be encrypted by shared secret logic (mentioned in chapter 6) and transferred to the Bank web server.

8. The CB will send general textual welcome message and session key to track the user session to the user (CA). If the first user authentication will fail then it will send invalid login message to the user.

After successful completion of first authentication of the user by login/password, two way authentications take place as mentioned in part II.

5.2 Part II: Two Way Authentication: Authentication of Merchant to the Customer

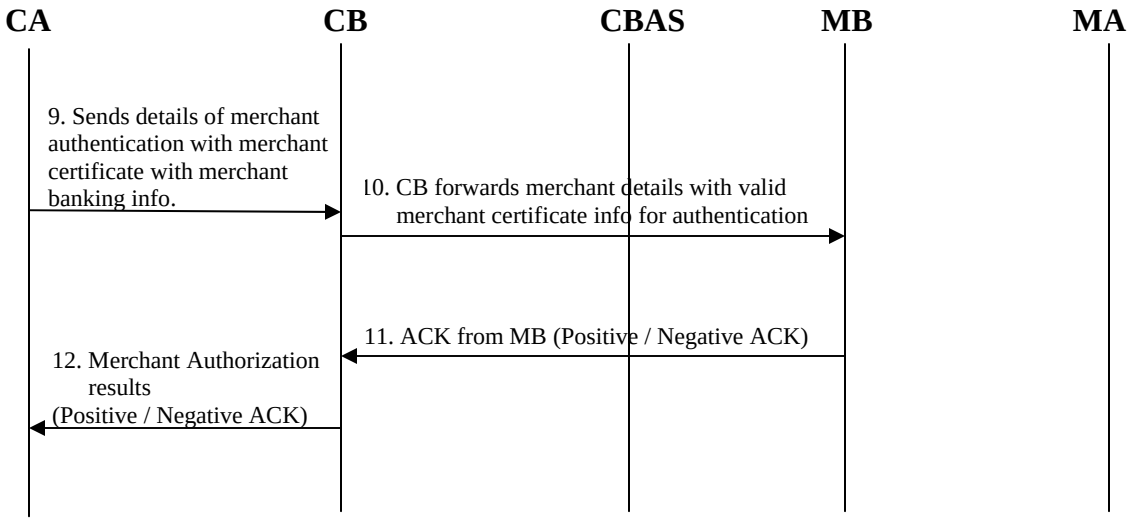


Figure 5: Two way Authentication

9. The user (CA) will send the request to the user's bank for merchant authentication before making payment to MB. The CA will forward details of the merchant received from merchant 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 bank to authenticate the merchant. Each merchant has legal authorization certificate which has been issued by 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 make payment it will run multifactor secure web authentication protocol as mentioned in Figure 2 in previous chapter. Detailed explanation of the transaction flows of this protocol is mentioned in part III.

5.3 Part III: Second Authentication of User to the Bank Authentication Server

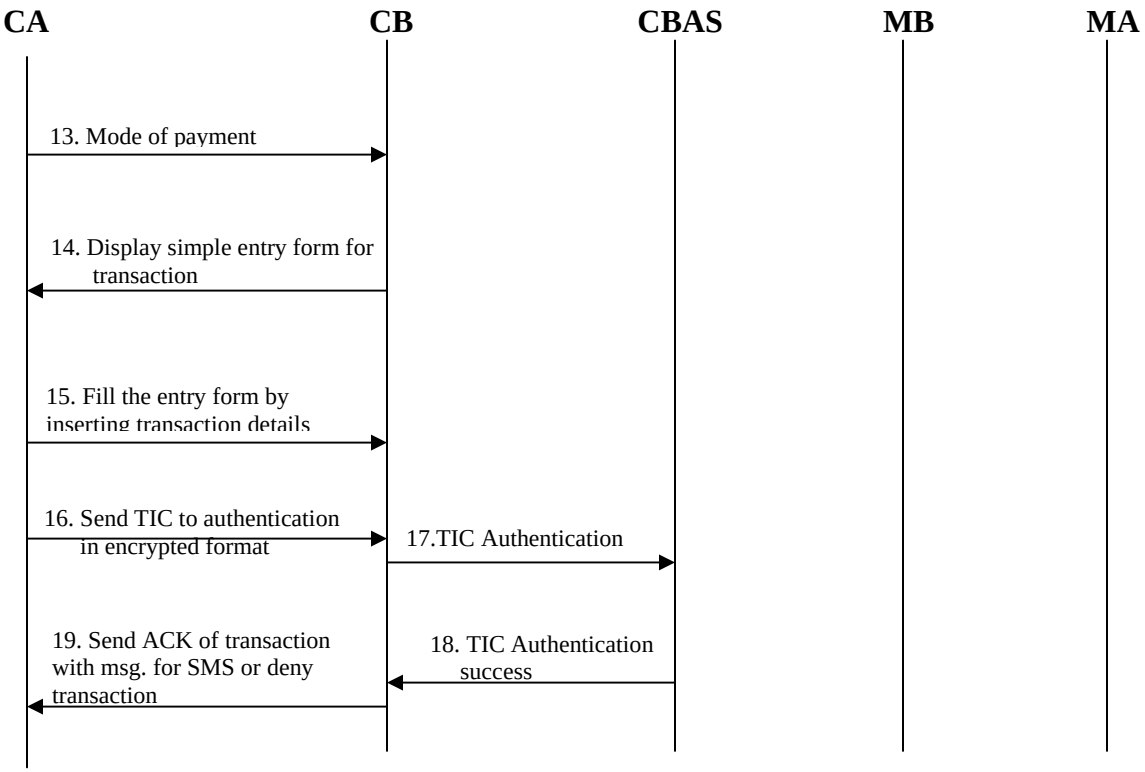


Figure 6: Second Authentication of User to the Bank

13. The user (CA) will select the mode of payment to make payment. Here we have considered two basic modes of payments:

    1. Credit Card based Payment System
    2. Account based Electronic Transfer

14. Selection of the mode of payment generates 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 on the client side environment and submit transaction to the server in an encrypted format. 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 screen. This selection will also remove the selected TIC from the list of TICs at client environment.
    - Local password of TICs may be the key for decryption of TIC and known to the user only or stored secret logic may be the key for decryption of TIC. Even the bank authentication server is unaware of this key. It can be changed at any moment according to convenience of the user.
    - Transmission of TIC from CA to CB is strictly in an encrypted format (refer to chapter 6).

17. The bank server will forward the received TIC to the CBAS for TIC authentication and CBAS decrypts the received encrypted TIC to match it 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 deletes the used TIC from its database and send a 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 an SMS. If TIC does not match with the user's 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 that the authentication server will generate a SMS destined to the user. As discussed in part IV.

5.4 Part IV: Third Authentication of User by SMS confirmation of Web Transaction to the Bank Authentication Server

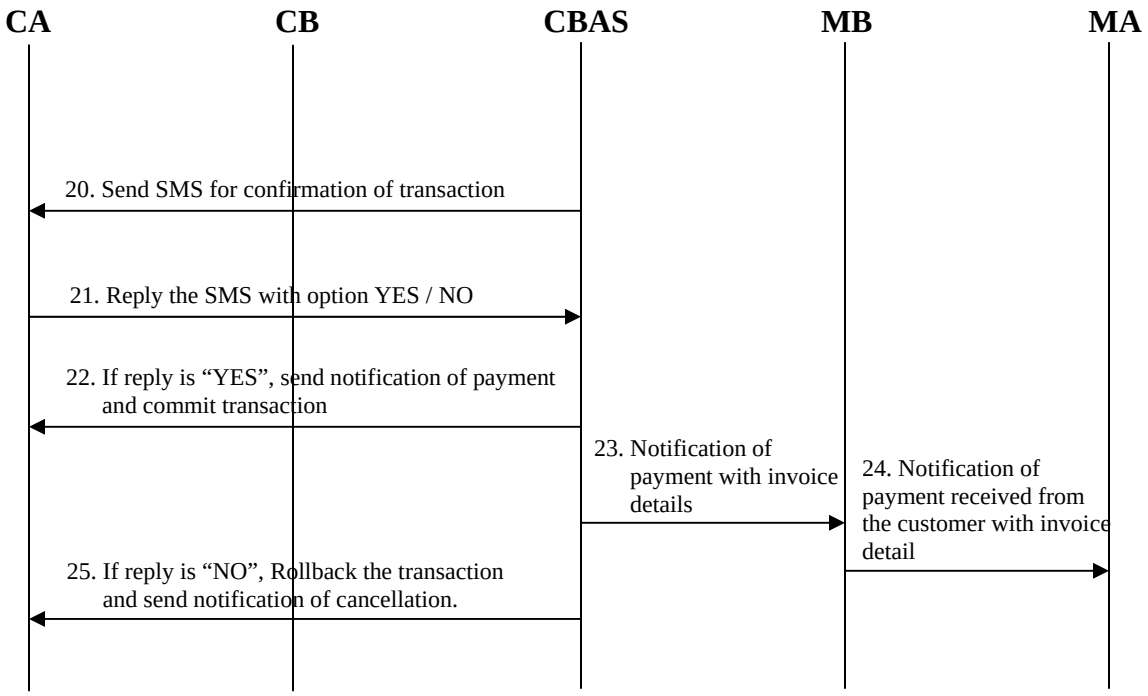


Figure 7: Third Authentication of User to the Bank

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

21. The user will reply 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 user’s SMS confirmation, it generates notification of a payment to the user and commits user’s transaction.

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

24. The MB is responsible for sending notification of a payment received from the customer to the merchant. The 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.

5.5 Summary

- This chapter describes the detailed transaction flow of the proposed system.

- The system starts when the user has decided to make payment to the merchant and terminates when merchant will receive a confirmation of payment reception from the Merchant bank.

- To demonstrate the basic working of the system we first run Two Way Authentication to authenticate the merchant based on the merchant authentication certificate.

- After merchant authentication, user authentication takes place by the Secure web Authentication Protocol.

- The user authentication includes TIC identification and validation followed by a SMS confirmation.

- The complete transaction flow from client to server is strictly in an encrypted manner to maintain system security and protect confidential data of user.

Chapter 6
Cryptography and Key and session management

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography, which is the focus of this chapter since it plays a crucial role in our protocol.

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 [21]. As mentioned in [21] public-key encryption needs more computation and processing time in comparison of symmetric-key encryption. Therefore, public-key encryption is not always suitable for large amount of data communication. However, public-key encryption is used to exchange a symmetric key, which can be later used for further encrypt of data [13, 21].

6.1 The Encryption Algorithm

The encryption algorithm that we used is the AES Rijndael algorithm [22]. AES Rijndael algorithms supports iterated block cipher, meaning that multiple transformations take place on entered input block before producing output. 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 wider. AES Rijndael algorithm has the following characteristics:

- Resistance: System resistance in various attacks.
- Compactness: Compactness of code and speed on various types of platforms.
- Simplicity: Very simple in design

The main feature of algorithm is block length and/or key length size can easily be expanded in multiples of 32 bits, and the system can be implemented in various types of hardware or software platforms and also functions well on range of processors. We have considered a simple example given in [35] which shows the AES key expansion technique. Example shows that algorithm takes input of 4 words (16 byte) key and generates output of 44 words (156 bytes) linear array. This size is adequate to provide a 4-word round key which is used in the initial Add Round Key stage and in each rounds of the cipher up to the 10 rounds. The pseudo codes for expansion are as follows:

```
KeyExpansion (byte key[16], word w[4] )
{
 word temp;
for (i=0; i<4; i++)   a[i] = (key[4*i], key[4*i+1], key[4*i+2], key[4*i+3]);
for(i=4; i<44; i++)
{
temp=w[i-1];
if ( i mod 4 = = 0) temp = SubWord ( RotWord (temp)) XOR Rcon[i/4];
  w[i] = w[i-4] XOR temp;
}
}
```

Initial four words of the expanded key are the replica of key. The remaining part of the expanded key is populated with four words at a time. Each new words, w[i], depends on the w[i-1] which is the just previous word of w[i] and the word four positions back, w[i-4]. A simple XOR is used in three cases out of four. A more complex function is used for words whose position is a multiple of 4 in w array. Figure 8 shows the creation of first eight words of the expanded key, here symbol g is used to represent a complex function.

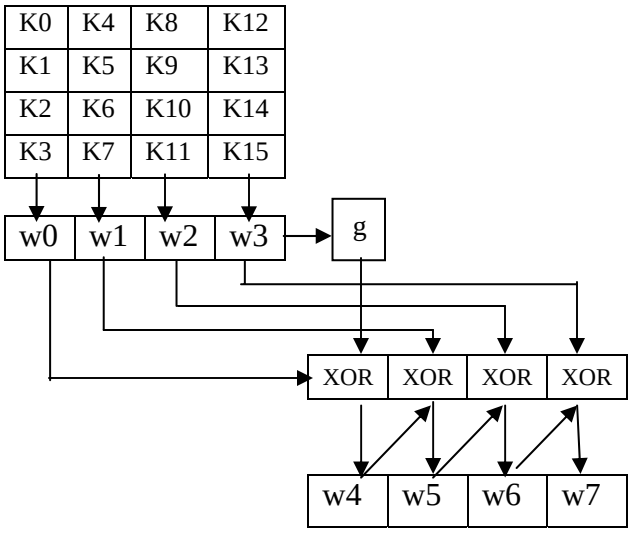


Figure 8: AES Key Expansion

The following are the sub-functions of function g:

1. One byte circular left shift on a word is done by RotWord. By this operation an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].

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

3. The output of the above two steps (i.e.,step 1 and 2) is XORed with a round constant Rcon[j].

Three rightmost bytes are always 0 in the round constant word. Thus, the XOR effect of a word with Rcon will affect only on the left most byte of the word. The values of round constant are different for each round as given below:

Rcon[j] = (RC[j], 0, 0, 0) with RC[1]=1 and RC[j]= 2* RC[j-1]

and with multiplication function on the field GF(2^8). The RC[j] in hexadecimal are:

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

Here we are assuming that the round key for the round 8 is:

EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F

Then the calculations of first four bytes (first column) of the round key for 9th round are:

i (decimal)	temp	After RotWord	After SubWord	Rcon (9)	After XOR with Rcon	w [i – 4]	w[i]= temp XOR w [i – 4]
36	7F8D292F	8D292F7F	5DA515D2	1B000000	46A515D2	EAD27321	AC7766F3

As mentioned in [35] AES Rijndael is a substitution-linear transformation network with 10, 12 or 14 rounds, based on the size of key. Because an encryption operation is byte oriented in AES encryption so data block to be encrypted is divided into an array of bytes. There are four layers for round function of AES. In first layer each byte is processed by an 8x8 S-box. The second and third layers are linear integration, which shifts the rows of the array and the mixed the columns. In the fourth layer, XOR operation is used on subkey bytes with each byte of the array. Here mixing of column is not involve in last round [12]. For the purpose of the present work the AES Rijandael algorithm can be implemented from the Legion of the Bouncy Castle cryptographic package [24] or Security and Trust Services API (SATSA) for J2ME [30] which is an open source Java implementation for the algorithms. We have considered Security and Trust Services API (SATSA) for J2ME to implement AES encryption.

In this project we have implemented an encryption scheme over a wireless medium. To get security we have used a block size of 16 bytes with 128-bit key encryption: this combination is suitable to implement operations on J2ME devices due to the limited resources like speed and memory [12].

6.2 Cipher Key Management

Secure communication between client and server is our prime objective. For this reason we have implemented a concept of secret session-key, session key is randomly generated for every client session and later used for encryption/decryption of data. 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 individually for each user. The server use 128 bit shared secret logic to encrypt this secret key, which is a shared secret and known to both ends i.e., client and server. This encrypted secret key is transmitted to the client. The client decrypts this secret key and uses it in the later stages of the transaction to encrypt the required account details of the customer with TIC code before transmission to the server. On server side same secret key is stored which decrypts the transaction details and TIC code, then matches the TIC code with the issued TICs to the customer. If this TIC matches with the database then it will next process the transaction otherwise transaction would be denied.

The protection of shared secret logic on the client and server is an important issue. 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. On client device, shared secret is stored in small mobile device memory, securing this storage is bit challenging. We suggest the following mechanism to protect the shared secret on the client:

As shown in Figure 9, the shared secret is stored after encryption and key is the confidential 128 bits pin code [12].

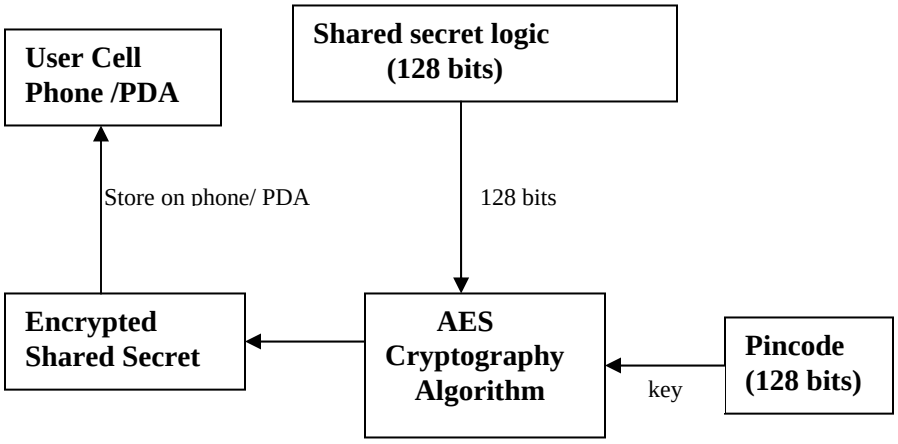


Figure 9: Storing of Shared Logic on client

As mentioned in [12] the user first subscribe for the mobile banking, bank authority makes necessary installation of the banking module on the cell phone and store shared secret on mobile phone/PDA after encryption with the secret 128 bit pin code number of client. If user's phone is lost or stolen, thief can not use this shared secret logic because shared secret is stored in encrypted format and system decrypts it when user logon to the bank portal with valid client authentication. This client pin code is a key for shared secret decryption, which later used in data/key encryption/decryption process.

Furthermore, we can make client more secure by obfuscated Java classes and JAR file. It protects the byte code from byte code decompiler. The details on Retroguard obfuscator v1.1 are mentioned in [12, 25].

In the proposed protocol TIC codes are the 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 Figure 10. The user will insert the local password of TICs to open the encrypted list of TICs and can

select any TIC from the list to initiate financial transaction. This selection of TIC automatically decrypts the selected TIC and displays it on the user screen. This selection will also remove the selected TIC from the list of TICs at client environment. Local password of TICs may be the key for decryption of TIC or it just a secret password to protect TICs and TICs would be decrypted by internally stored confidential secret logic known to the user only. Even the server is unaware of it. It can be changed at any moment according to the user convenience. 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 [12].

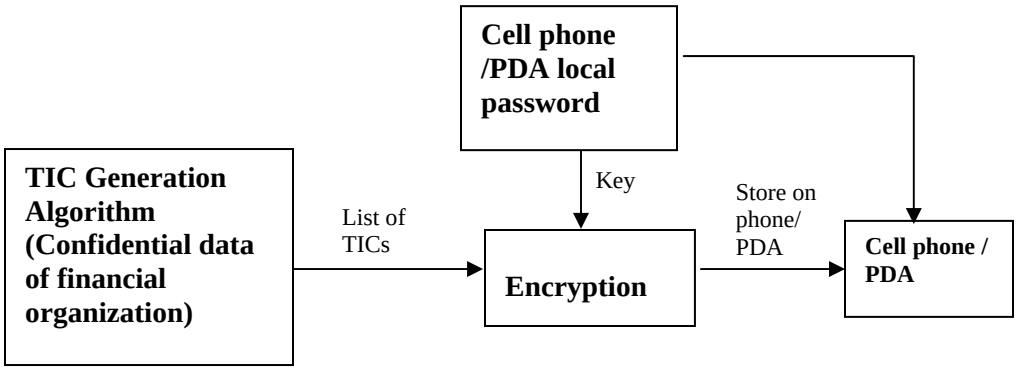


Figure 10 : TIC protection at Client Environment

6.3 Session Management

Referred to [12] HTTP is a stateless protocol. Each HTTP request is treated as a new request and the protocol specification does not supports a facility to bound the group of request belongs to the same user session. Over time, various strategies have considered for session tracking; the most practically adopted one is the use of cookies and URL rewriting. HttpSession object is an object for session management in Java Servlet API provides the HttpSession object, which represents each user's interaction with the web server. By cookies mechanism web containers can easily maintain track on user session. The cookie interchange mechanism is taking place between a client device and a web server.

We have used cookies to keep track on user sessions. As referred to [12] in our proposed protocol, the client MIDlet sends cookies back to the server with each http request explicitly. When user logon on the web server, server uses HttpSession object to generate a new session and sends the JSESSIONID cookie by setting values of "SET-COOKIE" field in response header. The MIDlet client invoke getHeaderField method on the HttpConnection object to retrieve the session id value from header and send it back with every subsequent http request to group the client requests which belongs to same user session.

We have used J2ME to implement the client environment and J2ME does not supports temporary text files to store the cookies. So, we have used the RMS system of MIDlet to maintain local database of the client and to store all details of the user session.

The MIDP provides a facility for MIDlets to store data locally in persistent storage and use it later. This simple record-based database is called the Record Management System (RMS) [39].

6.4 Summary

- The Cryptography and cipher key management are an important issue in security of the system. Cryptography is necessary when communicating over any mistrusted medium, which includes the Internet based wide network.

- Public Key encryption needs more computations and is therefore not always appropriate for large amount of data and cell phones have very limited power and processing capabilities. So it may degrade the performance of the system.

- AES algorithm is based on the symmetric key encryption/decryption and best suited for the devices with limited power and processing capabilities.

- AES is an iterated block cipher. So the algorithm can operate on variable length blocks and variable keys. It has resistance against all known attacks.

- Shared secret is used to make secure client-server communication. This secret is known to both ends. So there is no need to transmit it over the un-trusted channel.

- TICs are most sensitive data and stored after encryption. TICs will be decrypted only at the time of selection. All encrypted TICs are stored under password protection.

- Session tracking is very important to maintain multiple user sessions. Java Servlet's HttpSession objects are used at server and cookies are used at client to keep track on the user sessions.

Chapter 7

System Analysis with various internet threats

The proposed protocol is capable of handling various internet threats like phishing, loss of cell phone etc. In this chapter we present a detailed analysis of the resistance of our system under various internet 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 capture the sensitive information of users such as passwords and credit card details to gain unauthorized access to the user's confidentail financial data and perform illegal transfer of funds. Phishing is generally carried out using email or an instant message or via phone contact.

The report in [26] shows that identity theft is becoming more popular, because of the users come in the contact of the fake wesites and submit their personal information to phishers. Phisher fraudently get the user confidential information and gain the illeagal access to user personal data. After getting acess to user's personal information, the phisher can misuse this data by making illegal transfer of fund, or block the user's account and prevent them to access their own accounts.

The proposed protocol is secure against phishing attacks. A multifactor secure protocol for user authentication has the capability to secure the user data and maintain integrity, confidentiality and access control from malware access. To understand the origin of the security we consider various cases below.

Case I: If phisher fraudulently acquires user id and secret password

This is the general scenerio of phishing attacks, 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 user's account and private data. The attacker would not be able to perform any illegeal action, because of:

1. Figure 4 shows the First authentication of the user. As mentioned in step 5 in Figure 4, the user has to produce login id and secret password to log on to the bank server. If phisher fraudulently acquires the user's account password then he successfully achieves the authentication of step 5 and subsequently step 6, step 7 and step 8 of Figure 4. Still the phisher can not access the sensitive information of user account because the TIC verification at authentication server would deny the falsely ongoing transaction.

2. In reference to Figure 6 of chapter 5 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 in Figure 6. At step 17 the authentication server would deny the falsely going transaction if it does not find the valid TIC code from the user.

3. TIC codes are secret codes issued to valid account holders and TICs are not publicly accessible [18]. It is a one time code for each online transaction and it is randomly generated in nature so a phisher can not guess the next TIC code of user account.

Case II: Transmission of TICs over insecure channel

As step 16 in Figure 6 shows, the TIC code transmission from the user's cell phone / PDA to the web authentication server is in strongly encrypted format so phishing attackers can not decrypt it easily to access user's private information on server side. Encryption technique is dicussed in more detail in chapter 6. Moreover, one TIC is used only once and then discarded.

Case III: If phisher fraudulently acquires user's secrete password and also one TIC code by some phishing attack

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 secure in this extreme case also, as shown below:

1. There is another major security factor of the presented protocol to deal with this extremly vulnerable condition. The system is secure in this condition also by multifactor authentication technique as mentioned in step 20 of Figure 7.

2. In chapter 5 Figure 7 shows Third authentication of user to the Bank by SMS confirmation. An SMS confirmation is the next factor which saves the user information from malicious access of unauthorized user in this extreme situation. At step 21 in Figure 7 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 informations from attackers.

3. The TIC codes are psuedo 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 confidentential at web authentication server and we have assumed that banks and financial institutions are responsible

for time to time updation of TIC generation data and upgradation of TIC generation algorithms.

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

7.2 Virus Attack on Cell Phones and PDAs

Mobile wireless devices can also suffer from various virus attacks. Mobile device viruses like “Cabir” and “CommWarrior.A,” can copy data from cell phones without knowledge of user and transfer them from mobile phones and BlackBerrys through mobile messaging services or Bluetooth connections [26, 27, 28].

The proposed system is secure even if any mobile device virus attacks on the user’s cell phone. No virus can disturb the user’s data or cause any harm to user’s confidential data stored on cell phone /PDA. The system is secure from the virus attacks by the following points:

1. The users always carry their cell phone with them so an SMS confirmation will not be present in case of malicious transaction raised by any unauthorized user, who has gained access to the user’s confidential data from virus attacks as shown in Figure 7.

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 any virus attacks would not be able to disturb the user’s data.

3. It is always recommended that to avoid downloading a mobile device virus through a Bluetooth connection, user check the access permissions on their Bluetooth settings before making connection and close active Bluetooth connection if

users are not using it. The users can install anti-virus software on several mobile platforms to protect themselves from viruses [28].

7.3 User Session Hijacking

In this attack user's activities on internet are monitored using malicious software ("malware") and user is unaware of it. Malware software monitors all user actions over internet from user's local computer, or remotely after get control on user session known as Session hijacking [26, 27]. To overcome this threat our secure protocol provides security at the following steps:

1. In Figure 4 after successful completion of step 5 and 6 authentication server creates session id as mentioned in step 7 and 8 in Figure 4. 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, which are one time code for each transaction, are canceled by the web authentication server from the database after each transaction. So if a man in the middle attacks on the user session to monitor user activities then he/she will get a TIC that has already been canceled.

3. The TIC codes are pseudo randomly generated by confidential algorithm; it is a complicated code which can not be easily predicted by any person.

4. Sensitive and confidential transaction information would be encrypted before transmission over the channel.

5. As mentioned at step 16 in Figure 6, 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 & 8 in Figure 4.

6. 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.

7. Another factor of security is a SMS confirmation as mentioned in Figure 7. An SMS is not routed through the same channel which has been used in online web transaction. An SMS uses control channels over cellular networks. The messages are encrypted with A5/3 Algorithm which also makes system secure [23].

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 should suspend their wireless service connection immediatly to protect themselves against charges and illegal access. However, it is entirely possible that an unauthorized person may try to initiate a transaction with the lost/stolen cell phone before it has been de-activated. The proposed 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 should deactivate their wireless service and make necessary action to report lost. Once deactivated, the user would not be able to receive SMS generated for their number.

2. Another important issue of security is that if some person has stolen user's cell phone/PDA then that thief does not know the local password of stored TICs of user's cell phone/PDA. If the user's 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 user's 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 list of 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 Case I: 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 the popular protocol for online payment. Our proposed work also shows that this protocol can be extended for the wireless networks and mobile devices. So to answer the above point we are using SET strategy which is also applicable to this proposed system.

The bank confirms the successful completion of the transaction by sending a reference/transaction number to the merchant for audit purposes. At the end of the day, it also sends each merchant a database of the transactions which had carried out in merchant's favor during the day [7, 28]. The merchant would verify a received payment from the customers everyday and dispatch the purchased goods after transfer of full payment from the customer which includes taxes and shipping costs.

7.6 Case II: If Customer has transferred the payment and customer did not receive the purchased goods

Another important issue is after transferring the payment if customer did not receive the purchased goods. To avoid this possible case we have used the two way authentication protocol as mentioned in Figure 5, 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.

7.7 Case III: 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 easily break the security password because it is restricted by J2ME security model. To increase the system security, the class loader in CLDC has a built-in "bootstrap" class loader that cannot be replaced or reconfigured [14].

When need of persistence data storage in a MIDlet to store information, we can use RMS to store records. MIDlet supports facility to create shared persistent storage so data can be shared between all installed Midlets on the device, the TICs are stored in an encrypted format with the secret key known to the user which is the password for decrypting TICs. A secret shared logic is also stored after encryption as mentioned in chapter 6. This secret logic is encryption with a client pin code which is protected by the MIDlet security features. The persistence storage in J2ME CLDC is the record store which is secure storage. Each MIDlet suite can maintain more than one record store. A MIDlet is restricted to one protection domain that allows the AMS (Application Management Software) to authenticate the origin of a MIDlet. If MIDlet is authenticated then it is

called as trusted, if not, it is called un-trusted. So, sensitive APIs can only be accessible via valid user permission in un-trusted applications [14, 40].

7.8 Case IV: 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 an 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. An 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 period, then the Bank authentication server will resend an 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.

7.9 Summary

- This chapter provides an analysis of the presented system over various internet threats. The system is secure from the various types of attacks like – Phishing, Virus attacks, User Session hijacking.

- TICs and SMS confirmations are the weapons of the system which makes the system secure under various vulnerable conditions.

- The system is also secure in extremely vulnerable conditions, which has shown by studying various cases of attacks.

- All the communication between the client and server are strictly in an encrypted form, so no man in the middle can easily decrypt the transaction data.

- The proposed system is also secure in cell phone/PDA theft situation, we have also recommended to the users to take necessary steps of deactivation immediately if they have lost their cell phone.

- Multifactor Secure Protocol for Wireless Payment is very efficient system to protect the user data from malicious access and to maintain user data integrity, confidentiality and access control.

Chapter 8
Technologies

In this chapter we discuss the implementation issues. In particular, we discuss the specific technologies that were used in implementing the entire system. Since the client side programming was done using the J2ME, so we discuss it first. The Sun Wireless Development Toolkit provides a framework for developing wireless applications. The features of this toolkit are discussed next. Since security is an important aspect of the present work, so we discuss the security features of JDK 1.2 next. Other technologies used in the present work are also discussed briefly e.g. Java Servlets, Apache Tomcat server, JDBC for connectivity to the databases and Oracle database.

8.1 J2ME

Java 2 Micro Edition (J2ME) is the latest edition in the Java 2 family, java 2 Micro Edition (J2ME) is used to program various java based small the devices for consumer such as mobile phones, PDAs, TV set-top boxes and a wide range of embedded devices. Java Community Process (JCP) has defined standard Java APIs for J2ME just similar to other java versions like enterprise (J2EE), desktop (J2SE) and smart card (Java Card). The J2ME is used to implement the client side functionality of the proposed system [39].

The J2ME is used to program small consumer handheld devices and embedded systems. Now many manufacturers are adopting J2ME in implementation of larger number of wireless mobile devices. The reference [15] analyses the main security features of J2ME and its appropriateness for the wireless mobile devices.

8.1.1 Why J2ME is preferred?

Choosing J2ME as our development platform was due to the following reasons:

- The java codes are portable in nature, so on client device we can process data locally by utilizing the client power and reduce the network traffic load.

- It has ability to implement differential security policy on the client by which we can encrypt the most sensitive data before transmission on network instead of encrypting everything, this method saves the power of small device and we can utilize battery power more efficiently.

- It bridges the security gap of the security protocol conversion, between the WAP gateway and the secure sockets layer (SSL) [12].

8.2 Sun Wireless Development tool kit 2.3

The J2ME Wireless Toolkit is preferred to implement the client side functionality and server side management of the Messaging services. The J2ME Wireless Toolkit is a set of tools for implementing Java applications that run on java enabled devices for the Wireless environment (JTWI, JSR 185) specification. It consists of various tools for building applications, utilities and a phone based device emulator [30, 38].

The J2ME Wireless Toolkit has various APIs to implement different services for wireless application. The APIs are defined through the Java Community Process (JCP) in [30] are:

- Connected Limited Device Configuration (CLDC) 1.1 (JSR 139)

- Mobile Information Device Profile (MIDP) 2.0 (JSR 118)

- Java Technology for the Wireless Industry (JTWI) 1.0 (JSR 185)
- Wireless Messaging API (WMA) 2.0 (JSR 205)
- Mobile Media API (MMAPI) 1.1 (JSR 135)
- PDA Optional Packages for the J2ME Platform (JSR 75)
- Java APIs for Bluetooth (JSR 82)
- J2ME Web Services Specification (JSR 172)
- Mobile 3D Graphics API for J2ME (JSR 184)
- Security and Trust Services API (JSR 177)
- Location API (JSR 179)
- Content Handler API (JSR 211)

8.2.1 Toolkit Features :

The J2ME Wireless Toolkit supports the creation of MIDP applications with the following main features taken from [30]:

- **Building and packaging**: User is responsible for writing a source code and the wireless toolkit performs the rest of the action to run them, like compilation process of surce code, preverification of the class files and packages in a MIDlet suite.

- **Running and monitoring**: The installation process of MIDlet suit supports installation of application on a real device and running of a MIDlet suite directly on the emulator. It can also monitor the operation of the MIDlets by a memory monitor, network monitor and method profiler analyzer.

- **MIDlet suite signing**: The wireless toolkit also supports tools for cryptographically signing of MIDlet suites. This feature is useful for security and it also used to tests the MIDlets in different protection domains.

8.3 JDK 1.2 Security Features

The JDK 1.2 security architecture includes a verification of application and control management based on location. In the earlier version of JDK (JDK 1.1), the applications were classified as trusted or not trusted. The JDK 1.2 security architecture is more sophisticated in security management. In JDK 1.2 each Java class is bound in access rights to use resources of computer system based on its location from where the Java class is fetched and signer of the Java class. The security policy is defined for access rights. The security policy can be able to define its individual set of access rights to each signer and location combination. The security policy can be defined for example in a database, in a file, or other information resource [39].

8.4 Java Servlets

Java Servlets are used to implement the server side functionality. Java Servlets are the Java platform technology for extending and increase the functionality of Web servers. Servlets can implement plateform independent web server based applications based on various components. As mentioned in [29] this makes developer open to select a "best of breed" approach for servers, platforms and tools.

The users are free to use all java family APIs in servlets, including the JDBC API to connect java application with database. On servlets user can also make HTTP-specific calls and get the advantages of all features of java language, including portability of code, reusability, performance and crash protection.

Today servlets are frequently used in building of interactive Web applications. Servlet containers are available for Apache Web Server, Microsoft IIS and others. Servlet containers are a part of Web and application servers, such as BEA WebLogic Application Server, IBM WebSphere, Sun Java System Web Server, Sun Java System Application Server and others [29].

8.5 Web Server (Apache-tomcat-5.5.17)

Apache Tomcat is a web server which contains a servlet container to run Java Servlet and JavaServer Pages technologies. Java Community Process has developed Java Servlet and JavaServer Pages technologies specifications. We have used Apache Tomcat web server to handle the client requests and to execute the java servlets to respond the client requests.

Apache Tomcat version 5.5 supports the Servlet 2.4 specifications which includes many features which are useful in launching and deploying the web applications and web services [31].

8.6 JDBC (Java Database Connectivity)

The JDBC driver is used at server side to establish a communication between java servlets and database. The JDBC API provides facility to connect java program to relational database to access data. In the JDBC API, user can execute SQL statement in java programs, retrieve the fetched results and make changes in data source to update database. The JDBC API can operate in distributed or heterogeneous environment by connecting multiple data source.

The object of JDBC DriverManager class is used to make connection between Java applications and a JDBC driver. The DriverManager is very small in size and simple to operate, it plays a very important role in the JDBC architecture.

The JDBC API is used as a middle tier in multi-tier architecture and it is frequently used in development of enterprises application using the Java programming language. Distributed transactions, disconnected row sets and connection pooling are some of the features which make JDBC server technology more flexible [32].

8.7 ORACLE 9i with JServer

Relational Database Management System:

A database is an electronic system to store information or operational data. The user can store information, update and delete information and retrieved it for processing. In other words, a relational database is a tabular representation of information with rows and columns. A table is a collection of records which belongs to the same entity set also known as relation in RDBMS. Data stored in tables can be related to each other according to the defined keys or based on referential integrity constraints to make relation.

Oracle 9i is used at server to store data of the customers and transactions. Oracle 9i allows data to be stored and executed from within the database. Oracle 9*i* improves the following technical aspects:

Database performance, ease of management, scalability, security, availability and application areas: Internet content management, e-commerce integration, packaged applications, Business Intelligence [33].

8.8 Summary

- The system implementation requires exploring various technologies used to implement the client and server environment.

- The J2ME is the preferred client environment to program the small mobile devices. It is platform independent Java based technology.

- Sun Wireless Tool Kit is a J2ME tool kit with a set of various APIs to implement the impressive applications for hand held devices.

- We have preferred J2ME over the WAP because of the lack of security in bridging the gap of WAP gateway and SSL also to implement end-to-end security system.

- Java Servlets are popular choice for implementing the server side web applications, which runs on the Apache Tomcat Web Server.

- JDBC Driver provides a middle tier for establishing the communication between the Java based tool with the backend Database system.

- RDBMS is a collection of database tables which are interlinked by enforcement of integrity constraints. Oracle 9i makes easy procedure to stored data and executed from within the database. It maintains the scalability, security and availability of data.

Chapter 9

System Implementation & Simulation

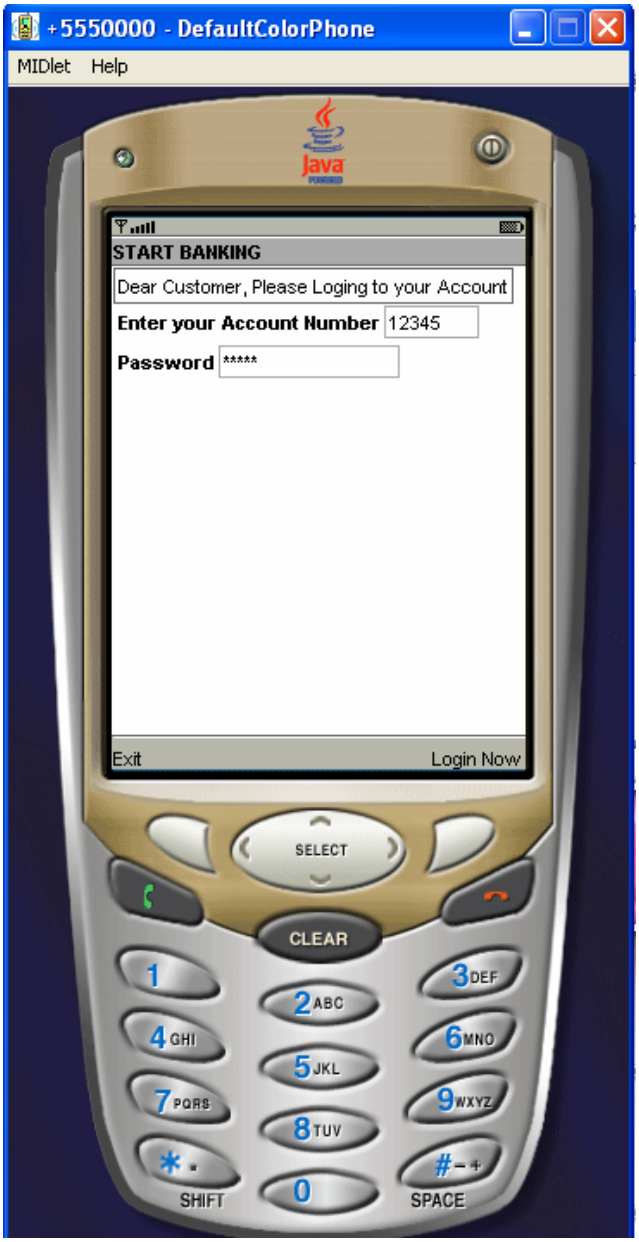
The simulation consists of the following functionality:

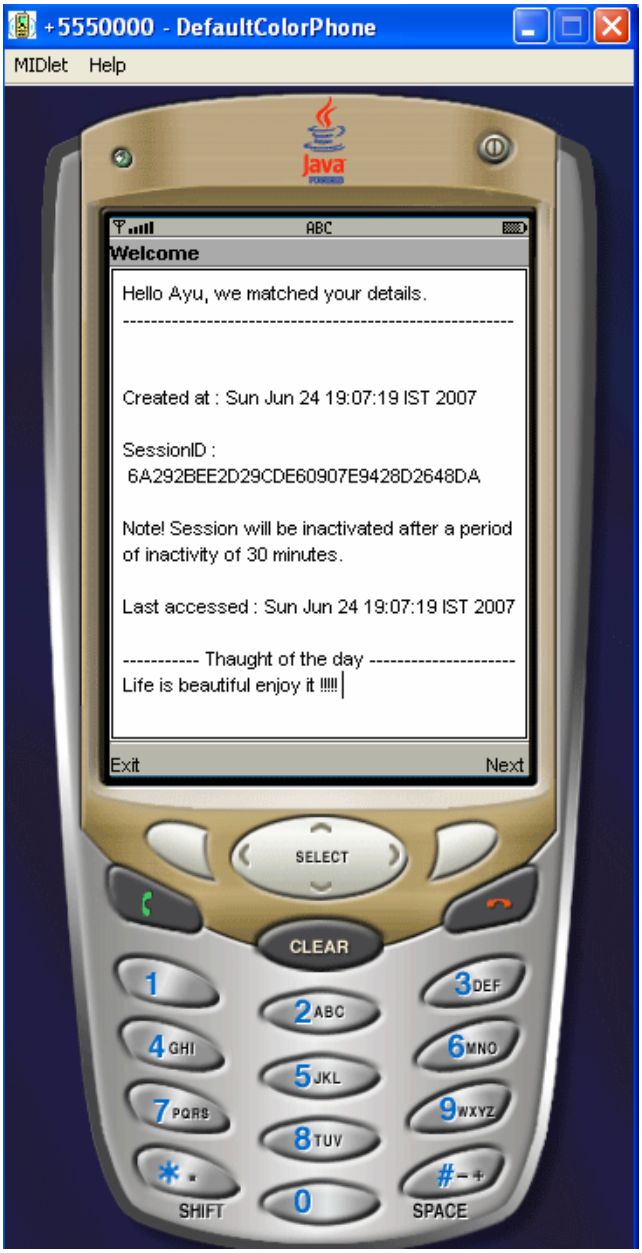
1. First Authentication of the user to the Bank or Financial Institution authentication Server based on user login/password.
2. Selection of the operation :
   - ❖ Account Balance Enquiry
   - ❖ Money Transfer Mode
     - Electronic Transfer
     - Credit Card Transfer
   - ❖ Merchant Payment
   - ❖ Change Account Password
   - ❖ Generate TIC
3. Second Authentication of the user to the Bank or Financial Institution authentication server based on TIC verification. The second authentication of the user will occur if user chooses any type of payment option (i.e., account based Electronic Transfer, Credit Card based Transfer or Merchant Payment).
4. Third Authentication of the user to the Bank or Financial Institution authentication server by SMS confirmation. The third authentication of the user will occur only if user chooses any type of payment option and successfully cleared the second authentication step and submitted financial transaction to the web server.

The essential components of simulation process are the Database Schema as a back end (Appendix – A), Server Side Java Servlets (Appendix – B) and various Commands and Parameters setting for Toolkit and System Environments variables (Appendix – C).

The simulation screenshots of the system implementation are on next pages.

9.1 First Authentication of user to the Bank or Financial Institution authentication Server





LOGIN AUTHENTICATION **LOGIN SUCCESS**

Java Servlet LoginServlet is responsible for first user authentication on server, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

9.2 Account Balance Enquiry

SELECTION BALANCE ENQUIRY OPTION

BALANCE ENQUIRY

Java Servlet BalanceEnqServlet performs Balance Enquiry and transmits results on user screen, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

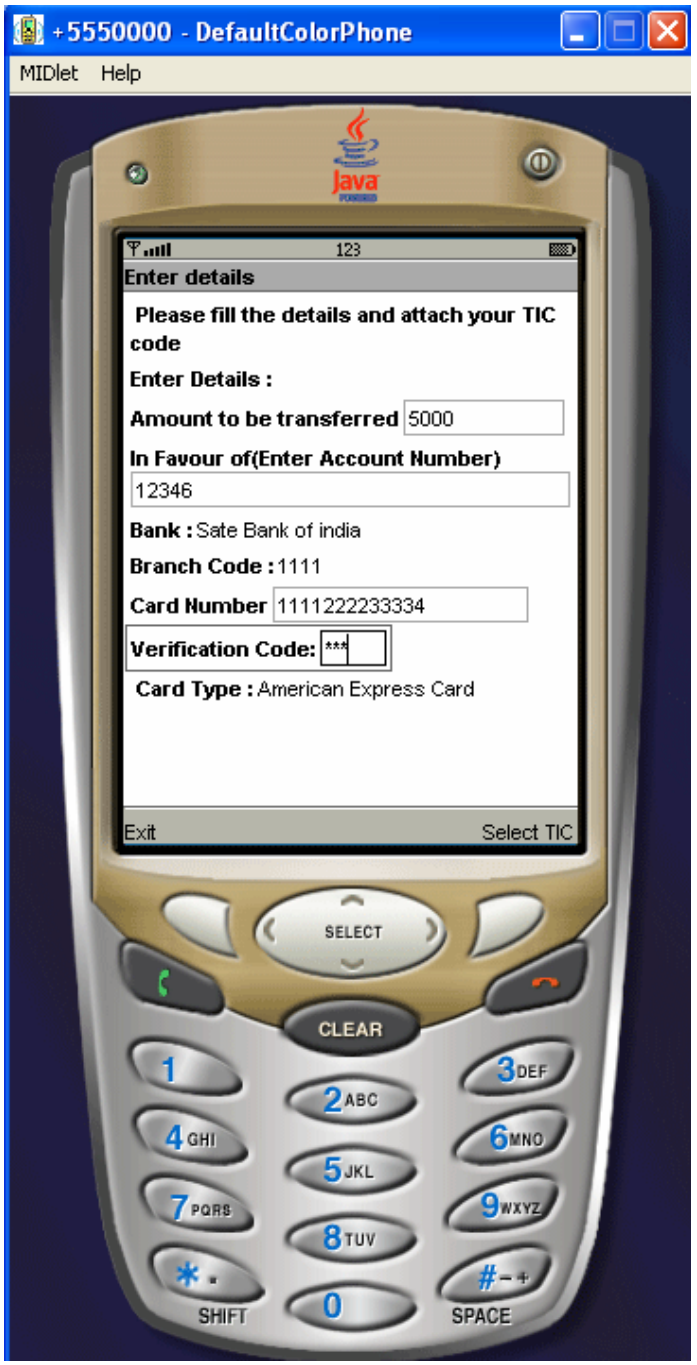
9.3 Credit Card Transfer

SELECTION OF CREDIT CARD TRANSFER

SELECTION OF THE BANK NAME AND BRANCH CODE

Java Servlet BankServlet retrieve the list of bank names and branch code and display them on user's screen, for detail description on database schema and server side java servlets please refer Appendix – A & Appendix – B.

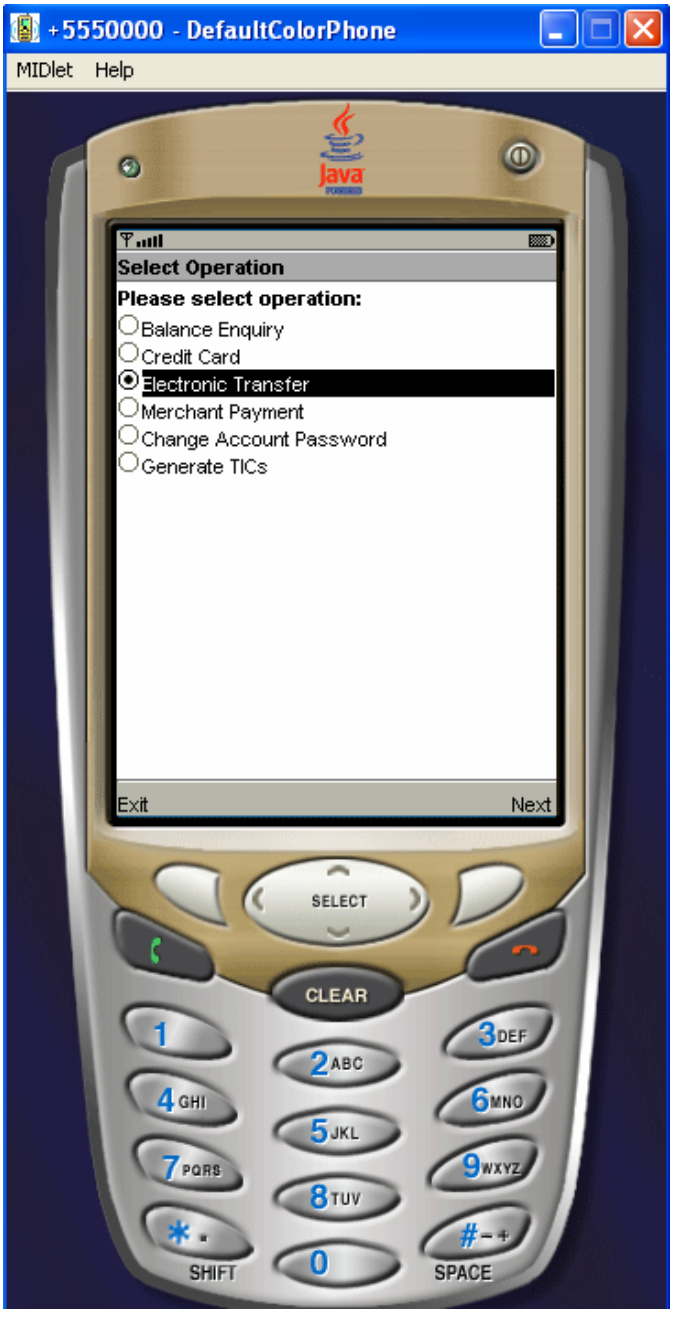
SELECTION OF CREDIT CARD TYPE



FILL SIMPLE ENTRY FORM FOR TRANSACTION

The Next step is the selection of the TIC as a second authentication of the user mentioned in section 9.3.

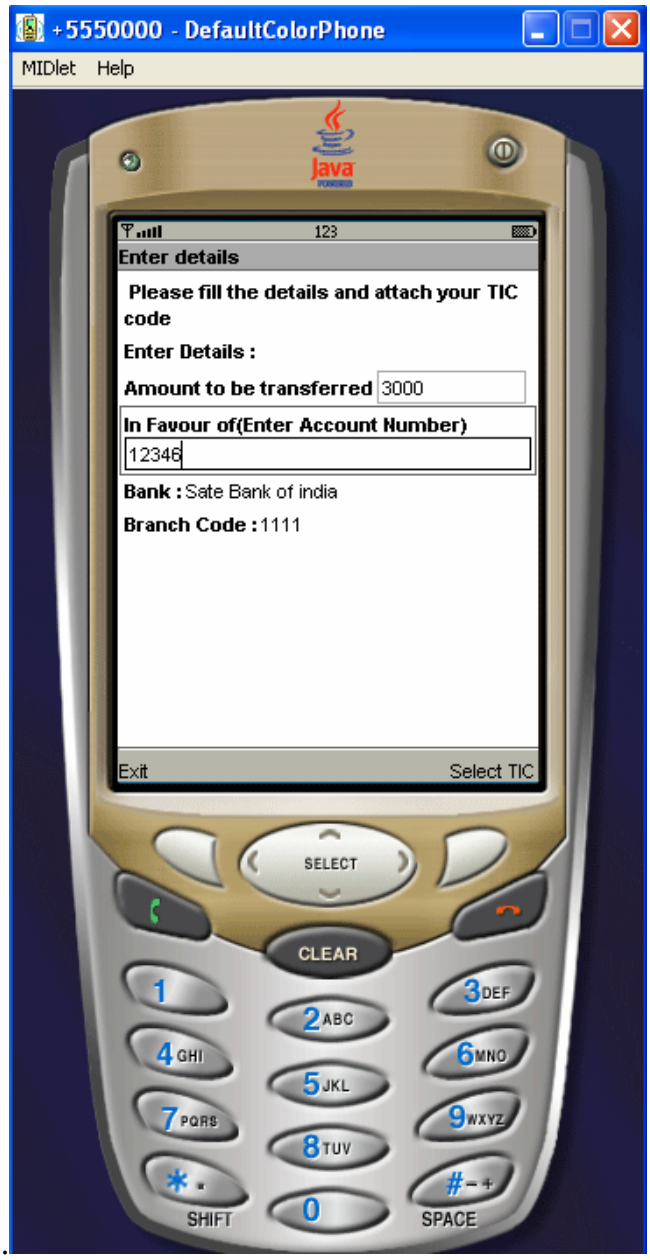
9.4 Account Based Electronic Transfer



SELECTION OF ELECTRONIC TRANSFER

SELECTION OF THE BANK NAME AND BRANCH CODE.

Java Servlet BankServlet retrieve the list of bank names and branch code and display them on user's screen, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.



FILL SIMPLE ENTRY FORM FOR TRANSACTION

TIC PASSWORD TO OPEN TIC LIST

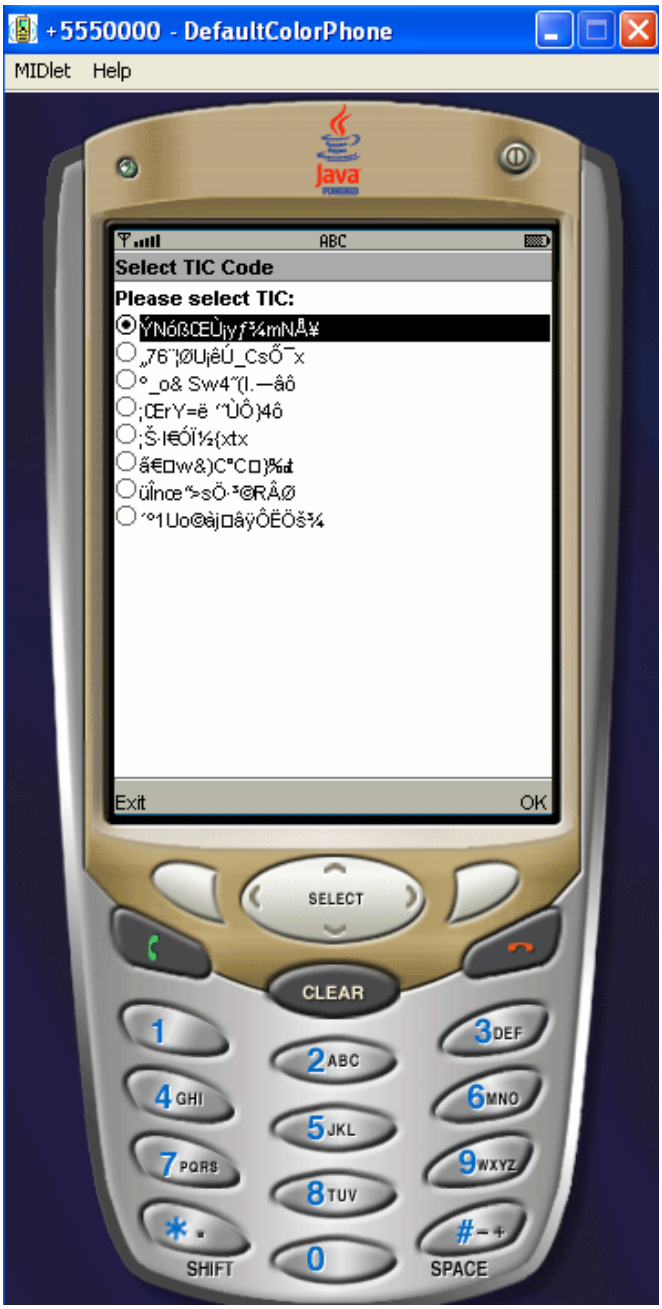
Java Servlet ETransferServlet is responsible for Electronic Transfer of fund, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

The Next step is the selection of the TIC as a second authentication of the user mentioned in section 9.3.

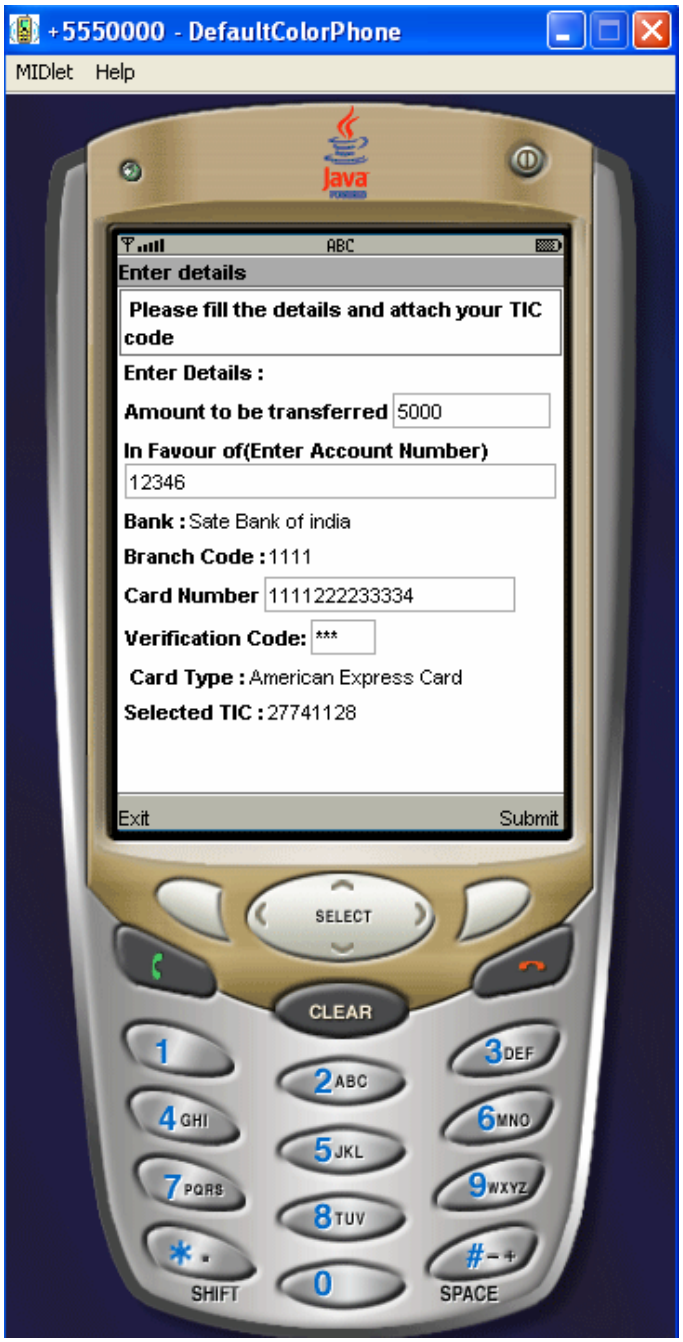
9.5 Second Authentication of user to the Bank or Financial Institution authentication Server

The Second Authentication of the user is based on TIC authentication.

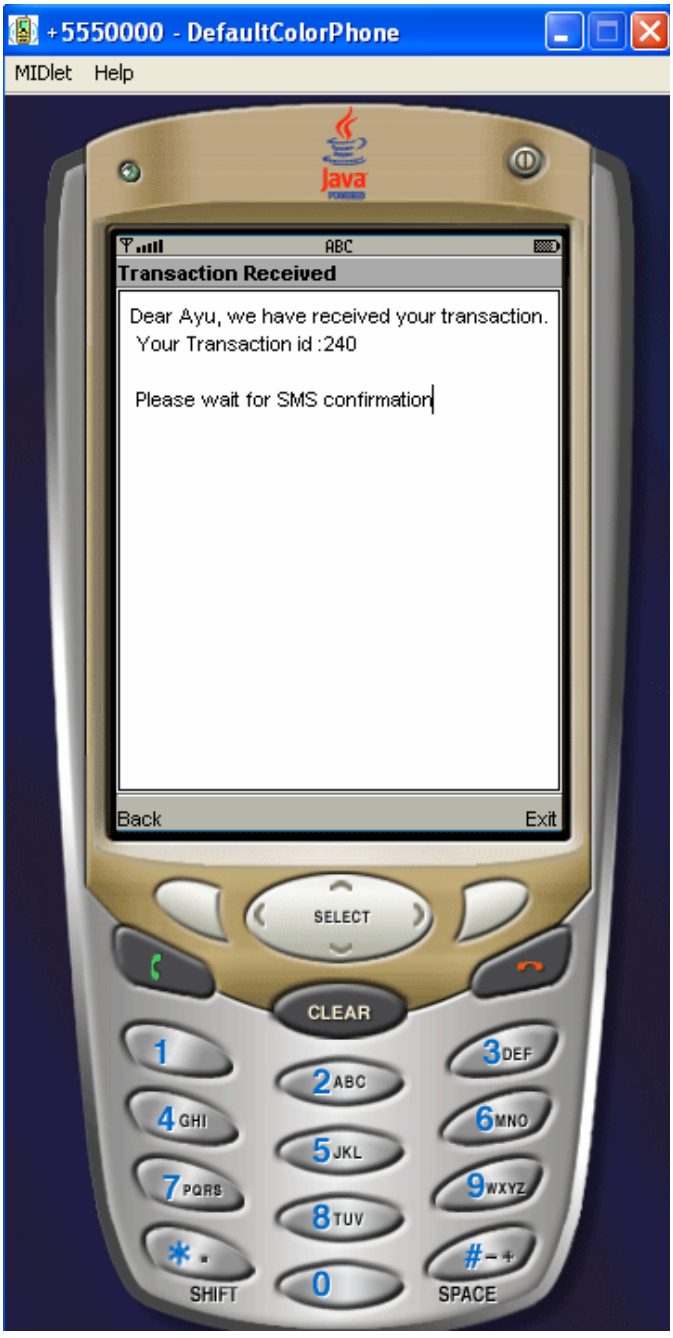
TIC PASSWORD TO OPEN TIC LIST



SELECTION OF ENCRYPTED TIC



SELECTED TIC IS ATTACHED WITH THE CREDIT CARD TRANSFER FORM



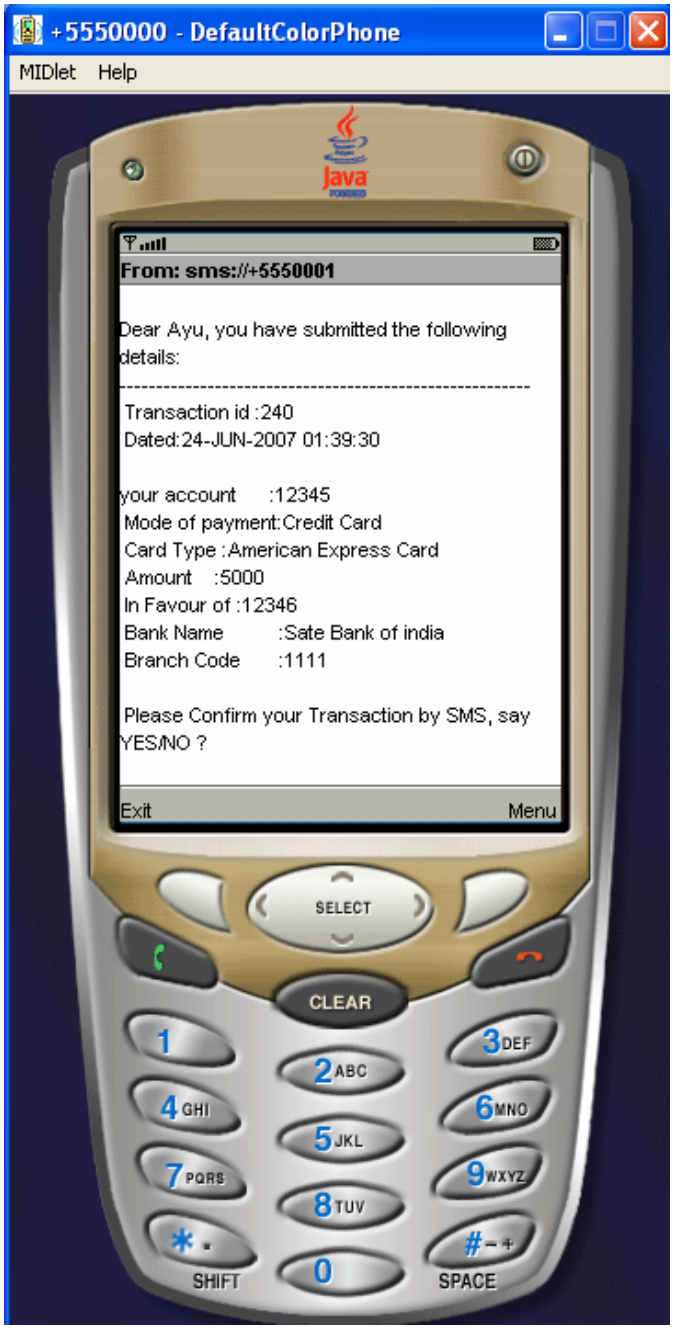
ACK FROM THE WEB SERVER WHICH SHOWS SUCCESSFUL TIC AUTHENTICATION OF USER

Java Servlet CardServlet is responsible for Credit Card based fund transfer and TIC authentication, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

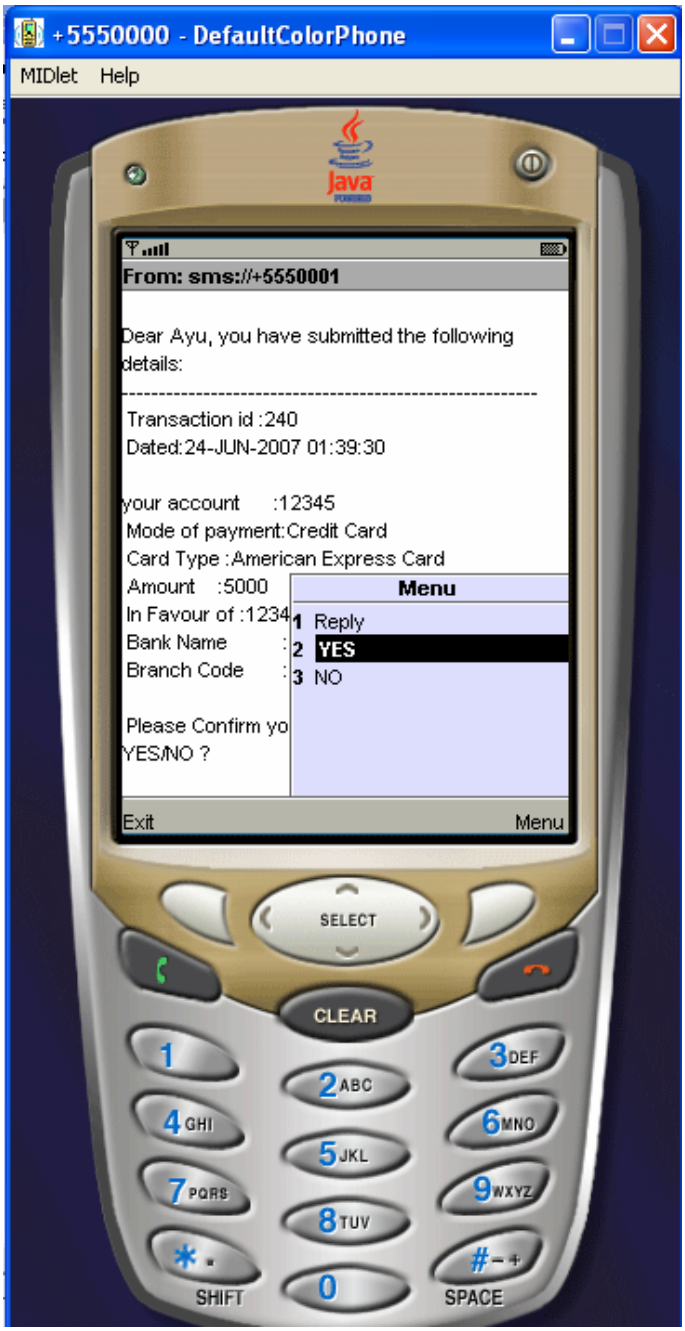
9.6 Third Authentication of user to the Bank or Financial Institution authentication Server

The Third Authentication of the user is based on SMS confirmation.

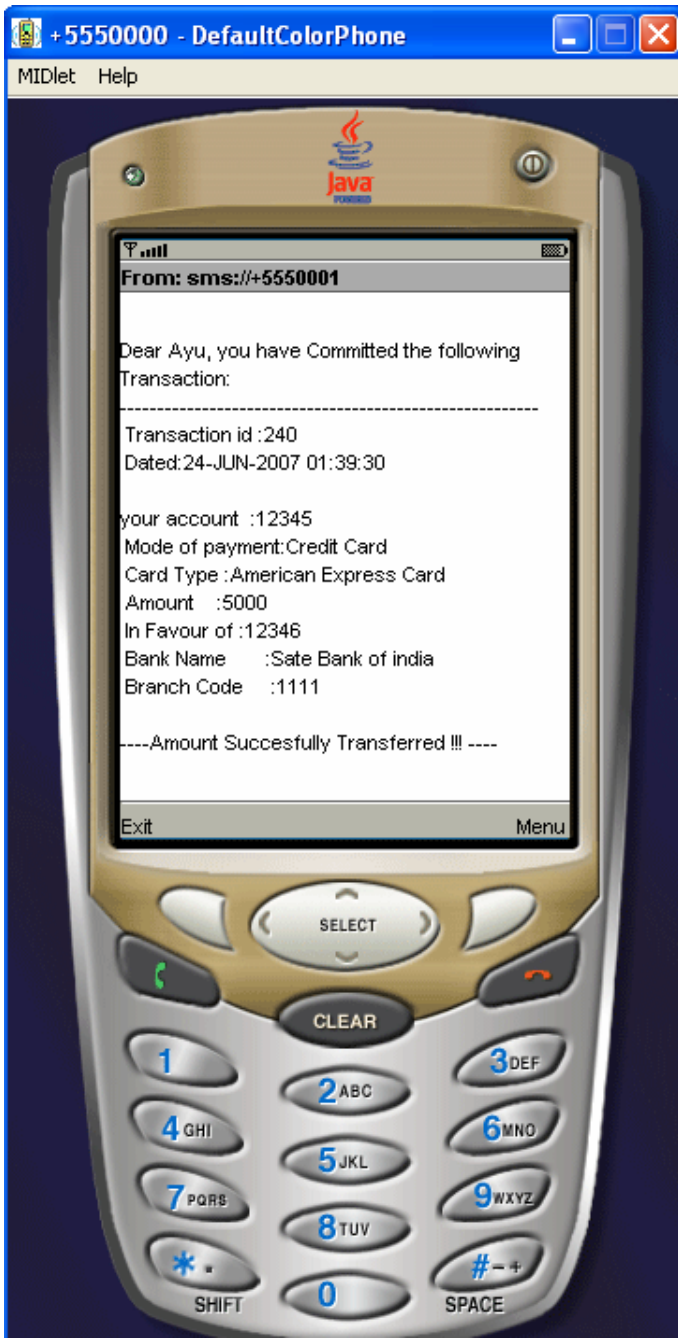
SMS RECEIVED FROM BANK AUTHENTICATION SERVER



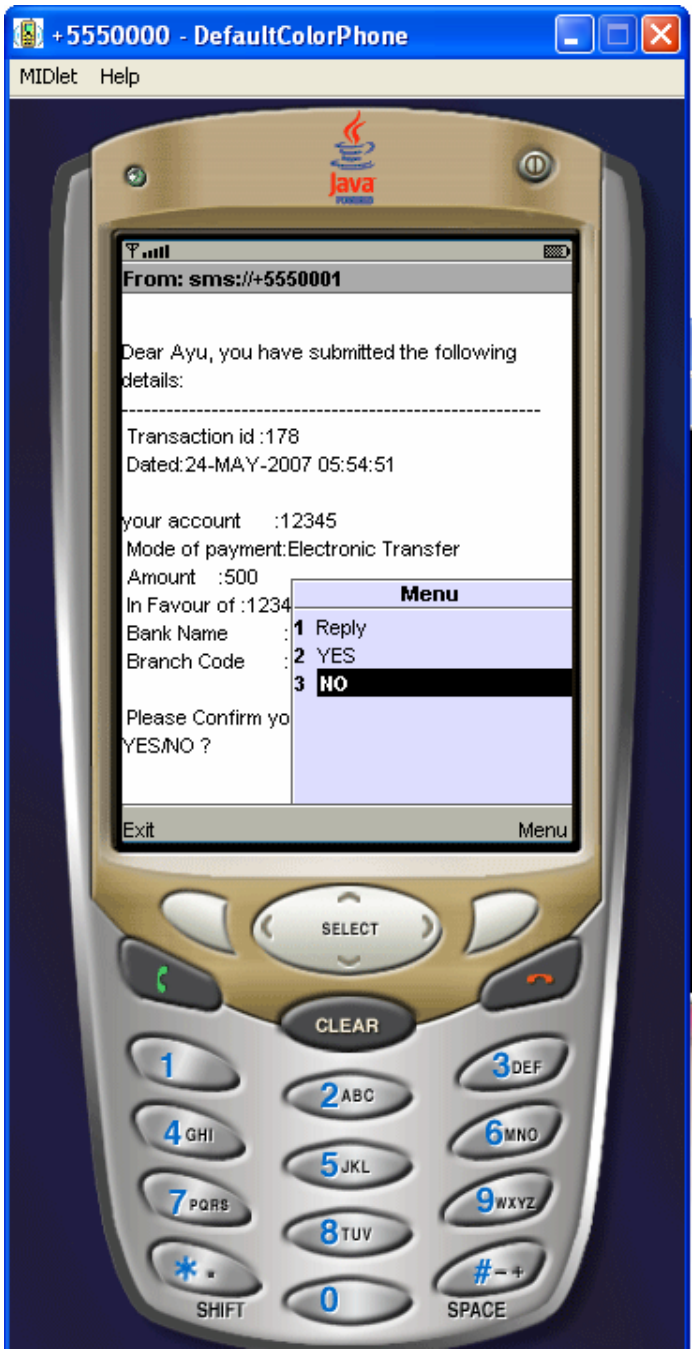
SMS SHOWS THE DETAILS OF SUBMITTED TRANSACTION



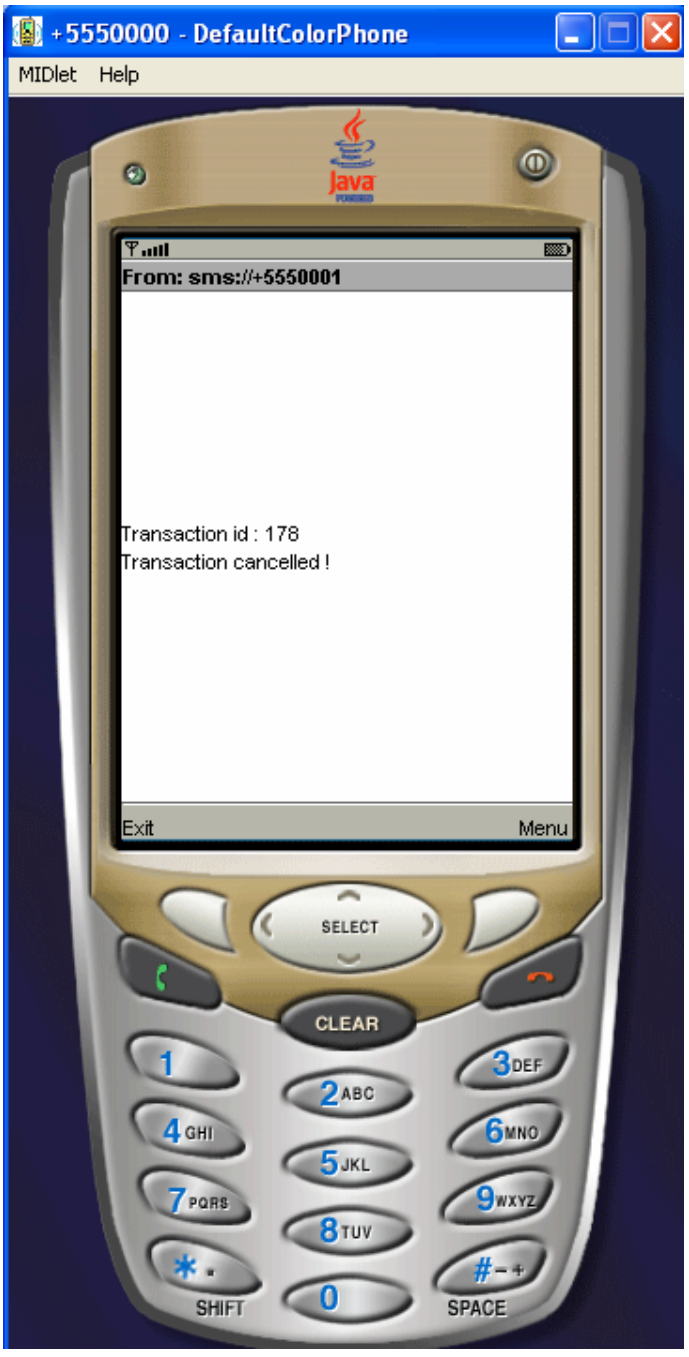
REPLY SMS WITH "YES"



RESPONSE FROM THE SERVER IF USER HAS REPLIED WITH "YES" SUCCESSFUL COMPLETION OF TRANSACTION



REPLY SMS WITH "NO"



RESPONSE FROM THE SERVER IF USER HAS REPLIED WITH "NO" TRANSACTION CANCELLED

Java Servlet SMSServlet is responsible to generate a SMS to the user for transaction confirmation & java servlet CommitServlet receives the response of the user confirmation SMS and takes action accordingly, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

9.7 Merchant Payment

Five easy steps of merchant payment are:

Step 1 : Merchant Authentication using Merchant Certificate.

Step 2 : Selection of Mode of Payment, There are two types of Mode of payment

- Electronic Transfer
- Credit Card based Transfer

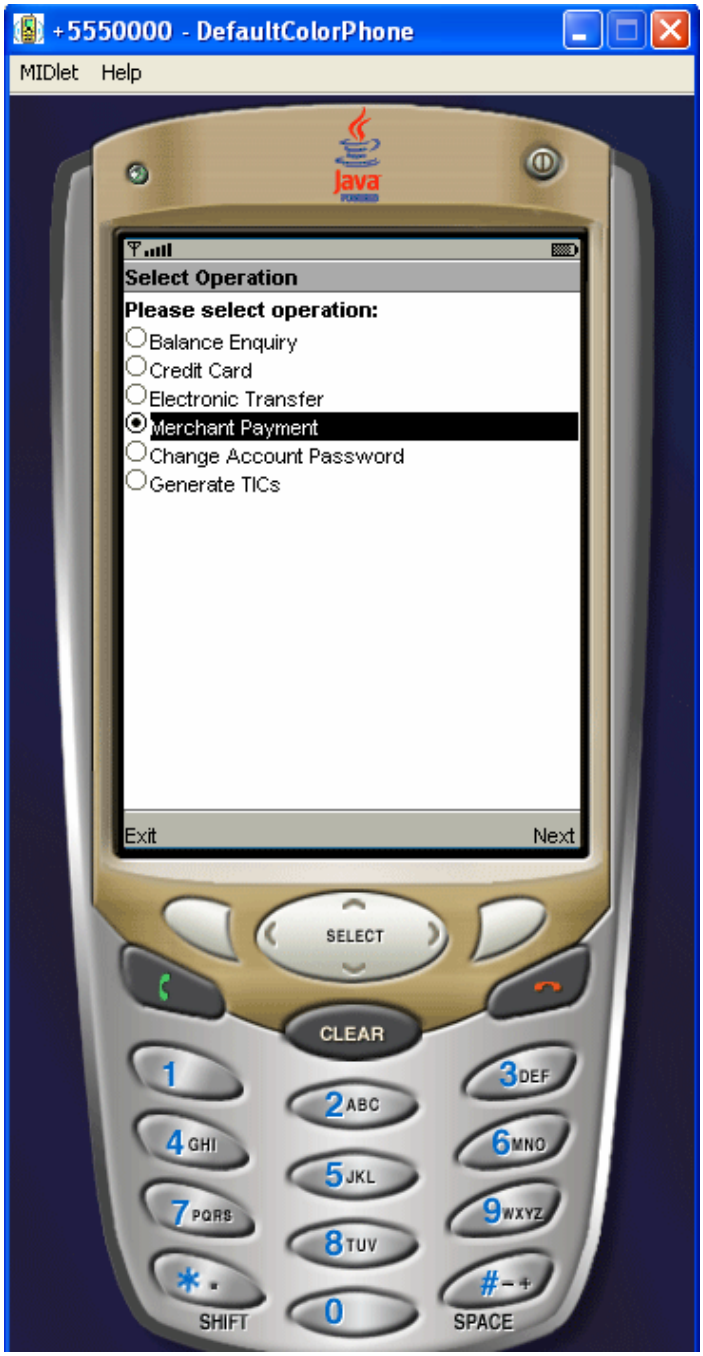
Step 3: Fill the simple entry form related to the merchant payment.

Step 4: Attach TIC code to the transaction for unique identification.

Step 5: Confirmation of transaction by SMS.

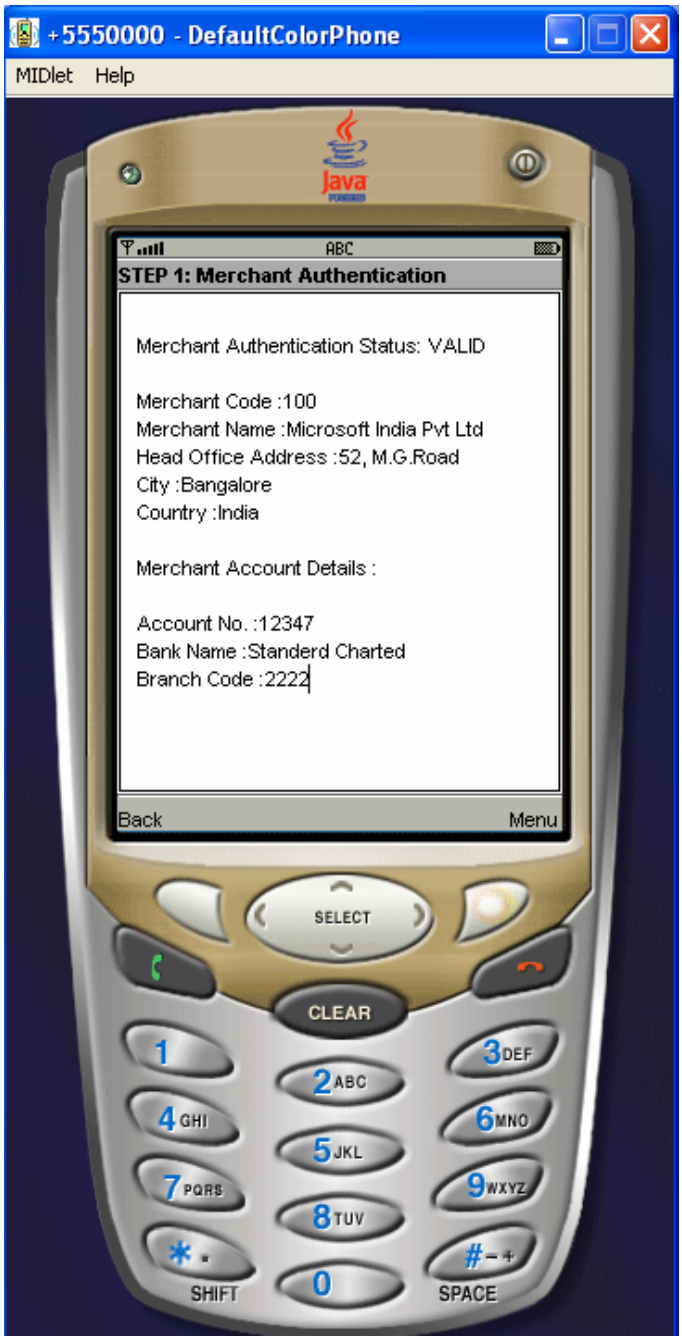
Simulation screens of all five steps are given on next pages.

Step 1 : Merchant Authentication using Merchant Certificate

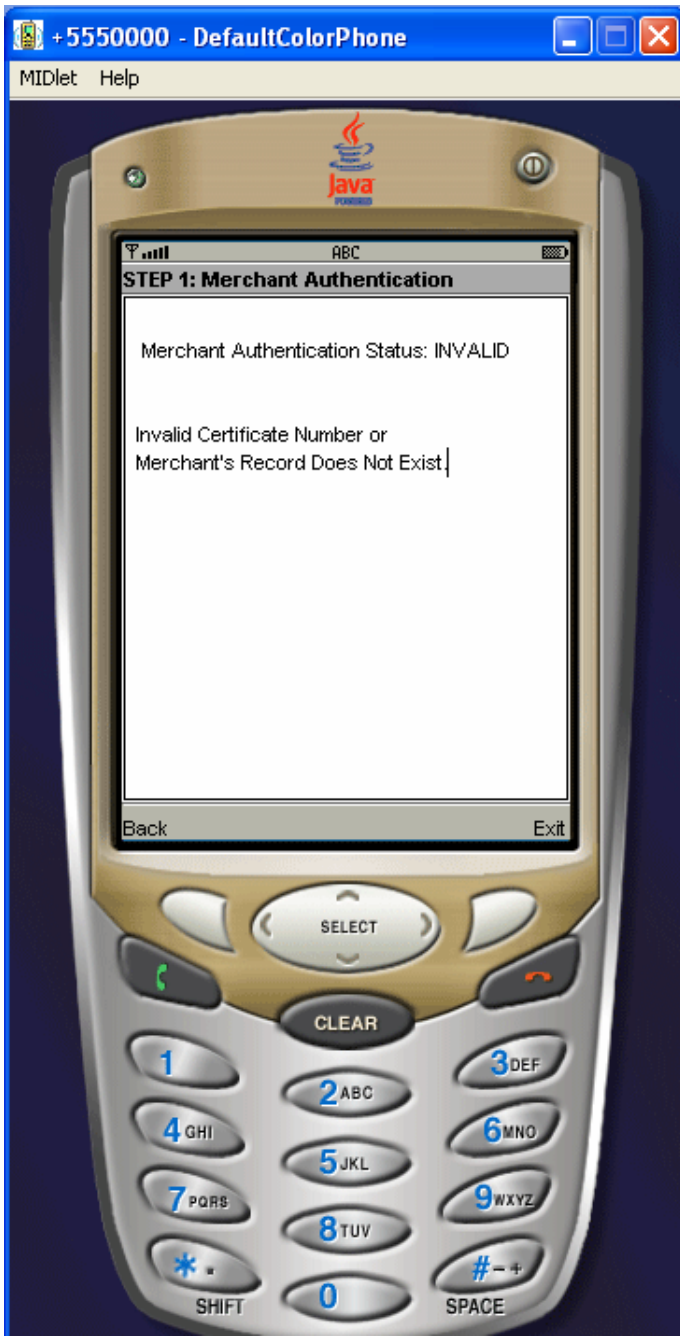


SELECTION OF MERCHANT PAYMENT OPTION

ENTER VALID MERCHANT CERTIFICATE NUMBER



VALID MERCHANT AUTHENTICATION RESPONSE



IF MERCHANT CERTIFICATE NUMBER IS INVALID

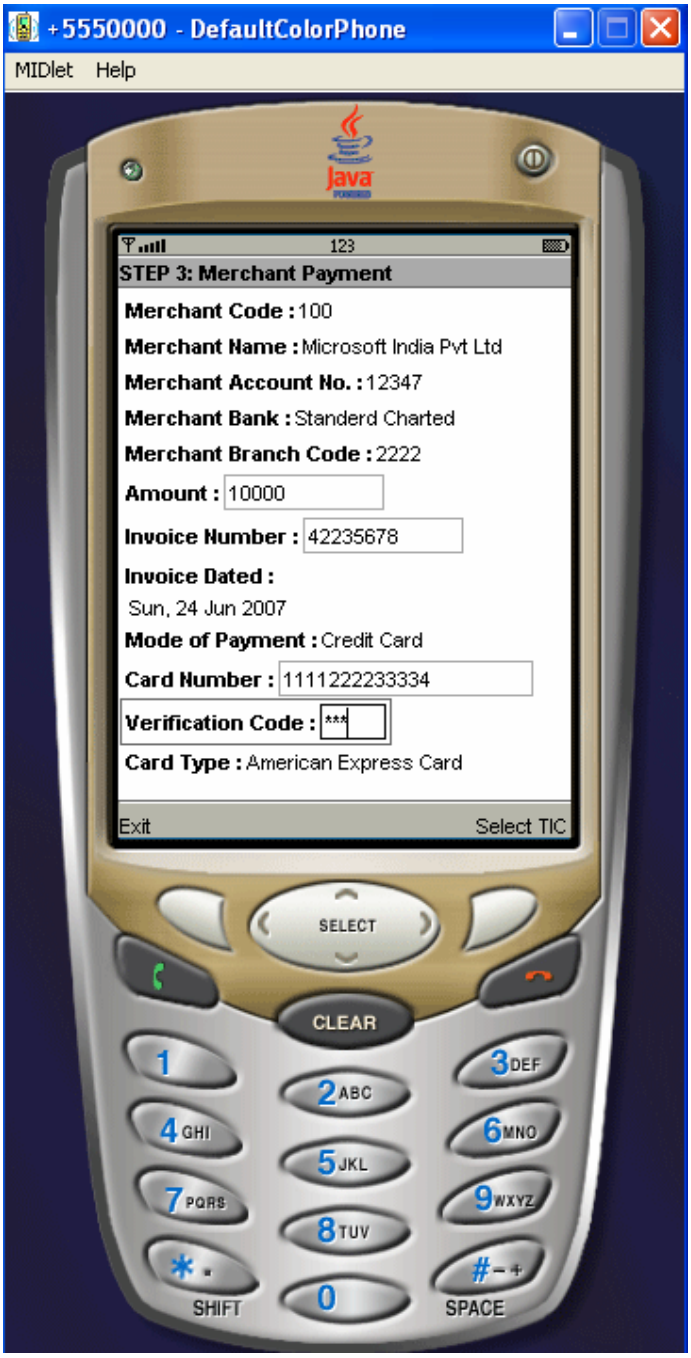
Java servlet MerchantServlet is responsible for Merchant authentication, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

Step 2 : Selection of Mode of Payment, There are two types of Mode of payment

MODE OF PAYMENT

SELECTION OF CREDIT CARD TYPE

Step 3: Fill the simple entry form related to the merchant payment

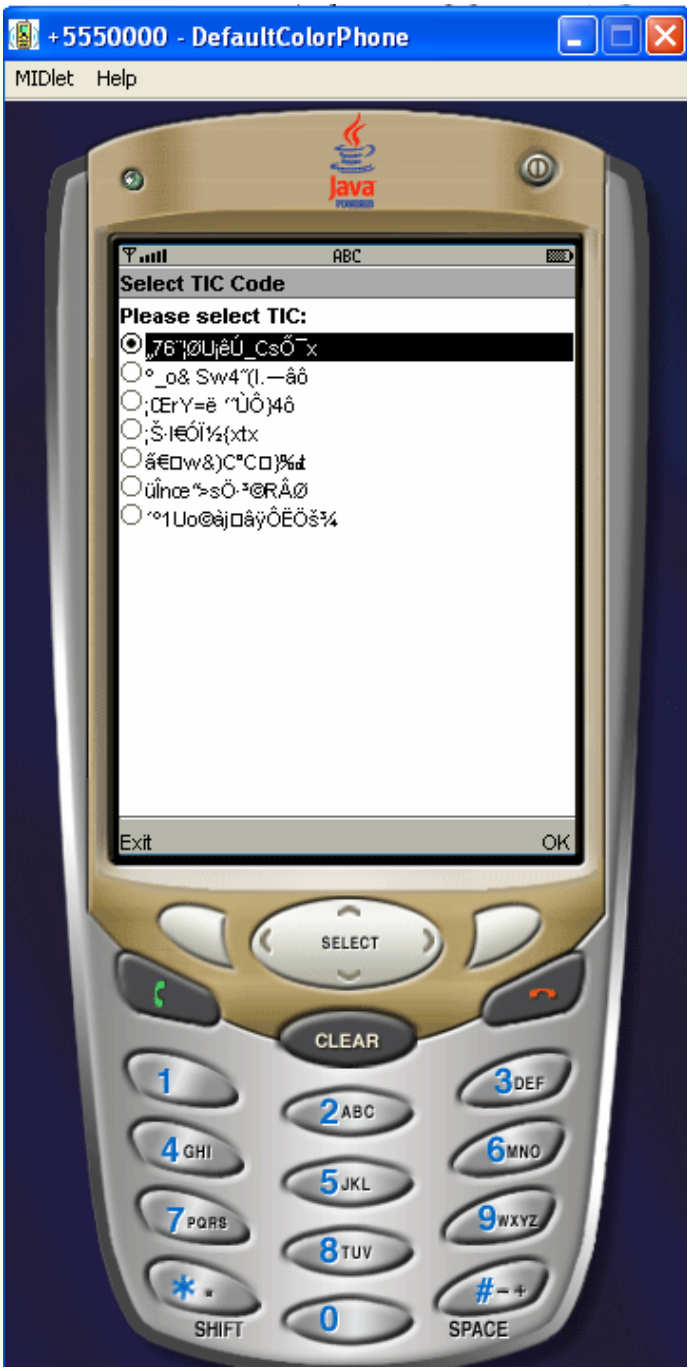


FILL PAYMENT INFORMATION

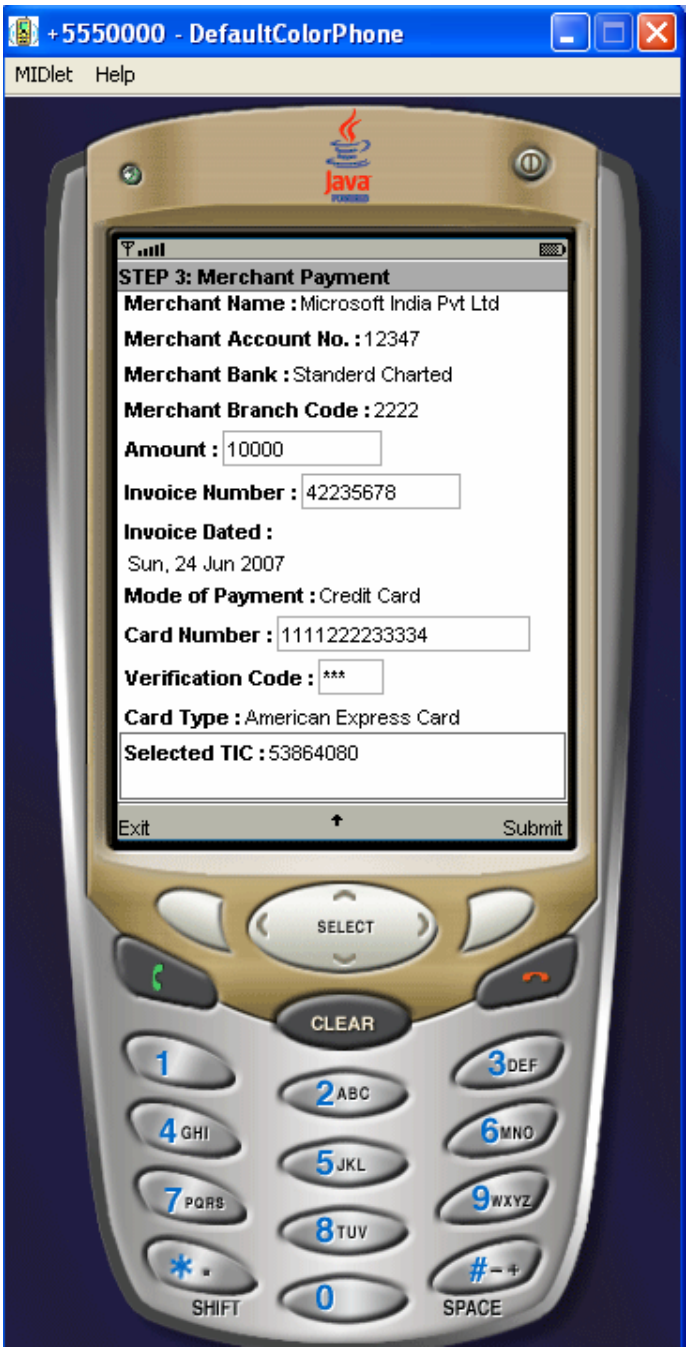
SELECTION OF INVOICE DATE

Step 4: Attach TIC code to the transaction for unique identification

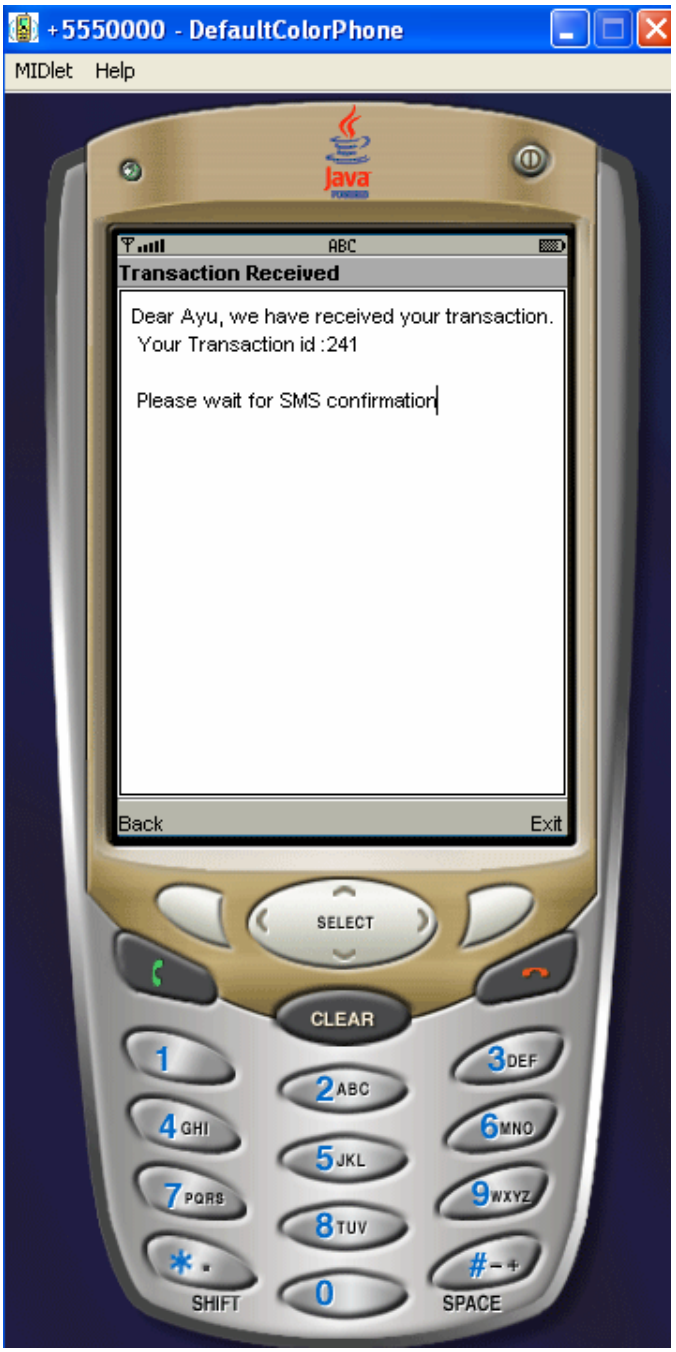
PASSWORD TO OPEN TIC LIST



SELECTION OF INVOICE DATE



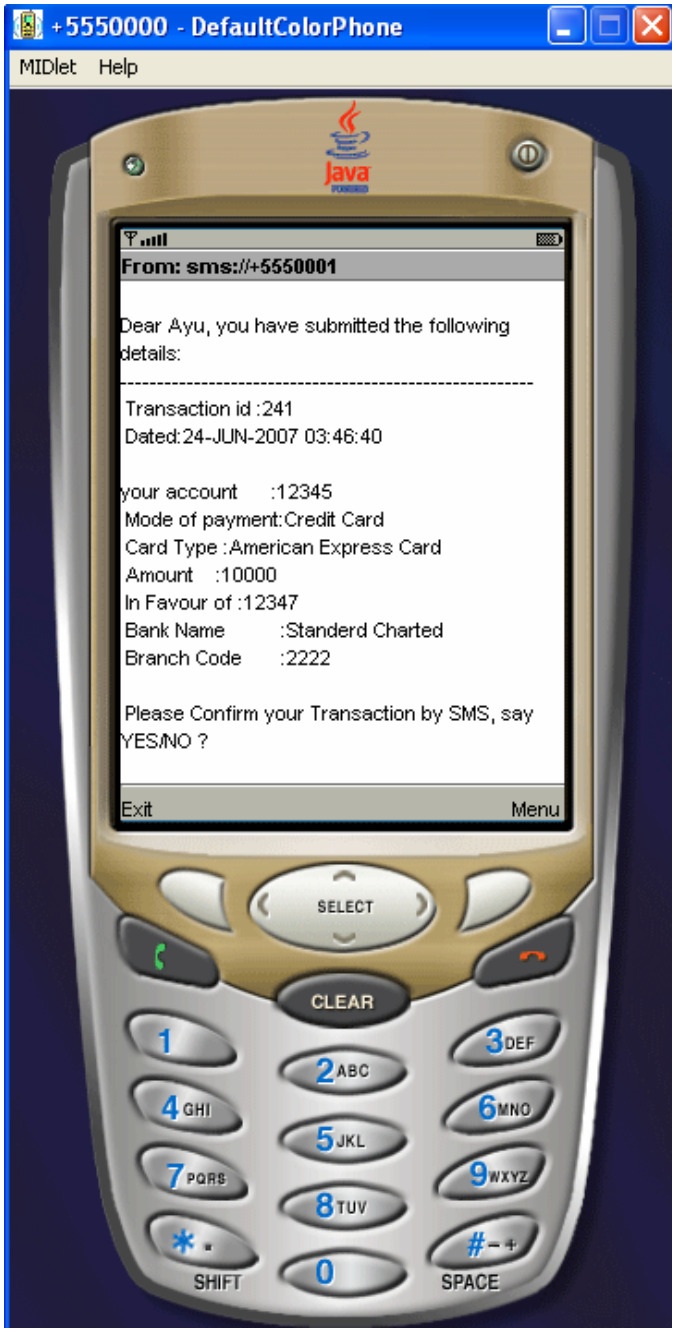
SELECTED TIC IS ATTACHED WITH THE MERCHANT PAYMENT FORM



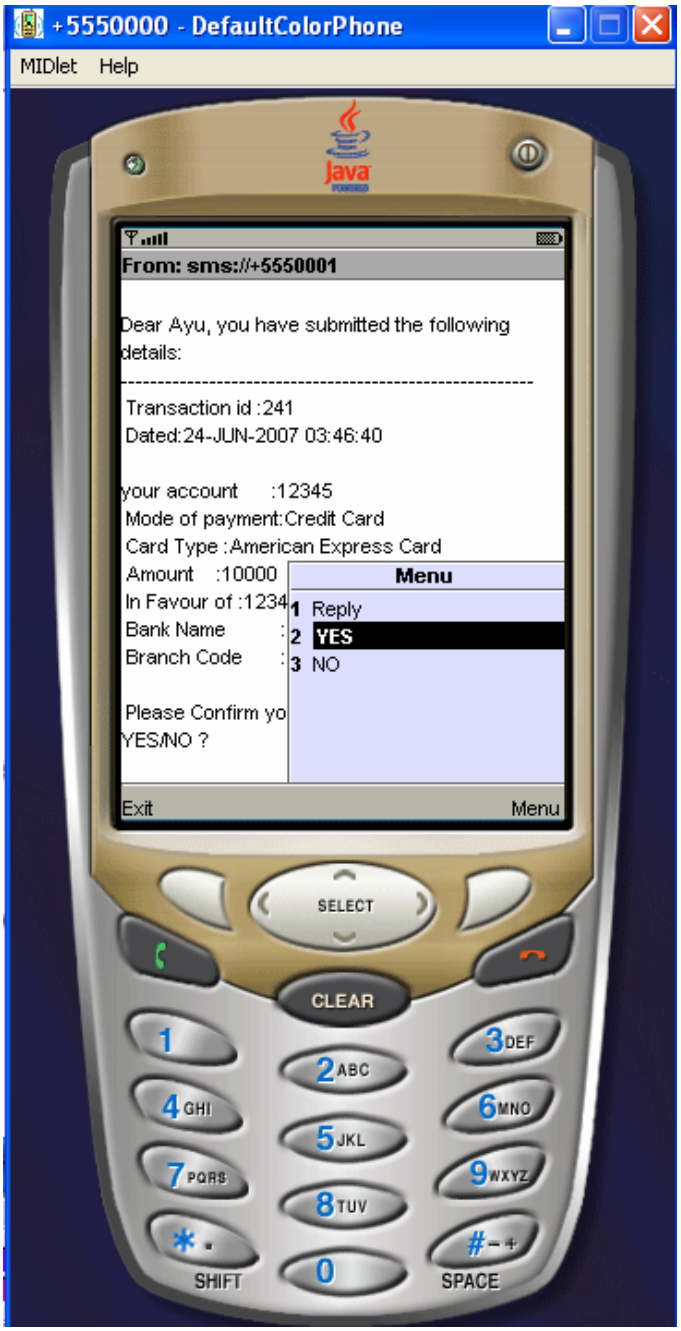
ACK FROM THE SERVER WHICH SHOWS SUCCESSFUL TIC AUTHENTICATION OF MERCHANT PAYMENT

Step 5: Confirmation of payment transaction by SMS

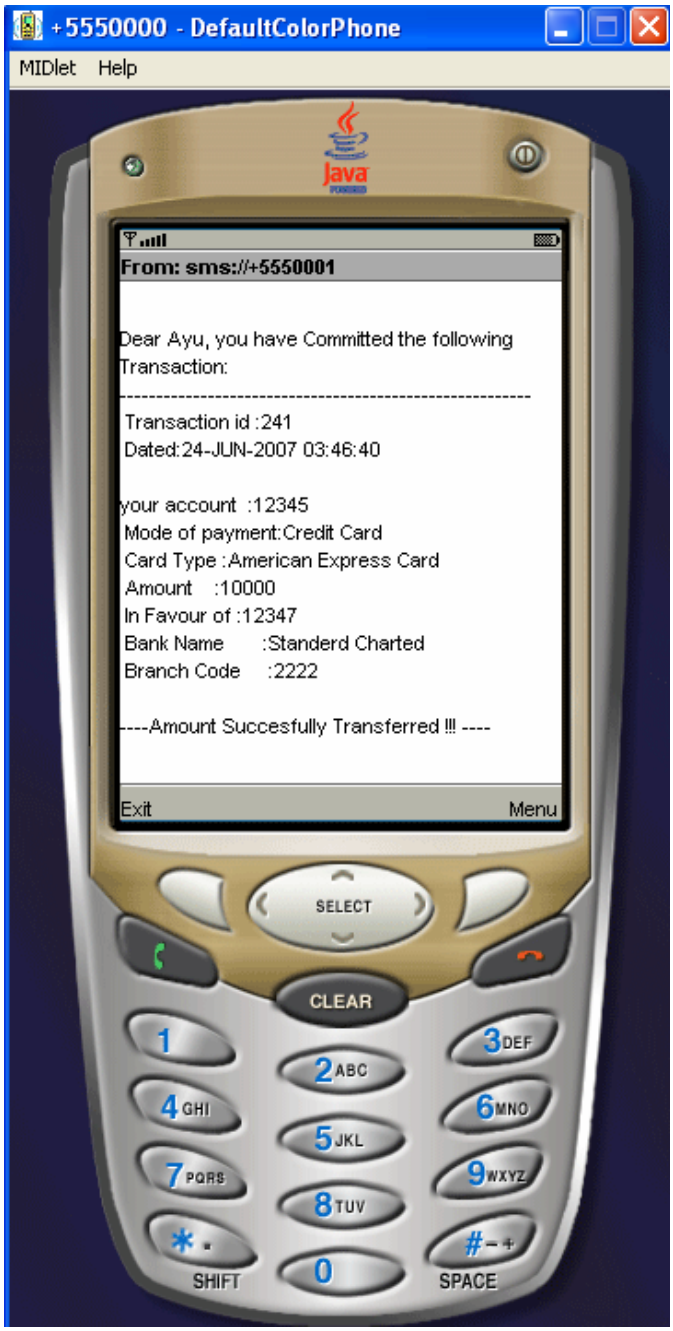
SMS RECEIVED FROM BANK AUTHENTICATION SERVER



SMS SHOWS THE DETAILS OF SUBMITTED TRANSACTION



REPLY SMS WITH "YES"



RESPONSE FROM THE SERVER SUCCESSFUL COMPLETION OF MERCHANT PAYMENT

9.8 Change Account Password

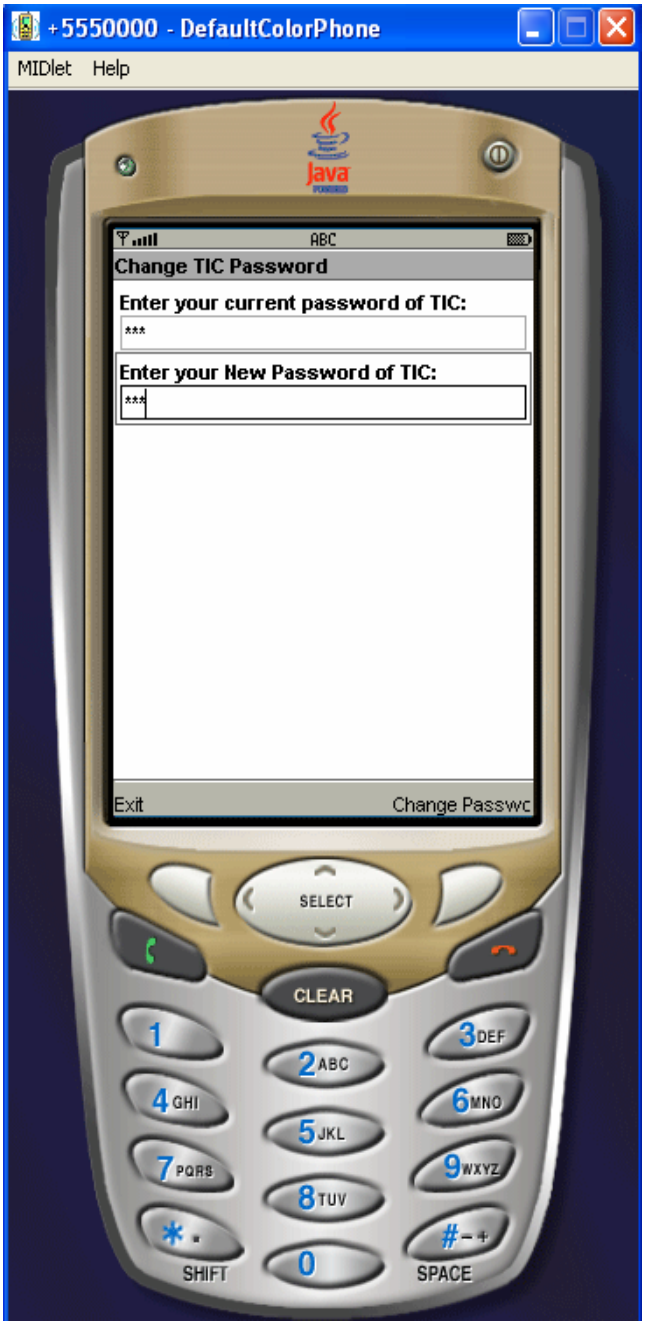
ENTER OLD PASSWORD AND NEW PASSWORD

RESPONSE FROM THE SERVER SUCCESSFULLY PASSWORD HAS BEEN CHANGED

Java Servlet PasswordServlet is responsible to change user account password, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

9.9 Change TIC Password

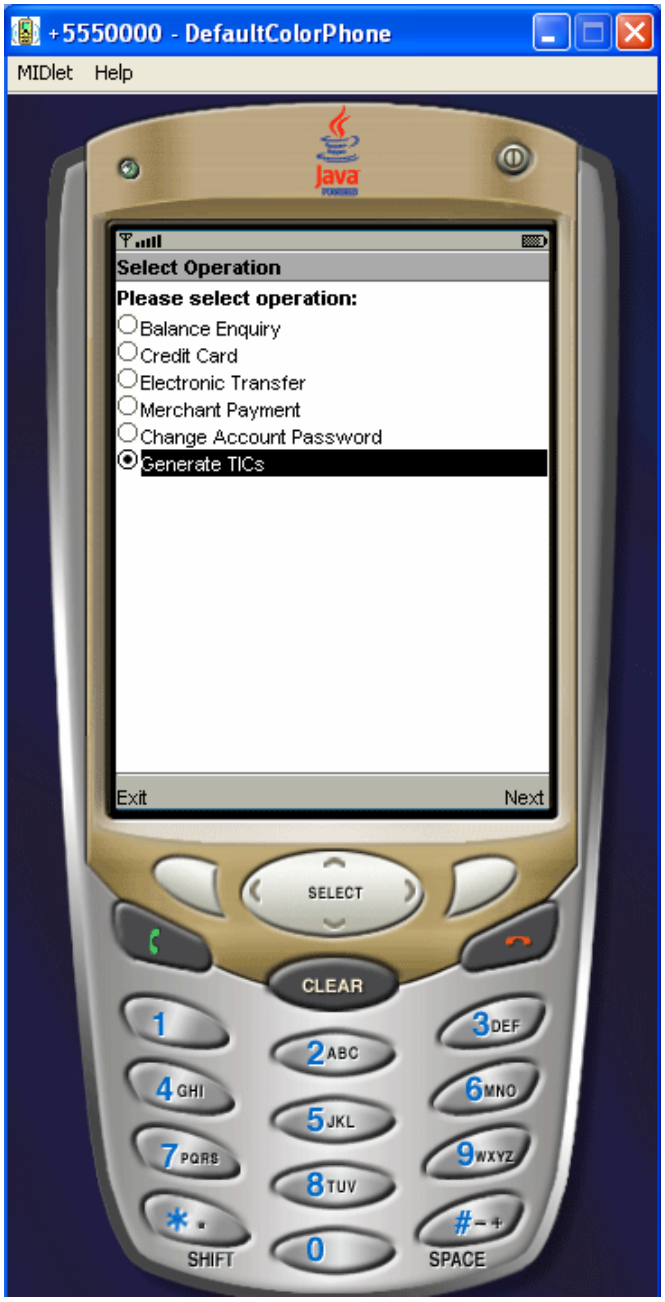
SELECT CHANGE PASSWORD OF TIC OPTION



ENTER OLD TIC PASSWORD AND NEW TIC PASSWORD

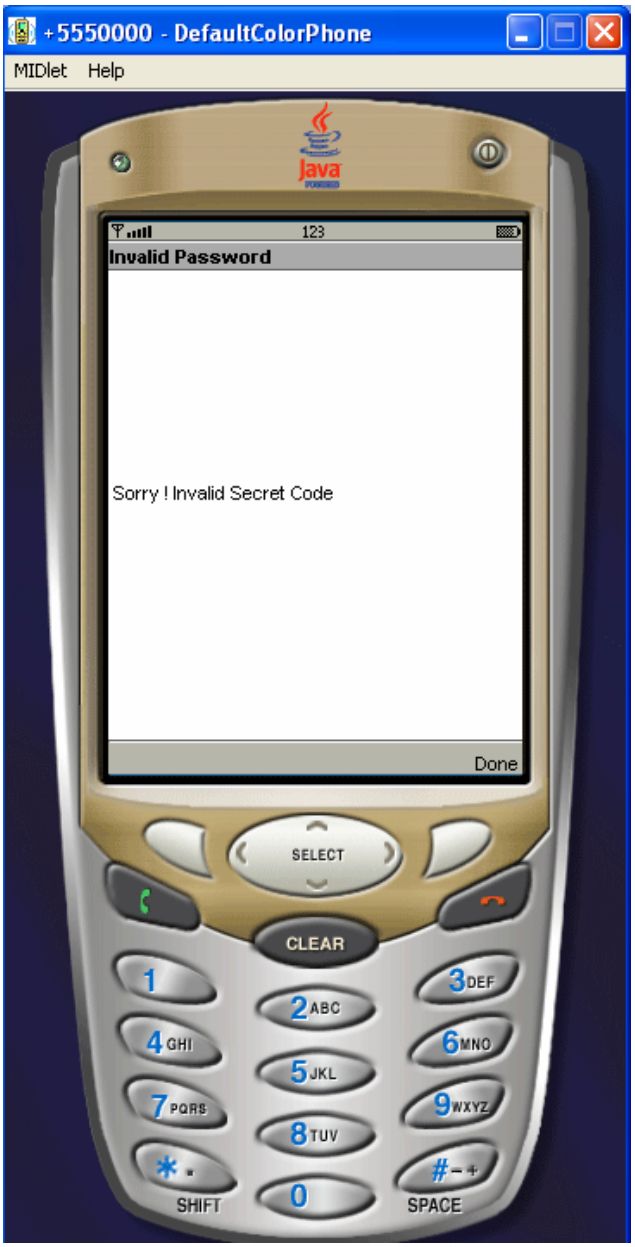
TIC PASSWORD HAS BEEN CHANGED SUCCESFULLY

9.10 TIC Generation



SELECT GENERATE TIC OPTION

ENTER NUMBER OF REQUIRED TICS AND VALID SECRET CODE



IF ENTERED SECRET CODE IS NOT VALID

IF ENTERED SECRET CODE IS VALID

Java Servlet GenTICServlet is used to load TIC codes on user cell phones/PDA from server, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

9.11 Some Alert Messages

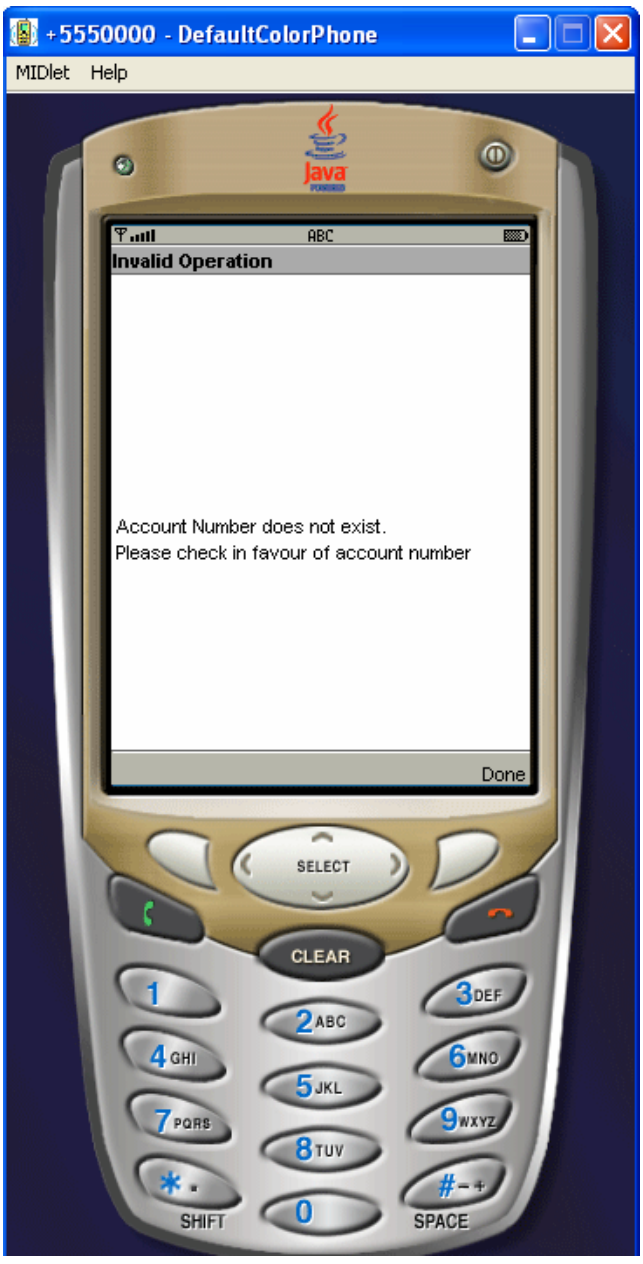
IF LOGIN FAIL

IF WRONG TIC PASSWORD

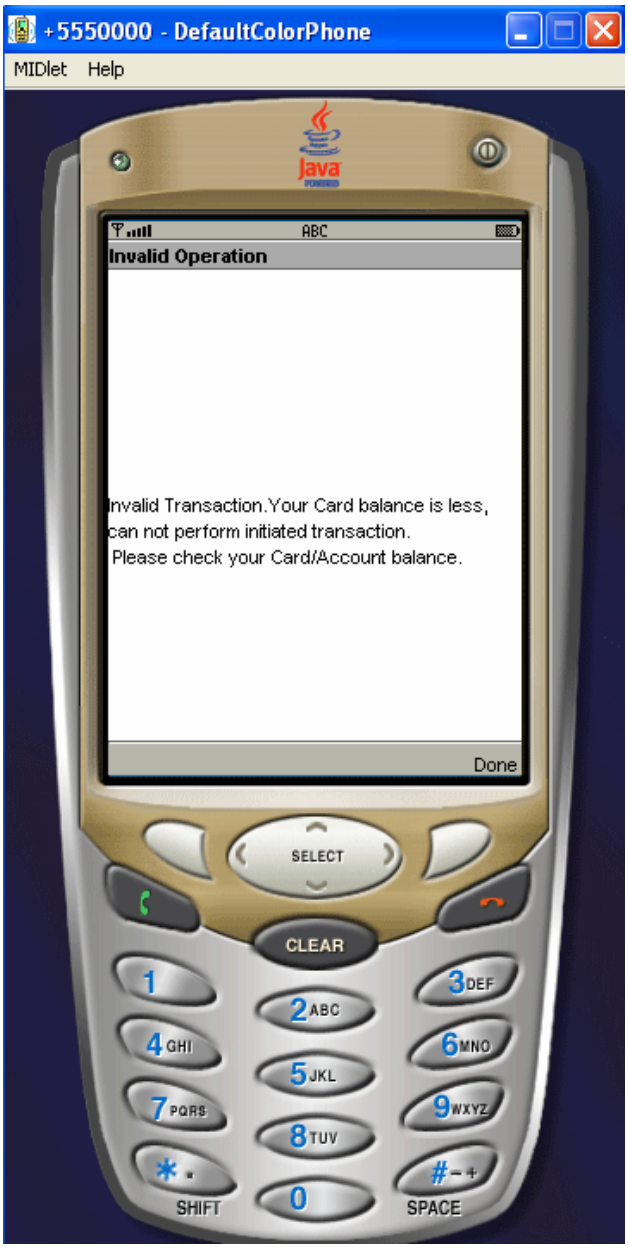
IF TRANSACTION SUBMITTED WITH INVALID TIC CODE

IF USER REPLY "NO" TO CONFIRMATION SMS

IF TRANSACTION AMOUNT EXCEEDS THE CURRENT BALANCE OF THE ACCOUNT



IF IN FAVOUR OF ACCOUNT NUMBER DOES NOT EXIST



IF TRANSACTION AMOUNT EXCEEDS THE CURRENT BALANCE OF THE CREDIT CARD

IF CREDIT CARD IS NOT VALID

IF USER SESSION TIME OUT

LIST OF PENDING TRANSACTIONS FOR SMS CONFIRMATION ON SERVER

Java Servlet PTServlet is used to generate the list of all pending transactions on the server to monitor by administrator, for detail description of database schema and server side java servlets please refer Appendix – A & Appendix – B.

Chapter 10

Conclusion and Future Work

Security is a major issue in internet based online payment system. There are various internet threats which affect the security system of internet and increase risk for electronic transaction. The current authentication technique for online payment system is not very secure to protect user from identity theft, as a the result any attacker gain the access on confidential information of user like credit card number or account password and make illegal transfer of fund which will be charged to the valid user's account. It is proved from our background study that single factor authentication increases risks posed by phishing, identify theft, online fraud and loss of customer confidential information. So, financial institution should implement an effective authentication to reduce fraud and make stronger security for applications. Strong customer authentication is necessary to enforce security and assist financial institutions to detect and decrease user identity thefts.

In the presented protocol we have focused on an application-layer security solution for wireless payment system to implement an end-to-end authentication and data confidentiality between wireless client and java based secure server. The presented work proposed a new protocol for web user authentication based on multifactor authentication approach which is completely secure and easy to implement.

We have also suggested an approach for two-way authentication protocol to authenticate both the parties. This solution can be implemented within the available resources of a J2ME based devices and it does not require any modification in existing wireless networks or protocol.

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 codes 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.

Appendix-A

Database Design & Schema

This appendix lists the database tables used in simulation of the system. Tables are linked to each other with various integrity constrains.

Table Name: Login_Master

Description: Table contains the user login information, user password and secret code which is used for TIC generation.

Field Name	Data Type	Integrity Constraints	Description
ACCOUNT_NO	number (8)	Primary Key	User Login Name
PASSWORD	varchar2(10)		User password
SECRET_CODE	number(4)		Secret code

Table Name: Customer_Master

Description: Table contains the customer information.

Field Name	Data Type	Integrity Constraints	Description
ACCOUNT_NO	number (8)	Primary Key	Customer Account Number
NAME	varchar2(20)	Not Null	Customer Name
ADDRESS	varchar2(30)	Not Null	Customer Address
CITY	varchar2(25)	Not Null	Customer City
COUNTRY	varchar2(20)	Not Null	Customer Country
CELL_NO	number (10)	Not Null	Cell no. of customer

Table Name: TIC_Master

Description: Table contains the list of TICs issued to the customers.

Field Name	Data Type	Integrity Constraints	Description
ACCOUNT_NO	number (8)	Foreign Key reference to customer_master table	Customer Account Number
TIC	varchar2(8)		TIC Codes issued to the customer

Table Name: Customer_Detail

Description: Table contains the detail of customer account.

Field Name	Data Type	Integrity Constraints	Description
ACCOUNT_NO	number (8)	Foreign Key reference to customer_master table	Customer Account Number
BRANCH_CODE	number(5)	Foreign Key reference to bank_master table	Customer Bank Branch Code
BALANCE	number(8,2)	Default 0.0 Rs.	Current Balance of Account
ACCOUNT_TYPE	varchar2(20)	Not Null	Account type

Table Name: Bank_Master

Description: Table contains Bank information.

Field Name	Data Type	Integrity Constraints	Description
BRANCH_CODE	number (5)	Primary Key	Branch Code Number
BANK_NAME	Varchar2(30)	Not Null	Bank Name
BRANCH_ADDRESS	varchar2(30)	Not Null	Branch Address
CITY	varchar2(25)	Not Null	Branch City
COUNTRY	varchar2(20)	Not Null	Branch Country
PHONE_NO	number (10)	Not Null	Phone Number of Bank.

Table Name: Card_Master

Description: Table contains Credit Card Information.

Field Name	Data Type	Integrity Constraints	Description
CARD_NO	number (16)	Primary Key	Credit Card Number
COMPANY	varchar2(25)	Not Null	Banker's Name
COST	number (8,2)	Not Null	Credit Card Amount
CARD_TYPE	varchar2(40)	Not Null	Card Type

Table Name: Card_Datail

Description: Table contains issued Credit Card detail Information.

Field Name	Data Type	Integrity Constraints	Description
CARD_NO	number (16)	Foreign Key reference to card_master table	Credit Card Number
ACCOUNT_NO	number (8)	Foreign Key reference to customer_master table	Customer Account Number
ISSUE_DATE	Date	Not Null	Credit Card issue date
EXP_DATE	Date	Not Null	Credit Card Expiry Date

Table Name: Card_Transactions

Description: Table contains details about the Credit Card transaction.

Field Name	Data Type	Integrity Constraints	Description
CARD_NO	number (16)	Foreign Key reference to card_master table	Credit Card Number
ACCOUNT_NO	number (8)	Foreign Key reference to customer_master table	Customer Account Number
TOTAL_EXP	number (8,2)	Not Null	Transaction Amount
TRANSACTION_ID	number (8)	Not Null, Unique	Credit Card Transaction id.
TDATE	Date	Not Null	Transaction Date

Table Name: Merchant_Master

Description : Table contains Merchant Information.

Field Name	Data Type	Integrity Constraints	Description
MERCHANT_ID	number(10)	Primary Key	Merchant unique id
CERTIFICATE_NO	number(10)	Unique and Not Null	Merchant authentication Certificate
MNAME	varchar2(25)	Not Null	Merchant Full Name
HEADOFF_ADD	varchar2(40)	Not Null	Merchant's Head Office Address
MCITY	varchar2(25)	Not Null	Merchant City
MCOUNTRY	varchar2(20)	Not Null	Merchant Country
PHONE_NO	number(10)	Not Null	Merchant Phone No.
ISSUE_DATE	Date	Not Null	Certificate Issue date
VALID_UPTO	Date	Not Null	Certificate Expiry Date

Table Name : Merchant_Detail

Description : Table contains Merchant accouant Information.

Field Name	Data Type	Integrity Constraints	Description
MERCHANT_ID	number (16)	Foreign Key reference to merchant_master table	Merchant id
ACCOUNT_NO	number (8)	Foreign Key reference to customer_master table	Customer Account Number
BANK_NAME	Varchar2(30)	Not Null	Merchant Bank Name
BRANCH_CODE	Number(5)	Foreign Key reference to bank_master table	Merchant Bank's Branch Code

Table Name: Transaction_Master

Description: Table contains information about online submitted transactions by customers.

Field Name	Data Type	Integrity Constraints	Description
TRANSACTION_ID	number (8)	Not Null, Unique	Online Transaction id.
ACCOUNT_NO	number (8)	Foreign Key reference to customer_master table	Customer Account Number
AMOUNT	number (8,2)	Not Null	Transaction Amount
FAVOUR	number (8)	Foreign Key reference to customer_master table	Customer Account Number
MODEOFTRANSFER	varchar2(25)	Not Null	Mode of Payment
BANK	varchar2(30)	Not Null	In the Favour of Bank Name
BRANCH_CODE	Number(5)	Foreign Key reference to bank_master table	In the Fovour to Branch Code
TIC	varchar2(8)	Not Null	Used TIC Code for a Transaction
CARD_NO	number (16)	Foreign Key reference to card_master table	Used Credit Card Number
SMS_CONFIRM	varchar2(3)		User Response to Confirmation SMS
TDATE	Date	Not Null	Transaction date
INVOICE_NO	varchar2(10)		Invoice number in case of merchant payment
INVOICE_DATE	Date		Invoice date in case of merchant payment

Appendix-B

Server Side Java Servlets

This appendix shows the server side implementations of the system, the list of Java Servlets which are responsible for server side functionality are a follows:

1. **LoginServlet:** A LoginServlet is responsible for users logging authentication, it decrypts the username and password from the http request and matches the details of user from database and generates welcome message with user session key.

2. **BalanceEnqServlet:** A BalanceEnqServlet is responsible for balance enquiry, it generates the current account balance of the user.

3. **ETransferServlet:** A EtransferServlet will be executed if the user will submit a transaction of Electronic Transfer of fund. It is also responsible for decrypting the confidential data received in an encrypted form and send ACK to the user with transaction id.

4. **CardServlet:** A CardServlet will be executed if the user will submit a transaction using Credit Card for transfer of fund. It is also responsible for decrypting the confidential data received in an encrypted form, check the authenticity of the Credit card and send ACK to the user with transaction id.

5. **BankServlet :** A BankServlet is responsible to generate the Bank Names with their corresponding Branch code to make for the transfer of fund. Note that it shows the list of all associated Bank names to which user can make money transfer.

6. **SMSServlet:** A SMSServlet is used to generate an SMS to the user for transaction confirmation. It automatically retrieves the Cell Phone number of the user and sends SMS for confirmation.

7. **CommitServlet:** A CommitServlet receives the response of the user confirmation SMS and takes action accordingly. If user has chosen "YES" then it commits the transaction on the server and generates ACK message to the user. If the user has chosen "NO" then it cancelled the transaction and generates cancellation message to the user.

8. **PTServlets:** A PTServlet is used to generate the list of all pending transactions on the server. It gives functionality to the administrator to monitor the pending transactions.

9. **PasswordServlet:** A PasswordServlet is responsible to give the functionality of password changing. It also uses necessary encryption/decryption to maintain the confidentiality of the system.

10. **MerchantServlet:** A MerchantServlet is responsible for Merchant authentication. It uses merchant certificate to make merchant authentication with necessary encryption/decryption to maintain system confidentiality.

11. **GenTICServlet:** A GenTICServlet is used to load TIC codes on user cell phones/PDAs according to the user requirement. It follows strictly encryption/decryption mechanism to transfer TICs to the client environment.

Appendix-C

Commands and Settings

The proposed system has been implemented in a Java based environment. In order to run the system various commands have been used. Some of the main commands are listed here:

CLASSPATH Setting:

It is used to run J2ME and Wireless Tool kit, Tomcat Web Server and Java Servlet:

CLASSPATH =C:\ProgramFiles\Java\jdk1.5.0_06\bin;

CLASSPATH = C:\apache-tomcat-5.5.17\common\lib\servlet-api.jar;

CLASSPATH = C:\apache-tomcat-5.5.17\common\lib\jsp-api.jar;

CLASSPATH = C:\Program Files\Java\jdk1.5.0_06\jre\lib\jce.jar;

CLASSPATH = C:\satsa1.0\bin;

CLASSPATH = C:\satsa1.0\lib;

CLASSPATH = D:\oracle\jdbc\lib\ojdbc14.jar

CLASSPATH = D:\oracle\jdbc\lib\classes12.jar;

Other Environment Variable settings:

JAVA_HOME =C:\Program Files\Java\jdk1.5.0_06

MIDP_HOME= C:\satsa1.0

ORACLE_SID= iiita

JSERV= D:\oracle\Apache\Jserv\conf

JSRV= D:\oracle\Apache\Jserv\conf

Command to Compile Java Servlets :

C:\Servlets > *javac Servletname.java*

Wireless Development Tool kit required parameters settings:

MIDlet-Name = Multifactor

MIDlet-Jar-Url = Multifactor.jar

MIDlet-Vendor= iiita

MIDlet-Version= 1.0

MicroEdition-Configuration= CLDC-1.0

MicroEdition-Profile= MIDP-2.0

MIDlet Names:

MIDlet	MIDlet-Name	Package.ClassName
MIDlet-1	Multifactor	Multi.Multifactor
MIDlet-2	Send SMS	sms.SMSSend
MIDlet-3	Receive SMS	sms.SMSReceive
MIDlet-4	Server Application	serversms.SMSSend

Wireless Development Tool kit for user defined parameters settings:

Bank-Cell= +5550001

SMS-Port= sms://50000

Appendix-D

Terms and Abbreviations

The following key words have been used throughout the thesis, Standard definitions have been taken from various websites including www.wikipedia.org, www.sun.com, and various research and white papers as mentioned in reference section.

ACK Acknowledgement

AES Advanced Encryption Algorithms (AES) is a symmetric key encryption/decryption technique.

AMS Application Management software (AMS) is used to manage applications. The application model defines various techniques related to the management of application and the distribution of the management process between the application and the underlying system.

API Application Programming Interface (API) is a programming code interface used in program library to support various application specific services.

CA Customer Agent (CA) is a software running of the client environment (on user's cell phone/ PDA)

CB Customer Bank (CB) is a financial institution in which the user has valid account.

CBAS Customer Bank Authentication Server (CBAS) is a separate server responsible for user authentication. It is installed at bank or financial institution.

CLDC Connected Limited Device Configuration (CLDC) is a specification given by Sun MicroSystem for Java ME applications. This is designed for devices with very limited resources like mobile phones and pagers. The defined specifications for CLDC are JSR 30 & JSR 139.

GPRS General Packet Radio Service (GPRS) can be supprt services such as WAP, Internet browsing, email of mobile phones. Charges of GPRS are on the basis of data transfer per megabyte instead of connection time.

HTTP Hyper Text Transfer Protocol (HTTP) is a stateless protocol which supports feature of independent data transferred. It is an application-level protocol for collaborative, distributed, hypermedia information systems. It is used in Internet web browsing.

JAR JAVA Achieve (JAR) file is a file format which is similar to ZIP file format and it can aggregate many files in a one file. A JAR file is basically zip file that contains META-INF directory.

JDBC Java Database Connectivity (JDBC) is an API to establish a database connection in Java programming language. It supports various methods for data manipulations and database queries.

JDK Java SE Development Kit (JDK) is used to implement java applets and command line development tool for applications, it includes the Java Runtime Environment (JRE).

J2ME Java 2 Micro Edition (J2ME) is a java based application development language for ubiquitous application platform for small wireless devices.

MA Merchant Agent (MA) is software which is running on the Merchant site; user interacts with MA to do Online Commerce.

MB Merchant Bank (MB) is the financial institution in which merchant has a valid account. MB is also responsible for merchant authentication.

MIDlet Mobile Information Device toolkit (MIDlet) is a Java based tool for small mobile device, it is a part of Java ME. Like other Java programs, MIDlets have a "compile once, run anywhere" facility.

MIDP Mobile Information Device Profile (MIDP) is a specification published by Sun Microsystem for Java enabled small mobile devices like cell phones and PDAs. MIDP is a part of Java Micro Edition framework.

OTP One Time Password (OTP) makes the system more secure over the static password. It is difficult break which protect unauthorized access to restricted resources, like a user confedential financial details. It reduce the risk by constantly altering the password, each parword is used only once.

PDA Personal digital assistants (PDAs) are small handheld device similar to computers, it is widely accespted as a personal organizer. PDAs are also known as pocket computers or palmtop computers.

PKI A public key infrastructure (PKI) is a technique used to bind public keys with user identities issued by certificate authority. The term PKI term is also used for cryptographic public key algorithms.

POS The Point of Sale / Point of Service (POS) term is used for electronic cash register system which is commonly used to make payments.

P2P The Point to Point (P2P) term is used in communication to establish a direct communication between two entities. It can connect two cell phones using Bluetooth to make payment.

RMS Record Management System (RMS) is used to implement persistence storage in J2ME MIDlets. It is record based persistence storage, J2ME RMS can support multiple record stores.

SATSA The Security and Trust Services API for J2ME (SATSA) is used to implement security features in J2ME based applications, it supports cryptographic APIs, user credential management and digital signature service.

SET The Secure Electronic Transaction (SET) is a standard protocol used to make secure electronic payment over internet. It is a card based payment system involving interaction among credit card holders, merchants, issuing banks, payment processing organizations and public-key certificate authorities.

SMS Short Message Service (SMS) is a protocol which supports wireless short messaging service.

TIC Transaction Identification Codes (TICs) are the pseudo randomly generated code which are uniquely assigned to the customers by their financial institution to perform online secure financial transactions. TIC is a one time code for each transaction.

WAP Wireless Application Protocol (WAP) is used in wireless communication, it is a defined as an international standard for wireless applications. Its purpose is to use internet on cell phones/PDAs.

WMA Wireless Messaging API (WMA) is a portable APIs in J2ME which provides facility to implement various resources of wireless communication such as Short Message Service (SMS). It is an optional package works with CLDC and MIDP.

WPP Wireless Payment Protocol (WPP) is a payment system used over the wireless medium or in M-Payment.

REFERENCES

Journals and Conference papers:

[1] Adi W., Mabrouk A., Al-Qayedi A., Zahro A. , "Combined Web/Mobile Authentication for Secure Web Access Control", In Wireless communications and Networking conference, IEEE Communications Society, Atlanta, GA USA, volume 2, pp. 677- 681, March 2004.

[2] J. Gao, J. Cai, K. Patel, and S. Shim , "Wireless Payment", In Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05), Xian, China, pp. 367-374, December 2005.

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

[4] Y.B. Lin, M.F. Chang, H. C.H. Rao, "Mobile Prepaid Phone Services", In IEEE Personal Communications, volume 7 Issue 3, pp. 6-14, June 2000.

[5] A. Fourati, H.K.B. Ayed, F. Kamoun, A. Benzekri, "A SET Based Approach to Secure the Payment", In Mobile Commerce, Proceedings of 27th Annual IEEE Conference on Local Computer Networks, Tampa, Florida, pp. 136 – 140, November 2002.

[6] Huang Z., Chen K., "Electronic Payment in Mobile Environment", In Proceedings of 13th International Workshop on Database and Expert Systems Applications (DEXA'02),University of Marseille, France, pp. 413 – 417, September 2002.

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

[8] V. Pasupathinathan, J. Pieprzyk, H. Wang and J.Y. Cho, "Formal Analysis of Card-based Payment Systems in Mobile devices" , In Fourth Australasian Information Security Workshop, Hobart, Australia, Conferences in Research and Practice in Information Technology, Volume 54, pp. 213-220, January 2006.

[9] Halevi Shai, Krawczyk Hugo**,** " Public-key cryptography and password protocols", In Proceedings of the 5th ACM conference on Computer and communications security, San Francisco, Volume 2 Issue 3, pp. 230 – 268, November 1998.

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

[11] Soriano M. and Ponce D., "A Security and Usability Proposal for Mobile Electronic Commerce", In IEEE Communication Magazines", Volume 40, Issue 8, pp. 62- 67, August 2002.

[12] Itani Wassim and Kayssi Ayman I., "J2ME End-to-End Security for M-Commerce", In Journal of Network and Computer Applications, Elsevier Ltd, Volume 27 Issue 1, pp. 13-32, January 2004.

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

[14] 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)

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

[16] J. Kelsey, B. Schneier, and N. Ferguson, "Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator", In Sixth Annual Workshop on Selected Areas in Cryptography, Kingston, Ontario, Canada, Springer Verlag, August 1999.
(Available at: http://www.windowsecurity.com/uplarticle/4/yarrow-full.pdf)

[17] Jerry Gao, Krishnaveni Edunuru, Jacky Cai, and Simon Shim, "P2P-Paid: A Peer-to-Peer Wireless Payment System", In Proceedings of the Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05), Munich, Germany, pp. 102-111, July 2005.

[18] 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.

White papers:

[19] White paper: AEP Smartgate Security, Strong Multi Factor User Authentication for secure information sharing, white paper, AEP Networks. http://www.aepnetworks.com/products/downloads/wp_SmartGateSecurity.pdf

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

[21] E. Limor, "Using Public Key Cryptography in Mobile Phones", white paper, VP Research, Discretix Technologies Ltd.,2002. http://www.discretix.com.

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

Websites and Articles:

[23] GSM calls even more secure - thanks to new A5/3 Algorithm" *ETSI*, 2002, http://www.gsmworld.com/news/press_2002/press_15.shtml; http://www.cellular.co.za.

[24] Website on bouncycastle package: http://www.bouncycastle.org

[25] Website on java code Java Obfuscator Java Obfuscation : http://www.retrologic.com

[26] Article on internet attacks: www.educause.edu/ir/library/pdf/CSD4433.pdf

[27] Article on attacks on mobile phones : http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci1232051,00.html

[28] Article on security threats of mobile phones : http://news.zdnet.com/2100-1009_22-5602919.html

[29] Website on java Servlet: http://java.sun.com/products/servlet

[30] Website on Wireless development tool kit 2.3 : http://java.sun.com/products/sjwtoolkit

[31] Website on Web Server: http://tomcat.apache.org/

[32] Website on Java database connectivity : http://java.sun.com/docs/books/tutorial/jdbc/overview/index.html

[33] Article on Oracle 9i with Jserver Facility :
http://www.oracle-base.com/articles/9i/Articles9i.php
http://www.smart-soft.co.uk/Oracle/oracle9i-new-features-part1.htm

Books:

[34] MasterCard Inc., "SET Secure Electronic Transaction Specification" , Book 1: Business Description, MasterCard Inc., May 1997.

[35] William Stallings "Cryptography and Network Security", Third edition, Pearson Education, 2003.

[36] Mitzenmacher M., Upfal E, "Probability and Computing: Randomized Algorithms and Probabilistic Analysis", Cambridge University Press, New York, NY, 2005.

[37] Motwani R., Raghavan P," Randomized Algorithms" , Cambridge University Press, New York., 1995.

[38] Vartan Proumian , "Wireless J2ME Platform Programming", Sun Micro system Press, Java Series, April 2002.

[39] Peeter Paal, "Java 2 Platform Micro Edition", Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2000.

[40] Mourad Debbabi, Mohamed Saleh, Chamseddine Talhi and Sami Zhioua, "Embedded Java Security Security for Mobile Devices", Chapter "Java ME-CLDC Security", Publisher Springer London, pp. 81-114, March 2007.

Survey and Thesis Reports:

[41] Jan Ondrus, "Mobile Payments: A Tool Kit For A Better Understanding Of The Market", Advisor: Prof. Yves Pigneur, Ecole des HEC, University of Lausanne, July 2003.

[42] Dr. Winston Seah, Santhosh Pilakkat, Jaya Shankar P., Seng Kee Tan, Chin Siang Kee, Anindita Guha Roy, Edwin Ng., "The Future Mobile Payments Infrastructure A Common Platform for Secure M-Payments", A Joint Study by Institute for Communications Research and Systems, December 2001.

[43] Teppo Halonen, "A System for Secure Mobile Payment Transactions**",** Supervisor: Professor Teemupekka Virtanen, Helsinki University of Technology, Department of Computer Science and Engineering, January 2002.

[44] Guidelines: "Guidance on Multi-factor Authentication", e-GIF Operations, State Services Commission, Wellington, Version 1.0, June 2006. (http://www.e.govt.nz)

[45] Guidelines : "Authentication in an Internet Banking Environment ", Federal Financial Institutions Examination Council, Arlington, (http://www.ffiec.gov)