Implementation Issues for Developing Credit Card Software for Mobile Phones

Sukhwant Kaur, Mritunjay Ojha, and Anand Pardeshi, *Member, IACSIT*

***Abstract*—Money Transaction has become common, frequent and a necessity in the current living and carrying cash always with a person is not a practical solution. The current trend of carrying the credit cards have become a crucial part of life and carrying of multiple cards is common nowadays. There is a risk involved when a credit card is stolen. Every one carries mobile phone. Our solution approach is to develop a system in which functions of the credit card is incorporated in mobile phone. The mobile phone is then used as a credit card and it replaces the function of swapping of the credit card each time we shop. Our system is having credit card application stored on mobile phone. This application has got all the information related to credit card operation, stored in encrypted form in the mobile phone. Further, this information is protected by a password. When a person desires to make any transaction through the mobile phone, the credit card data is passed from the mobile to the vendor machine through a Bluetooth communication interface [1]. The vendor machine validates the credit card data with the corresponding bank in standard fashion and issue the receipt [2]. Thus this eliminates the need for carrying credit card physically. This required modification on mobile software for safe storage of credit card information and few hardware modifications (add-on) to the vendor terminal for communication using Bluetooth. This paper focuses on various implementation issues of this application where mobile phone will act as a credit card.**

***Index Terms*—Mobile application, credit card, encryption, bluetooth, sim-Memory, PIN, IMEI, CVV, SMS**

I. Introduction

The current trend of carrying the credit card is increasingly becoming popular and is replacing cash transactions but this existing card system has many inherent issues. The credit card along with the PIN (Personal Identification Number) are delivered to the customer by the banks through couriers and during the process, there is a high chances of misusing the cards if it goes into wrong hands and the customer will not realize the theft till the card statement is delivered. The authentication used on credit cards is a signature panel or in some cases a photograph with signature panel which the vendors do not bother to see the photograph of the credit card Holder.

We have developed software on mobile phones that will eliminate the need of using credit card physically. The credit card [3] information such as type of card, name of cardholder, expiry date, credit card number, CVV (Card Verification Value) etc. which is there in magnetic stripe is stored in encrypted form in the mobile phone memory. The mobile phone then act as a credit card which holds multiple types of credit cards of the bank. The mobile-based system will facilitate any purchase made by the user. The transaction through mobile phone is passed to the vendor machine through the Bluetooth Communication Interface of the mobile phone. The vendor machine or point-of-sale terminal authenticates the credit card holder from the bank and generates the receipt of the transaction in standard fashion [4].

Manuscript received May 11, 2012; revised June 17, 2012.

Sukhwant Kaur is with Manipal University, Dubai Campus in the Department of Engineering (e-mail: sukhwantsagar@gmail.com).

Mritunjay Ojha is with Fr.C.Rodrigues Institute of Technology, Vashi, Navi Mumbai, 400703, in the Department of Computer Engineering (e-mail: mritunjayojha@rediffmail.com).

Anand Kumar Pardeshi is with Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, 400703, in the Department of Information Technology (e-mail: anandpardeshi23@gmail.com).

II. Implementation of Credit Card System on Mobile Phones

The application is installed in mobile phone. When the user runs this application, it asks for the password. After validating the password, it shows multiple cards, a particular user can choose. Then the user selects the proper credit card and enters the PIN for that particular card along with the amount. All these information is then sent to the vendor terminal using Bluetooth communication interface and then the receipt gets generated in standard fashion. This saves user for taking many credit cards in his wallet.

We have implemented the system in different modules as discussed below:

A. Transfer Module

The transfer module is responsible for putting data in mobile phones from the bank application. The information related to the credit card cannot be stored as raw data as it is very confidential data. Therefore, it is being encrypted first and then stored. Further, this application is protected by two passwords. First password is required for using the application itself that is, only authorized user of the credit card can use the application. Second password is required to view the credit card details. Further, the credit card details are stored as read-only data so that no user can modify it. In addition, the credit card details are stored in phone memory because sim-memory of the phone is limited to 32kb or 64kb, which is not enough for such kind of application and external memory is not suitable for storing the data as it can be stolen.

We have simulated a bank application using Java Swing [5] and backend is developed using MS-Access. The bank will take details like name, mobile number, IMEI (International Mobile Equipment Identity) number, address, type of card, etc. from the user and store it in bank application database.

DOI: 10.7763/IJIEE.2012.V2.215

The bank then transfers the encrypted form of data (card number, PIN, credit limit, expiry date etc.) to the users mobile through Bluetooth. The validations such as none of the text fields should be blank, mobile number should be of 11-digits, IMEI number should be a 16 digit unique number and credit card number should have only 16-digits etc are performed.

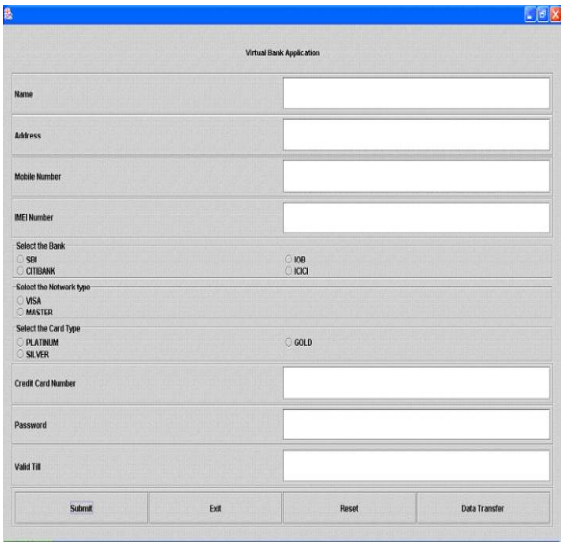

Fig. 1. Bank application

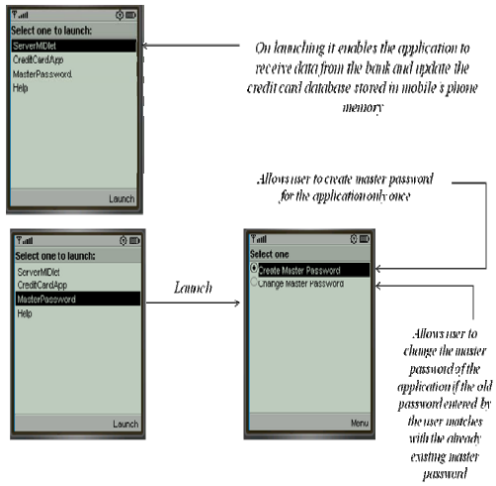

Fig. 2. The sequence of actions involved when user chooses "server MIDlet" or "master password" option

B. Transaction Module

The user enters the master pin to view the application and to view the number of cards he/she is carrying. If the password is authenticated the application will display the list of credit cards available to the user. The user then selects the card and enters the PIN for that particular card. If the PIN is validated then it displays the amount user wants to pay to the vendor. If the amount is less than the credit limit then the transaction will be done and data will be sent to Point-of-Sale terminal through Bluetooth.

C. GUI of the Bank

It allows the card issuer to enter the card details of the customer, store it in the bank's database at the click of Submit button, transfer data to customer's mobile via Bluetooth at the click of Data Transfer button, clear the text fields at the click of Reset button and close the application by clicking on Exit button.

D. Vendor's Application

It display's the data received from the customer's mobile through Bluetooth.

III. The Actual Working of the Application

The actual working snapshots are taken and are presented here. The forms that are displayed on the mobile's screen when user clicks on "Server MIDlet" and "Master Password" option is shown in Fig. 1.

When the user selects the CreditCardApp the application will ask the user for master password. The steps are shown in Fig. 2.

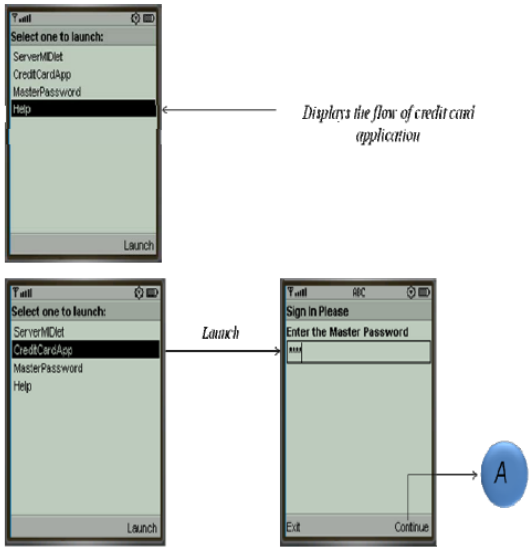

Fig. 3. The first form that occurs on choosing "Credit Card Application" option

When the user enters the master password, the application displays the list of credit cards the user is having and if it is incorrect, it will display that the master password is incorrect as shown in Fig. 3.

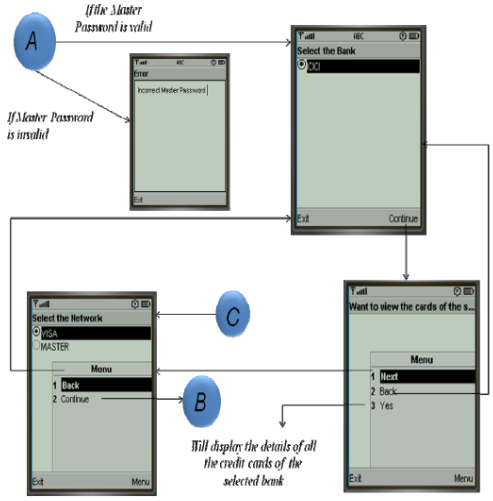

Fig. 4. The steps that occur after user enters the master password

If the master password is correct the user will get an option which will display the credit cards of various banks the user has. The user will than select a particular credit card and will

enter the Credit Card PIN of that particular card, this is done to increase the level of security for the credit card as shown in Fig. 4.

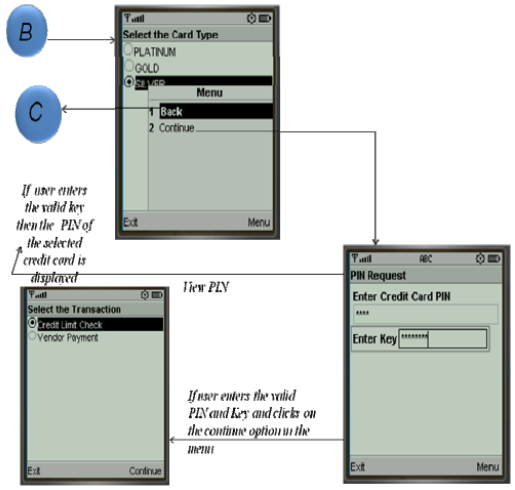

Fig. 5. Steps that take place after user enters the invalid PIN and key of the selected card

If the user wants to perform any transaction he can do so by selecting the vendor at the point-of-sale terminal and entering the desired amount for transaction if the credit limit is available the transaction is done successfully as shown in Fig. 5.

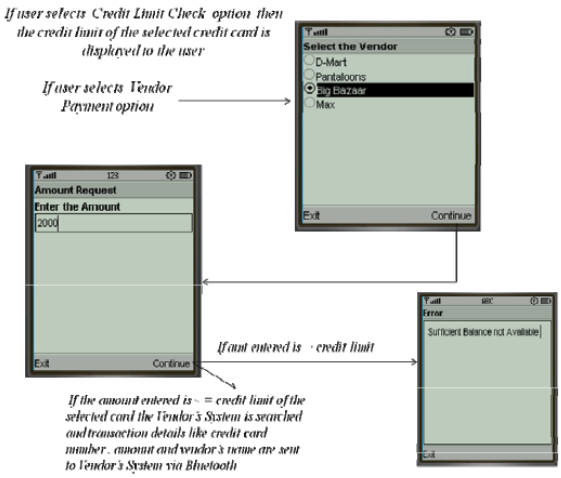

Fig. 6. Steps involved in performing the vendor payment transaction

IV. Implementation Issues

A. Encryption and Decryption in J2ME

J2ME [6] does not provide any API for security. We used API's provided by third parties like Bouncy Castle. Bouncy Castle is a collection of APIs used in cryptography. It includes APIs for both Java and C# programming languages. The low-level or 'light-weight' API is a vendor-specific set of APIs that implements all the underlying cryptographic algorithms. The intent is to use the low-level API in memory constrained devices (Java ME) or when easy access to the JCE libraries is not possible. The cldc_classes and cldc_crypto zips provided by Bouncy Castle needs to added in the library folder of the application using Bouncy Castle as the third party for encryption-decryption process. Any application that uses, such third party APIs should be build using high obfuscation [7].

But even after building the application under high obfuscation many a time following error occurs:

1) Error Preverifying Class

It gives verifier error as it sometimes fails to preverify certain class files present in the zips provided by Bouncy Castle.

2) Importing Packages

Many times it fails to import java.security and javax.crypto package and thus gives error for building, all the inbuilt classes of java.security and javax.crypto package used in the application.

3) Solution Approach

We have built the application successfully by not using the inbuilt classes in java.security and javax.crypto package for DES encryption, thus not importing the java.security and javax.crypto package.

Also we executed our program with the intent of finding errors. We executed our program by providing valid inputs and conditions to test whether it is producing the expected correct output. We also executed it by providing invalid inputs to check whether it displays the error message to the user as we have considered.

We applied the test cases to each module separately and to the entire application after integration of the modules to check whether it performs the desired function after interfacing.

V. Conclusion

The credit cards have become a necessity in everyone's life. People are highly possessive in holding multiple cards. The advantages of carrying credit cards are equally associated with the risk of being stolen and misused.

To mitigate the above problems we have successfully implemented a system in which credit card features are incorporated in mobile phones. This will eliminate the need of carrying the plastic cards.

Our application is more secure as it cannot be opened without the valid master password. The credit card's PIN information is stored in encrypted form. To view the PIN information the user has to enter the valid decryption key. If user desires to carry out any transaction he needs to enter the valid PIN and decryption key of the selected card. In case the mobile phone is lost the cards implemented in it can be blocked using the mobile phone's IMEI number.

Our software is of great advantage as it is more convenient to carry a single mobile phone with credit cards implemented in it as compared to carrying multiple cards with associated risks.

References

[1] Bluetooth technology, [Online]. Available: http://en.wikipedia.org/wiki/Bluetooth

[2] S. Kaur, H. K. Kaura, and M. Ojha, "Design Issues for Implementing Credit Card on Mobile Phones," *601-604 International Conference on Recent Trends in Business Administration and Information Processing*, 2010.

[3] Credit card, [Online]. Available: http://en.wikipedia.org/wiki/Credit_card

[4] A. H. A. Kwaja, "Proposal for an Open Minimal Standard-Processing, Financial Transactions using Mobile Phones," *Gelszus Banker Trendcheck*, 2002.
[5] H. Schildt, "*The Complete Reference - Java*," *Tata McGraw Hill*, Seventh Edition, 2007
[6] J. Keogh, "*The Complete Reference – J2ME*," *Tata McGraw Hill*, Edition 2003
[7] J2ME, [Online]. Available: http://www.articlesbase.com/software-arcticles/overview

Sukhwant Kaur is currently working with Manipal University, Dubai Campus in the Department of Engineering. She has done B.Tech (Computer Science and Engineering) in 1999 from Punjab Technical University. She has completed M.S. (SOFTWARE SYSTEMS) in 2001 from BITS, Pilani .

She has 12 years of teaching experience. She started her career as a Lecturer in Computer Engineering Department at Institute of Engineering, Bhaddal, Punjab, in the year 1999. Then she joined as a Lecturer in Fr. C. Rodrigues College of Engineering, Vashi, Navi Mumbai in the Department of Computer Engineering in the year 2001. She was promoted as the Assistant Professor in Computer Engineering Department in January 2008. She was the examiner of various subjects of engineering in Mumbai University.

Ms. Sukhwant Kaur Sagar published 20 research papers in International Journals and International and National Conferences. She is the life member of Indian Society of Technical Education (ISTE, New Delhi) and International Association of Computer Science and Informational Technology (IACSIT, Singapore). She is also the life member of Computer Society of India (CSI, India). She is a Program Committee member of the International Conference on Computational Intelligence and Communication Networks (CICN-2012), Gwalior, India and Communication Systems and Network Technology (CSNT-2012), Jammu, India. She is also a reviewer for CICN-2012.

Mritunjay Ojha is currently working with Fr. C. Rodrigues College of Engineering, Navi Mumbai in the Department of Computer Engineering. He has done B.E. (Information Technology) in 2008 from University of Mumbai and is currently pursuing M.E. (Information Technology) from Mumbai University.He has 3 years of teaching experience. He started his career as a Lecturer in Department of Information Technology at Fr. C. Rodrigues College of Engineering, Navi Mumbai and is currently pursuing Masters in Engineering at Vidayalankar Institute of Technology, Wadala, Mumbai. He is the examiner of various subjects of engineering in Mumbai University. Mr.Mritunjay Ojha published 4 research papers in International Journals and International and National Conferences. He is a member of International Association of Computer Science & Information Technology (IACSIT) Singapore .

Anandkumar Pardeshi is currently working with Fr. C. Rodrigues College of Engineering, Navi Mumbai in the Department of Information Technology. He has done B.E. (Information Technology) in 2007 from University of Mumbai and is currently pursuing M.E. (Information Technology) from Mumbai University. He has 3 years of teaching experience. He started his career as a Lecturer in Department of Information Technology at Fr. C. Rodrigues College of Engineering, Navi Mumbai and is pursuing Masters in Engineering at Vidayalankar Institute of Technology, Wadala, Mumbai. He is the examiner of various subjects of engineering in Mumbai University.

Mr. Anandkumar Pardeshi published 3 research papers in International and National Conferences. He is a member of International Association of Computer Science & Information Technology (IACSIT) Singapore.