Journal of Engineering Science and Technology
Vol. 10, No. 9 (2015) 1203 - 1214

SMART PHONE USER ASSISTANCE APPLICATION FOR ANDROID

P. PRABHAVATHY[1,*], S. BOSE[1], A. KANNAN[1], C. GOPINATH[2]

[1]College of Engineering, Guindy, Anna University, Chennai, Tamil Nadu, India
[2]Tagore Engineering College, Chennai, Tamil Nadu, India
*Corresponding Author: pprabhavathy@gmail.com

Abstract

Nowadays people seem to be more dependent on smart phones rather than any other electronic devices. Smart phones act like mini laptops with the mobile communication facility. Moreover, people possess more than one SIM card/Smart phone for many purposes. So non-ambiguity between various roles performed by them is crucial. For an example, person can have smart phone for his personal use at the residence and another phone for his official use. Consider a scenario: person at the residence urgently needs the official contact information available on the phone at his office (remote place). This application plays major dual role by acting as Server (official Smart phone) and Client (personal Smart phone). Irrespective of geographic area, the server smart phone (SSP) provides various services based on the request received from the client smart phone (CSP). The CSP send various requests through the SMS communication. Various requests can be fetching information from SSP such as log for unread messages and missed calls, unread message content, contact numbers, SIM and IMEI numbers. When the SSP is on silent mode and got misplaced, the CSP can be used to change the sound profile of SSP from silent to ringing mode by sending a request through SMS. If the SSP is in audible distance, then a phone call to it will help us to find the misplaced phone. Besides, the CSP can delete secret data available in the SSP's memory. This application is different from other applications because it provides User Interface having options to send request through SMS and web database login through internet connectivity for phone's data backup to provide unlimited memory. Upload any information such as contacts and messages from the smart phone into web database and save phone's memory space. This application will upload the information in encoded format over the internet, which can be decoded using the application's login password for security purpose.

Keywords: Android mobile OS, Remotely control smart phone, Phone's data web backup..

1. Introduction

In recent years, there has been an explosion in the Smart phone ownership. This is due to the fact that Smart phones can perform all operations that are possible with the Personal Computer. The mobile operating system (OS) used by modern smart phones include Android, BlackBerry, iOS and Symbian. These operating systems have differences in their features and performance. The Android Application Development is the choice for mobile application developers because of its essential features. The features are open source platform, networking technology support (Bluetooth, WIFI, EDGE, 3G) and Peer to Peer interaction.

Various sensory inputs of these smart devices are utilized for mobile application development to make human lifestyle as comfortable as possible. In this application, SMS Broadcast transceiver is used to send request to the smart phone placed at the remote place and receive response from it through the SMS communication channel. Besides it requires the internet connectivity for accessing backed up data of smart phone. The backed up data can be contacts or account information such as online banking User Id, password or any vital information. This content is encoded and stored in web database for security by this application. The one time installation of this application in the smart phone requires password for application login and genuine phone number for sending verification codes during password recovery.

Memory has to be consumed optimally in mobile devices. Hence this application provides an efficient way to store unlimited contacts into the web database, which can be retrieved to perform actions such as Make Call, Send message or save contact into the smart phone. These can be done if and only if the internet connection is available in it. Thus it differs from other applications in the mobile application market and acts as a best companion for Smart phone users. This application has explored the great flexibility and capability of Google's Android mobile phones.

The remainder of this paper is organized as follows: in the Section 2, existing methods are explained and compared with this android application. In Section 3, the functionality of this application is provided. In Section 4, the implementation details along with working application's screen shots are provided. Finally, this paper is concluded in the Section 5.

2. Comparison of Existing Works with this Application's Functionality

The smart phone usage among people is increasing rapidly. With the phenomenal growth of smart phone usage, the smart phone theft is also increasing. The paper [1] proposes a model to secure smart phones from the theft as well as provides some options to access a smart phone through other mobile phone through Short Message Service. According to the paper [2], the Smart phone contains some critical and sensitive data of user such as automated call records, photos, videos and saved passwords of his bank accounts. So losing the smart phone means a very high amount of irrecoverable data loss. Surveys about the mobile phone theft in USA, UK and India are discussed in [3-5] web pages. It reveals the need of an intelligent application to be run in smart phones.

Smart phone has evolved from simple voice terminal into the highly-capable and general-purpose computing platform. According to the paper [6], people are becoming increasingly dependent on devices to perform sensitive operations and protect secret data. Hence it is very clear that an application for smart phones is essential to protect them. Various research models for security aspects of mobile devices are an important research area and it is discussed in the papers [7-10].These models use SMS as the communication channel. According to the paper [12], data flowing through SMS can be encrypted and decrypted for confidentiality purpose.

In this paper, the android based mobile application provides the following services:

1) Request/Command framing service: CSP sends SMS in this pattern *<SecretCode><PassKey><ServiceType>* and deletes the message on dispatch to the SSP. Secret Code is the unique code used by this application to differentiate service request message from the normal message. Passkey is the password of the SSP's application, which is used for authentication purpose. ServiceType can be one of the following services: fetching of contact, missed call log, unread message, IMEI number, SIM number, deleting SSP's data or sound profile change. Hence it avoids unauthenticated CSPs requesting for services from the SSP.

2) Web database Login service: It helps to update and store unlimited contact information from this application enabled smart phone into the web database. A contact can be fetched from the web database to make call, send message or even save the contact into the smart phone's memory, where the web database login action has been performed.

Hence this application differs from others by providing an option to choose various services, where the service request message sent from CSP to SSP cannot be framed by any non-authenticated smart phone users. The Web database login is provided to store valuable information from the smart phone into the web for backup purpose since memory restriction is found in smart phones. Thus smart phones can be used efficiently as responsible devices with the help of this application which aims to save phone's memory space by adding huge list of contacts as well as bank account credentials into the web database in the encrypted form.

2.1. Client smart phone application functionality

This application acts as User's Smart Phone Assistance application when it is installed and configured in the smart phone. The one time configuration process stores the application's login password and genuine phone number in the phone's database. After successful login into the application, it provides an option for sending the service request to SSP or web database login for backup of CSP's data. It is depicted in Fig. A-1 (Appendix A).

2.2. Server smart phone application functionality

It receives the service request message from CSP and acts based on the **ServiceType** mentioned in it. This application ensures the user permission for erasing data from the phone's database. The service request/command pattern *<SecretCode> <PassKey> <ServiceType>* involves **PassKey** for authentication and **SecretCode** for authorization purposes. It is depicted in Fig. A-2.

3. An Android Application: Service Request/Command and Web Database Storage

Various services are provided by this application using service request message from CSP to SSP and Web database storage. Figure B-1 (Appendix B) shows the screenshot for service request and web database login.

3.1. Command/Service request through SMS

Eight number of service requests are available in Command through SMS. They are defined below:

Fetch Contact: This service request for fetching contact numbers with the specified contact name in the SSP through SMS.

Example: <SecretCode> <PassKey> contft <contact name>

Fetch Missed Call Log: It requests for retrieving missed call log from the SSP.

Example: <SecretCode> <PassKey> miscal

Unread Message Log: It requests for retrieving unread message log from the SSP.

Example: <SecretCode> <PassKey> msglog

Get Unread Message: It requests for fetching inbox's new message which has not been read in the SSP.

Example: <SecretCode> <PassKey> getmsg <contact number>

Change Sound Profile: Sound profile can be Normal, Silent or Vibration. It requests to change the SSP's sound profile to anyone of these three modes.

Example: <SecretCode> <PassKey> pfchng <normal/silent/vibrate>

Delete Memory: It requests to delete data from the SSP's database in case of theft. Critical data has to be fetched from the SSP's database, so that it can be deleted from the SSP's memory for security purpose. Such data for deletion can be: Specific Contact, All Contacts, Inbox Messages, Sent Messages, Draft Messages or Message of a specific contact number from inbox, sent folder and draft folder.

Example :<SecretCode><PassKey>delmem<all/name/msgof/inbox/ sent/draft>

Fetch Subscriber Identity Module (SIM) Number: It requests for retrieving SIM number of the SSP.

Example: <SecretCode> <PassKey> simnum

Fetch International Mobile Station Equipment Identity (IMEI) Number: It requests for retrieving IMEI number from the SSP.

Example: <SecretCode> <PassKey> imeino

3.2. Web database storage

Internet connection in the smart phone is a must for this feature to work.

Web Database Login: The web database facility is provided in this application to avoid the SMS communication cost, so that user can make use of free Wi-Fi

Hotspots for the Internet connectivity. After successful login, it provides an option for downloading or uploading of the smart phone's data. The web database login credentials are User's Smart Phone SIM number and this application's password. The data can be contact number, SMS message or any information such as bank account credentials.

Contact number storage: Unlimited Contact numbers can be uploaded into web database to save phone's memory. Upon downloading Contact number, it can be used to make call or send message directly without saving contact information in phone's memory. If necessary then particular contact number can be added to contact list of user's smart phone.

SMS Message storage: The important message in inbox or sent folder can be uploaded into the web database to save the phone's memory. Since messages occupy more memory, this application helps us to save the phone's memory by uploading all messages into the web database in a secured manner by encoding information.

Critical Information storage: Important information can be uploaded in the encoded format to provide security. To decode the information, application's password and decoding method have been used by this application. When the user uploads any information, it is available online for downloading at anytime and anywhere using this application. The downloaded information will be decoded first and then represented to the user.

3.3. Android Application's functionality-Server Smart Phone (SSP)

This application retrieves information about missed calls such as contact number, name, time of call along with number of missed calls found since last viewed from the SSP. If more than 2 calls are found in the SSP's log then it sends the information in subsequent messages.

The SSP can send the new inbox message log information such as sender contact number, name, and its arrival time. If more than 2 messages are found in the log then it sends that information in subsequent messages to the CSP. It can delete data in its database on the basis of service request/command received from the CSP through SMS. The SSP can retrieve SIM as well as IMEI number from its database and sends it as SMS to the CSP (service requested from user's phone).

This is the part of this application which has been developed to assist the user for feasible usage. Here the service request/command will be formatted automatically after getting the required input parameters from the user for sending command to the SSP.

4. Implementation and Results

This Android based application uses traditional MVC (Model view control) architecture for its implementation. Data access and design view are the two different modules where an xml file is used for layout purpose and Activity is used for performing action using that layout.

There are four packages available in this application where one is the main package and other three are the sub-packages of this application. The sub-packages are Configuration Activity, Login Activity and Forgot password Activity.

4.1. Configuration activity

This activity is responsible for configuring the application for its first use in the smart phone after which it won't provide any option to reconfigure it. In this activity, it asks for a password which will be used for accessing various services of this application. If this application's password has been forgotten, then forgot password option can be clicked to get the secure code for resetting the password. Secure code is like one time password (OTP) sent by this application to the genuine mobile number provided during the configuration activity. This application verifies the entered code by the user with the secure code sent by it to the genuine mobile number which has been mentioned during configuration. Configuration and Installation are shown in Fig. 1.

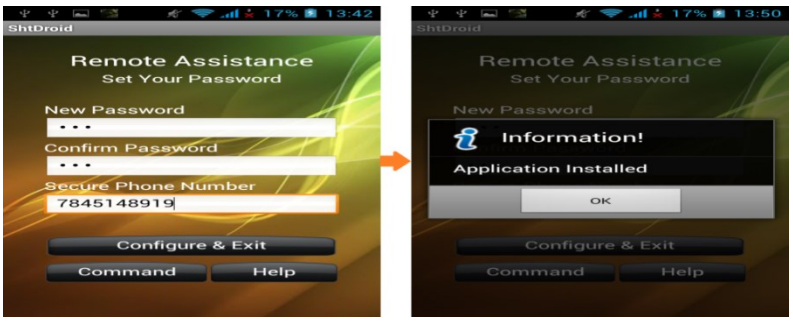

Fig. 1. This application's installation and configuration in smart phone.

4.2. Login activity

This activity is responsible for login into the application's home page. Here the application asks for its password which has been set by the user at the configuration time. If the user entered password matches with the application's stored password, then it will redirect to its home page which has the following features (refer to Fig. 2):

1) Change password and authorized/genuine mobile number.
2) Login or signup to web database.
3) Stop the application from running mode.
4) Send service request/command through SMS upon a single button click.

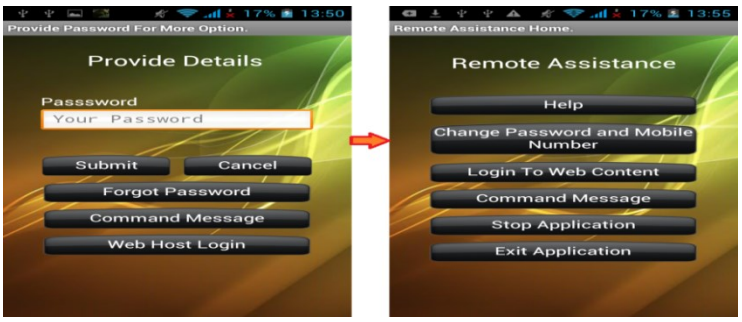

Fig. 2. Application's home page upon successful login.

4.3. Forgot password activity

This activity is responsible for resetting the application's password. Once "Forgot password" option has been selected it will send a secure code like OTP to the registered mobile number. If the user enters the secure code, then it will redirect to reset application's password page. It is shown in Figs. 3(a) and 3(b).

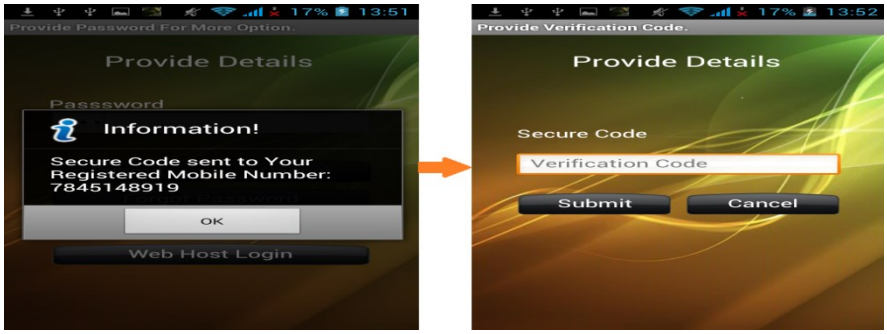

Fig. 3(a). Forgot password page of this application.

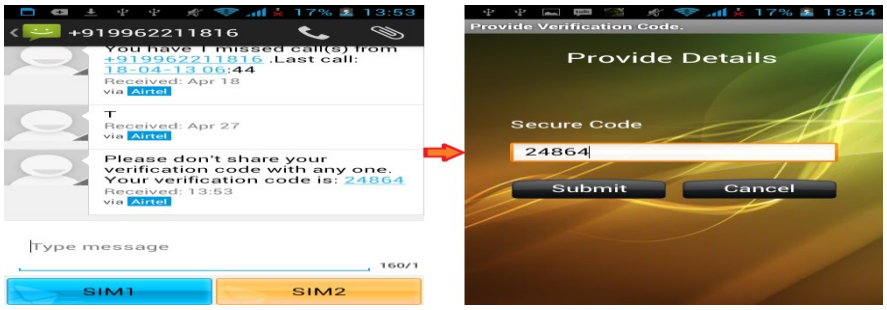

Fig. 3(b). Secure code received in registered mobile number and verification page of this application.

4.4. Send service Request/Command through SMS

This is responsible for sending command pattern message to the SSP for accessing various services. It is shown in Fig. 4(a). A sample screenshot to delete a particular contact number from the SSP is depicted in Fig. 4(b).

Fig. 4(a). Each button on click will send a service request to the SSP.

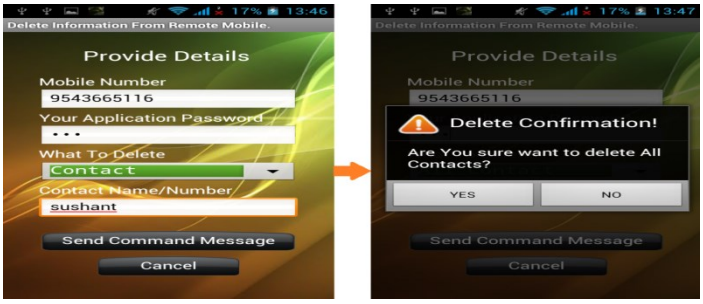

Fig. 4(b). Delete service request/command asks for confirmation.

4.5. Login into web database

User has to provide the credentials such as CSP's phone number and application's password for web database login. After successful login, it provides an option for the download or upload of data. It is shown in Fig. 5(a).

The download/upload has the following options: contact, message, and information. User can store contact numbers, Credential information of user accounts as well as SMS messages from user's phone into the web database to save its memory. Contact name provided by the user is fetched from the web database as shown in Fig. 5(b) and various actions can be performed using the fetched contact number in this application.

Three actions are possible with that contact. They are Call to that phone number, message to that number or save that contact number to this application's smart phone upon selecting that contact, which is shown in Fig. 5(c).

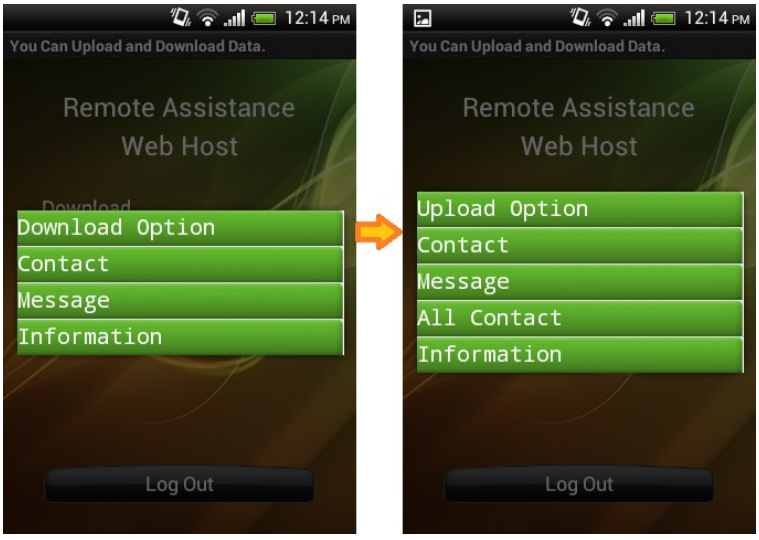

Fig. 5(a). Login page into web database of this application.

Fig. 5(b). Downloading the contact information whose name starts with an alphabet 's'.

Fig. 5(c). Application's page showing Downloaded contact and its various actions using that contact information.

5. Conclusions

Hence this Android based application performs various services on smart phones irrespective of their geographic area using SMS and web connectivity as a communication media. It provides an interface to send service request/command message to the Server Smart Phone (SSP) which has to be controlled remotely. These command messages activates various services such as fetching contacts, missed calls, SIM number, IMEI number and unread messages along with changing sound profile of the smart phone (SSP).

It also supports Web database facilities such as uploading/downloading our important contact, message or information over the web. After downloading contact information, it can call, message or save that contact to its phone (CSP). Hence it saves phone's memory by accommodating unlimited contacts and messages into the web database. All information uploaded into the web database will be in encoded format for security purposes.

Some features of this application which makes it different from others are:

- User need not type to frame the service request/command pattern for sending it to the SSP. This application does all these tasks internally based on a single click from the user. Hence it provides user flexibility.
- It deletes the sent command SMS message automatically from the CSP to save the phone's memory.
- It provides the web database storage for uploading unlimited contact details as well as SMS messages. This feature saves the phone's memory space.

- Any critical information such as bank account credentials can be uploaded into the web database. These will be uploaded in an encoded form into the web database for security.

References

1. Kuppusamy, K.S. (2012). A model for remote access and protection of smart phones using SMS. *International Journal of Computer Science, Engineering and Information Technology,* 2(1), 91-100.
2. Hossein, F. (2010). Diversity in smart phone usage. *Proceedings of the 8th international conference on MobiSys,* 179-194, San Francisco, California, USA.
3. BBC NEWS, UK. (2002). Survey about mobile theft in UK. Retrieved September 3, 2014, from http://news.bbc.co.uk/2/hi/uk_news/1748258.stm
4. Consumer Reports, USA. (May 28, 2014). Smart phone thefts rose to 3.1 million last year, Consumer Reports finds. Retrieved September 3rd 2014, from http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm
5. InformationWeek News Network, India (2011). 53 percent of Indian mobile phone users are victims of mobile theft. Retrieved September 3rd 2014, from http://www.informationweek.in/informationweek/news-analysis/176773/percent-indian-mobile-phone-users-victims-mobile-theft?utm_source=referrence_article
6. Patrick, T.; and Chaitrali, A. (2011). From mobile phones to responsible devices. *Security and Communication Networks*, 4(6), 719-726.
7. Karsten, S.; and Tanveer Mustafa. (2011). Software security aspects of Java-based mobile phones. *Proceedings of the ACM Symposium on Applied Computing*, 1494-1501, New York, USA.
8. Enck, W. (2009).Understanding Android Security. *IEEE Security and Privacy,* 7(1),50–57.
9. McGraw, G. (2006). Software Security: Building Security In. *Book Publisher Addison-Wesley Professional,* 448 pages, First Edition.
10. Bo Li; and Eul Gyu Im. (2011). Smart phone, promising battlefield for hackers. *Journal of Security Engineering,* 8(1), 89-110.
11. Kyungwhan Park; and Gun II Ma. Smart phone Remote Lock an the Wipe System with Integrity Checking of SMS Notification. *IEEE International Conference on Consumer Electronics ,* 263-264, Las Vegas, Nevada.
12. Adrienne, P.F. (2011). Android permissions demystified. *Proceedings of the 18th ACM conference on Computer and communications security*, 627-638, New York, USA.

Appendix A

Representation of this Application's functionality performing the dual role in Client Smart phone (CSP) and Server Smart phone (SSP)

The following figure shows this android application's functionality in the Client Smart phone (CSP).

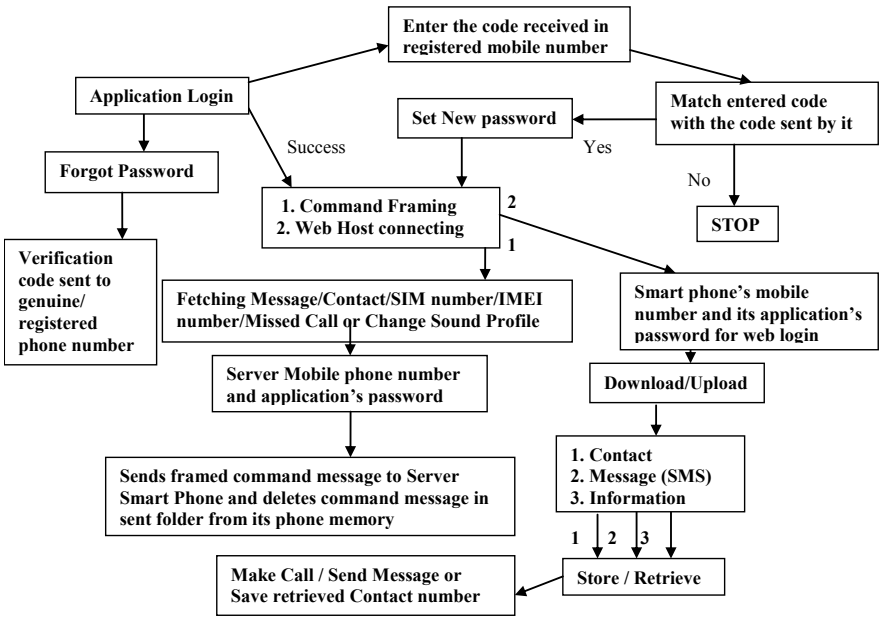

Fig. A-1. Application's functionality performed in client smart phone.

The following figure shows this android application's functionality in the Server Smart phone (SSP)

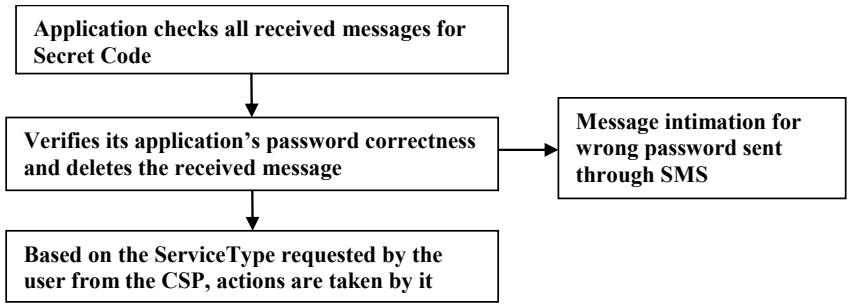

Fig. A-2. Application's functionality performed in server smart phone.

Appendix B

The overview of its dual functionality is shown in the following figure.

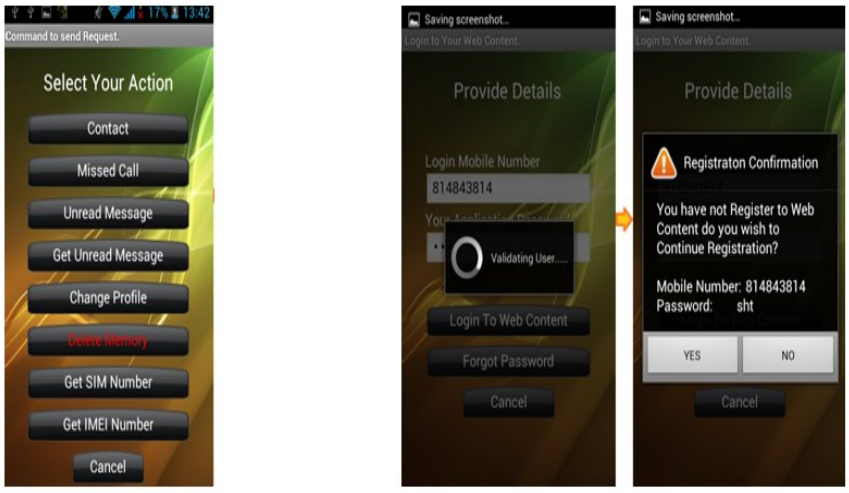

Fig. B-1. Service Request/Command screen and web database Login/Register screen.