Design and Implementation of Third Party Mobile Phone Backup System for Ethiopia

Mekonnen Mulugeta
Department ICT, Entoto TVET College, Addis Ababa, Ethiopia
mekobrat@gmail.com

Tibebe Beshah
School of Information Science, Addis Ababa University, Ethiopia
tibebe.beshah@gmail.com

Abstract

Losing a mobile phone has many related problems than the lost hardware itself. Mobile phone users are complaining about their contacts than the lost device. In addition to data lost, mobile phone users need additional storage than they have. The main objective of this paper is to design an application in order to store phone contacts in some other place than the phone memory or SIM card, so that users can access it whenever they want. Hence, mobile phone users will have an option to backup their contacts on a server that is placed for this purpose. Qualitative research approach along with standard software engineering process is employed in this research work. The solution discussed in this paper tells how the solution is designed, work and what makes it different from other existing solutions. Backing up contacts can be to put contact in safe place in case a mobile phone is lost or to use the advantage of additional storage. The application has options for users either to backup all at a time, or to select and backup or to write and backup. This application is different from the others because it is a GSM application instead of GPRS. This means the user need not have Internet access on the mobile phone to use the application. Test and evaluation of the prototype justified the relevance of the system.

Keywords: Mobile Phone Backup System; Architecture; Third Party

1. Introduction

A mobile phone, which is also known as cell phone, is a device that is used to communicate wirelessly using radio wave or satellite transmission. A mobile phone can be used for voice communication and also for short message service and multimedia message services [14]. It has also become a common practice to access the Internet through our mobile phones.

Cell phone technology is based on radio technology that was developed in the 1940s and onwards. For instance, the beginning of cell phones can be traced to the innovation in taxi cabs, police cars, and other service vehicles where two way radios allowed taxi drivers or police officers to communicate with one another or with a central base.

Ethiopian Telecommunication Corporation (now ethio telecom) was the only responsible organization for telecommunication services in Ethiopia in the past several years. Mobile phones are also brought to usage by ETC in 1999 [1]. Since then, there are tremendous changes on the usage of mobile phone. At the starting time, ETC was the only one to deliver a SIM card and the handset with postpaid system, which discouraged most of the community, who are not sure whether they can pay or not [1]. After some years, ETC started a prepaid system which encourages most of the community to use mobile communication. Currently, there are around 20 million mobile phone users in Ethiopia [1].

Mobile phones are used for different purposes, in addition to communication [7]. Mobile phones are also used to store contacts and short text messages either on the mobile phone itself or on the SIM card.

With the increase in usage, lots of problems related to mobile phone have been identified through researches. To mention some, health problems, data loss problems, technology adaptation problems, and others. This paper tries to address the data loss problem [17]. Mobile users lose their mobile phones in different situations. Losing a mobile phone is not losing the hardware only, but lots of data like user contacts, short messages or other key numbers which are saved on the phone.

Losing lots of "small sized" but "essential" data continues as the loss of the mobile phone is not stopped. It is evident that different telecommunication companies are trying to provide mechanisms for the user on how to trace lost phones, if they are with some one's hand [16]. But mobile phones are not always stolen. There are different cases to lose mobile phones such as through damage.

The purpose of this paper is to design and implement a mobile buckup system. As mentioned previously, losing data from a mobile phone is a big problem for cell phone users. In this research, attempt is made to address the problem by designing a suitable mobile application for backing up mobile data.

Backing up mobile data is not only reasoned because users may loose their phone, but also due to other reasons. Among the reasons, the user may need additional space on his/her mobile phone by moving contacts, incase if the memory is full and does not allow him/her to save extra. In this case, the user may move all contacts and make free the mobile's memory, so that memory will be used for additional purposes. As a second reason, sometimes a mobile user may be forced to pass his/her phone to some other user due to different reasons. This time, if the user feels unsecured to give the phone with all data on the phone, the user can send data to the server and free his/her mobile.

The reasons listed above can be applied in different ways at the interest of the phone user. In general, backup in this paper is about using extra storage which is located on the server other than the phone's memory that can enable the user to save his/her data for different purposes.

Mobile backup system is a way of sending or retrieving data (text), especially to some storage area. According to information obtained from ethio telecom, there is no application/service which is currently available in our country by the service provider.

2. Literature Review and Related Work

Frencel *et al.* [12] describes an architecture for mobile backup. Mobile device backup and accessing through a website is possible but not available all the time, for example while driving. There are also cases in which the user can't get Internet access in order to access a website. The authors showed how the architecture is implemented. Accordingly, a request to access a service is received from a client running on the mobile telecommunication device via a mobile telecommunication network. Communication with the backup application is performed on behalf of the client. The system exchanges security question with the client to authenticate a user of the mobile. In this study, the telecommunication device is mobile or any device that is configured to communicate via a mobile telecommunication network. Mobile gateway facilitates communication between the client on the mobile telecommunication device and the backup application. This mobile gateway transforms information exchange between the client on the mobile telecommunication device and the backup application. Mobile gateway is used to compress the message between the backup application and the mobile device to reduce transmission bandwidth.

In [13], Mobile Solution Platform (MSP) architecture and server are described. The MSP provides backup and synchronization services to a wide variety of mobile handsets. In addition to supporting a wide variety of mobile handsets, the MSP architecture and server provide support for a wide variety of data types like contact information. This architecture has device dependent configuration which is set on the server's table which is device catalog. In addition to synchronizing data with end user device, it enables easy and quick data importing and synchronizing to other data services, like Yahoo address book.

Figure 1 [12] shows that the backup system is architecture based on GPRS requirement. The signal transceiver communicates with the mobile gateway through HTTP signal. It is intended to solve the problem that arises due to web access through mobile phone, but the backup architecture still uses the Internet on the mobile phone, by reducing the previous system which must open a web to backup contacts.

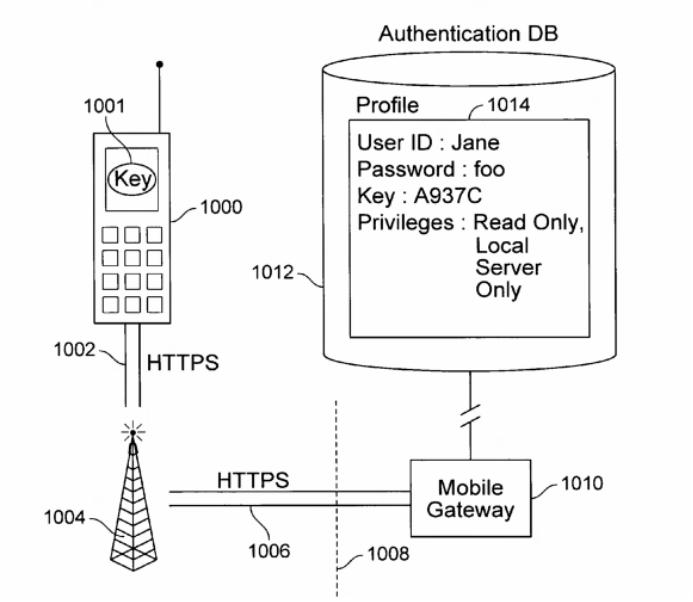

Figure 1: Some part of the architecture

Figure 2 [13] shows another architecture which aims to backup from different mobile devices and has better functionalities. But still it is a must to have Internet connection to do the intended activity. It specifies that the user even can synchronize his/her phone data with Yahoo address book, which is GPRS requesting activity.

In addition to those architectures, we also reviewed other applications working on such activity. Rseven [8], SmartFuzz [18], Gizmod [4], and Orange contacts backup [5] are some of them. These systems work on a website using the WWW. To backup on these websites, the user needs to open and register. They use databases for storing data. Operating systems like Android and Windows also enable their mobile users to take backup [2, 3, 6].

As it is explained in [12], a method or computer program for backing up data from a wireless device on to a server via a network is possible. The backup process is initiated by pushing the request to the server and the client transmits data to be backed up to the backup server. The backup server then receives the data from the wireless device and stores the data for later retrieval if the wireless device loses its data. However, as the authors described, it is not the best model for small, low-power computers like the palm VII organizer with its tiny screen, battery powered operation, and relatively slow and expensive wireless connection to the Internet.

Another work [13] shows that mobile device data is possibly backed up in a storage placed for that purpose. In this system, as the architecture shows, the first activity is to check whether the mobile device is seeking to backup information. Then the mobile device is checked if it is a trusted device and the amount of storage space which is available is checked for that specific legal mobile device. The process continues by notifying the device to send data to be backed up and then the sent data will be backed up by the partner device, which is responsible to tell centralized server.

The above two works have their own limitations. The first one is not good enough for small devices due to battery usage and speed [10]. It is also stated that it is expensive. The second work's limitation is it needs mediatory wireless device than the BTS signal transceiver [11]. The existence of another party on the backing up process increases user's expense as well as it will raise a question on the speed of the process.

A work on "data backup for mobile computing devices" [26], shows that, backing up data from small devices like PDAs, mobile handsets, and palmtops, is possible through GPRS. The work shows that data can be kept on a data server per the backup schedule that the phone or the device has. Authentication is done by an authentication server, which delays the communication process.

Another work on in [21] is aimed at providing a solution for managing backups between mobile stations, and especially a solution that is able to take backups from both the SIM card and the mobile terminal vendors independently. According to the work, the backup process is not only from SIM card, instead it is also from the terminal that has the first backup.

As shown in [20], there is a device which is used to take backup of a SIM card. This device works using a cell battery and it is password protected. A SIM card is inserted into the device and the backup takes place. This device keeps the backed up data and the user can use the data any time. The device is on use in different countries including Kenya, India, and Honk Kong. This device shows the need of SIM backup. The device has its own disadvantages like

the user must switch off his/her mobile to take backup and this process will continue every time when the user has something new on his/her SIM card, so that it will be somehow a difficult task. In addition to this, the user has to be with the device in order to take backup (physical connection is a must), which makes the user not to be comfortable of taking backup from anywhere at any time. The other disadvantage is the SIM backup, which is just like other devices and it may be lost. This leads to go on to other solutions than using the device for SIM backup purpose.

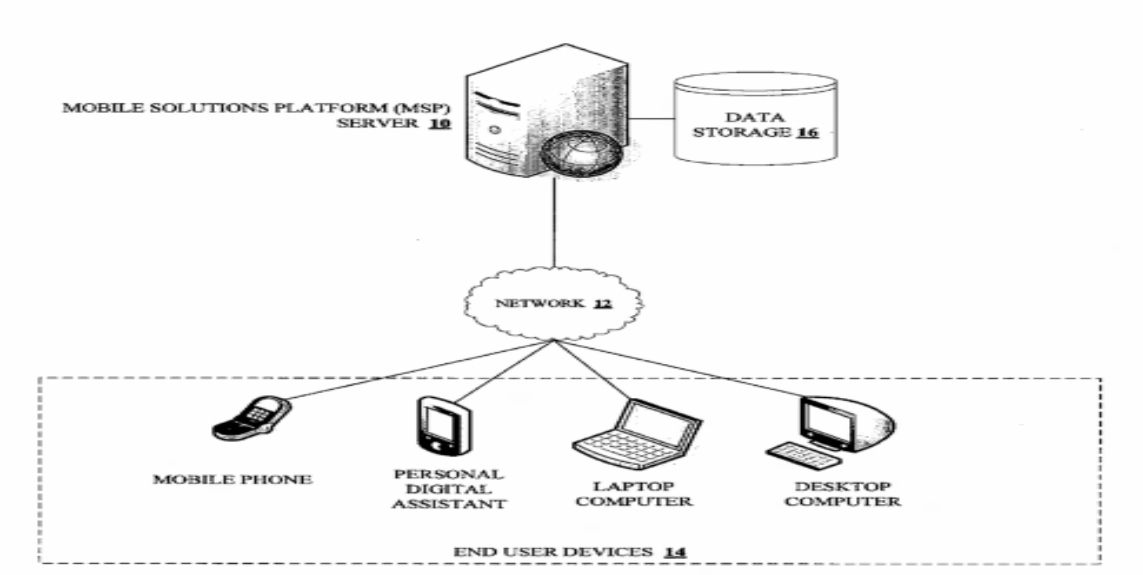

Figure 2: Mobile solution platform architecture

From a survey of literature made so far, the architecture to be proposed through this research will have an additional contribution to the domain of mobile backup systems. It is to mean that the system is expected to work without the need of GPRS, which is the basic requirement in most cases, so that the service will be available for most phone users. This is basically an applied research that solves a practical problem in low income countries like Ethiopia.

According to the reviews made, there are architectures which designed to work without the need of GPRS, but such systems are available only locally in their respective context with the help of the service provider. This leads us to design and implement an architecture which is GPRS independent and suitable for our context, so that it can work in our country with the help of the service provider. This is all about designing a system which is compatible for our country (Ethiopia) to backup mobile phones' data through a network that doesn't need GPRS.

Even if mobile data backup system is not designed in our country, there is some architecture defined on it in different countries. As we reviewed most of them, the backup system has direct relation with the GPRS, which enables mobile phone users to have Internet access. Using the Internet access has some disadvantages, especially in our country. The first is its cost and the second is mobile phone users may not have Internet access in their mobile and the other problem is even if a mobile user has Internet access, due to several reasons, it may not be satisfactory and confident to transfer such data any time.

Taking such things into consideration, we tried to develop a prototype that enables all mobile phone users to communicate with a server to store their contacts. The new thing in this work is to enable mobile phone users to backup their data on a server which is kept somewhere so that they can take it back whenever they need it and the application doesn't need Internet connection on the user's phone.

In addition, using GSM data transfer for backup is advantageous on battery usage. Since we are working on mobile phone, battery usage is an issue. In the works reviewed, all use GPRS for data transmission. But, using GPRS wastes more battery than GSM data transfer [9, 19].

3. The Proposed Solution

Qualitative research approach is employed to identify the existence of the problem in Ethiopia. Accordingly, it has been found out that the problem exists and needs solution.

The general architecture of the system is designed to show how the activity takes place from the beginning to the end of the connection establishment and data flow. The architecture uses a server which communicates with the mobile device through a transceiver.

Accordingly, as shown in Figure 3, the system works through the communication of 3 devices: mobile phone, server, and transceiver. Since backup is done through a request to the server, there must be connection between the server and the mobile device. This is possible through the BTS signal generator, which is a transceiver.

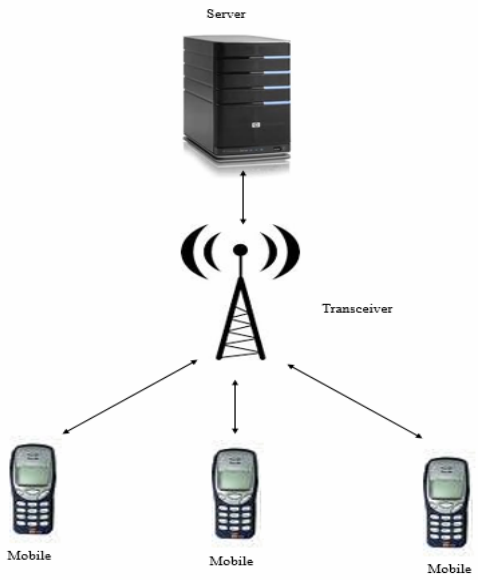

Figure 3: General architecture of the system

The system is 2-tier architecture in which the client requests to establish a connection with the server. The communication continues after the server authenticates the client.

As shown in Figure 4, a mobile phone user has 3 options to save contact and other data. The first two options are SIM and phone memory. These saving options need nothing but only the phone itself. According to the solution designed in this work, there is another option for the phone user to save contact and other data. This option has no physical contacts with the phone and all is done through the use of radio wave, unlike the first two options. As it is shown on the figure, the third option is done by communicating with the application server through the use of radio wave; basically there is a BTS transceiver. The process is done through GSM, no GPRS. The arrow between "contact + data" and "Radio wave" shows that there is a two way communication. The first is request. The first security shows the transmission is secured on the client side. This means, the user is not allowed to enter his/her number or user name. The application is responsible to take the user name which is the phone number from the SSID of the SIM card. This has its own protection for the phone user (discussed later). In addition to that the security information is also seen here. Security related information, "Password" and "Keyword", which are used for another time retrieval are located on the first "security" part. The application server sends the application according to the user's request. The application that is designed through J2ME is sent when the user makes a request. Information that needs more security is expected to be secured well during the process. "Security" after application server shows those security issues. In this case hashing is preferred due to its strength. Password and keyword are among those that are hashed. "Data store" is the place where information is kept.

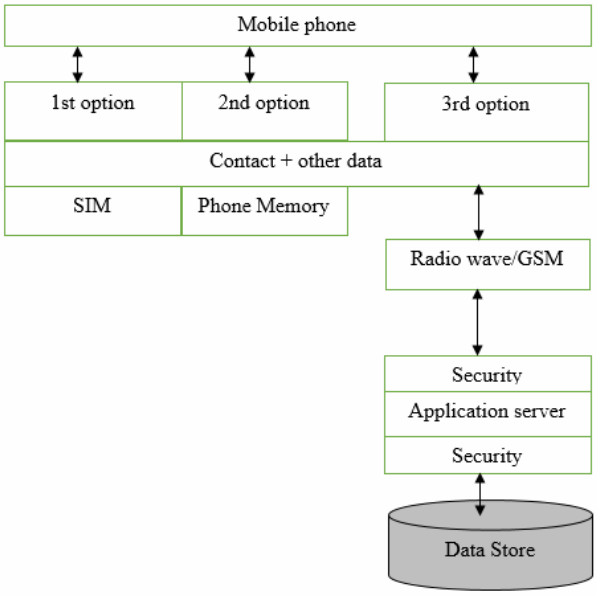

Figure 4: Block diagram of the application

The first option for phone users is to save their contact on a SIM card. SIM card is located within the phone itself so they are attached physically. If we see the third option, the user sends request and the request goes to the application server through the help of radio wave, generated by the BTS signal transceiver. This process has no physical relation and is represented through an arrow.

Connection is established in either when the user requests for the first time or when the user needs to use the application. As the order of the architecture, the first connection is done by the method in which it is sated. It can be by sending a number like *804#. This connection creation is used to send the application for the phone user. Connection is created successfully means that the user is registered and has the application on his/her phone.

As shown in Figure 5, the request is initiated by the user and uses the BTS signal transceiver to communicate with the application server in control of the service provider. The line shows two way communications, means, the user sends a request and the server sends back the application.

The diagrammatic representation of the application (Figure 6) shows how the request is sent from the mobile phone to the server through a signal transceiver called BTS and reached to the server so that the application is sent back to the mobile phone. The request is just like requesting for other services like *804#. The transceiver is the one that is responsible for taking the request to the server. The server has different applications and responses which are distinguished with different requesting numbers. According to the request number sent to the server, the server is the one to decide which application is needed by the phone user. In our case, when the phone user sends a request, the server selects the client code (J2ME code) which is designed for backing up operation and sends it to the phone of the requester. When the phone user gets the application, s/he uses it to register as first time application user. It means that the users has an application for backup and retrieve system.

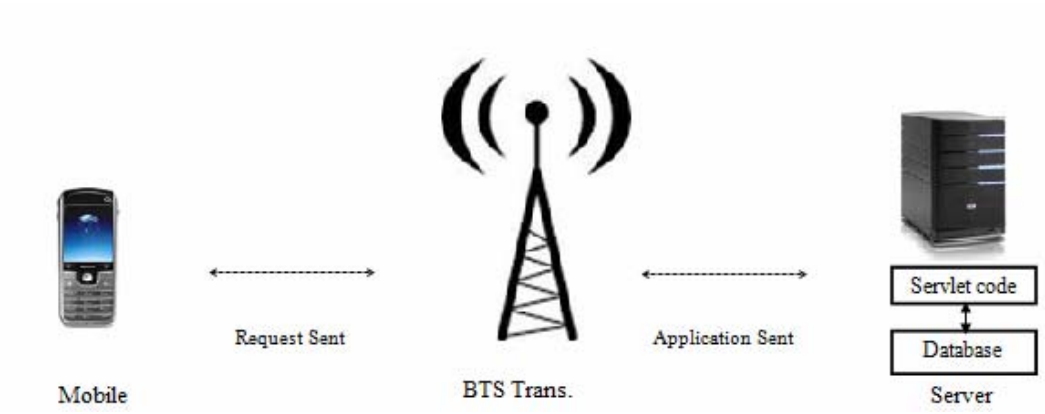

Figure 5: How a request is send and return back

Figure 6B shows the process after the phone user received the application from the server. This time the user can use the application either to send his/her contacts and other text to the server or to retrieve the data which is kept on the server. In this case when the user selects one of the applications on the application menu, connection is established between the phone and the server. The J2ME code directly calls the IP address of the J2EE application which is kept on the server. The server is tomcat server in this case. Servlet code on the server helps the connection requested to communicate with the database which is also kept on the server machine. Mobile application code uses servlet as an interface to communicate with the database which is kept remotely.

4. Description of the Prototype

This system is designed to send contacts and text from the user's phone to the server which is kept somewhere. This application starts by registering a user requesting for the service. Once the user registers, s/he uses the application to backup his/her contacts. Sending contact or text needs the user to be registered only.

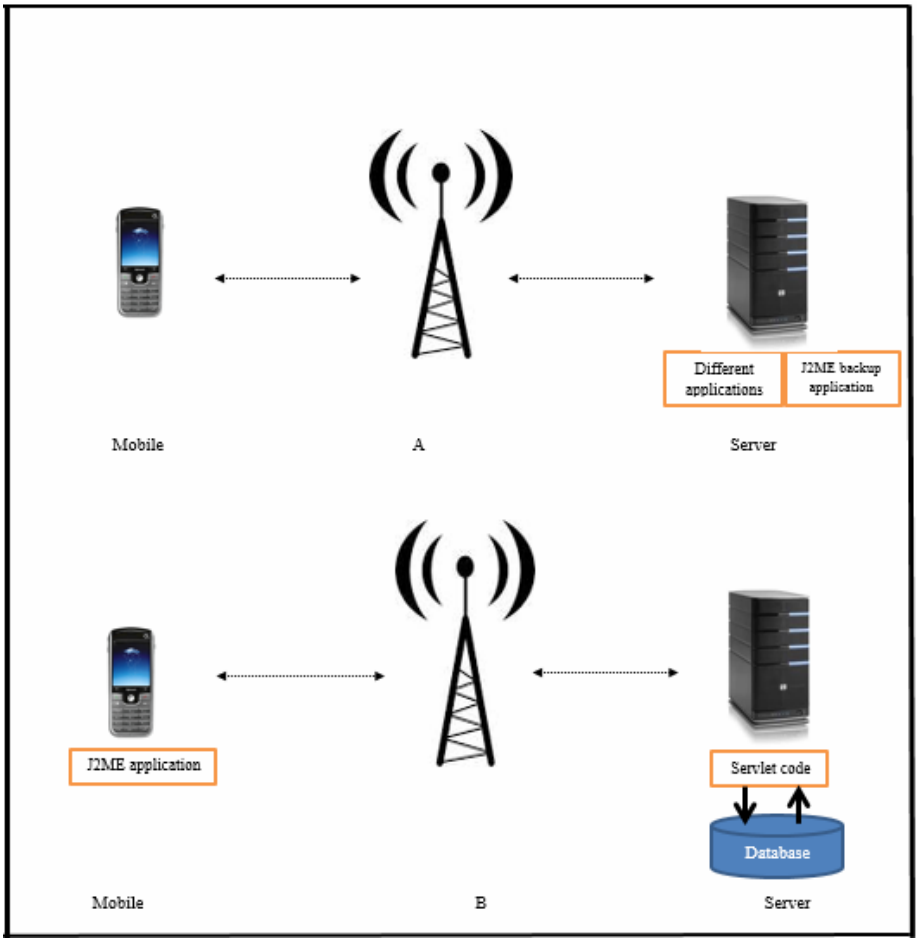

*Figure 6: D*iagrammatic representation of the system

The application is not limited only to sending contacts to a server, but also retrieving those contacts and text from where they are saved. These processes need to be authenticated in order to minimize the probability of someone accessing some others data because s/he has the SIM card of that user. The authentication asks for a password in which the user inputs during first time registration. During retrieving, if the user gives the right password, then the contact saved will be displayed.

Users also have the chance to change their passwords. This increases the safety of users by changing their passwords frequently.

There is also a security question entered during registration. The answer that the user enters uses to retrieve back the password incase the user forgets it.

All options on the application have their own user interface except 'send all contacts' and 'select and send' which are used to send all contacts on the phone including name and number and sending selected contacts consecutively.

4.1 How the Backup System Works

Mobile backup is done in different areas using Internet connection, especially on a website, which allows users even to save their contacts using computers. In this case the backup system is intended to do without Internet connection so that any mobile user in Ethiopia can use it. The system works as follows:

The user sends request to the server using a number that is assigned for this purpose. When the request reaches to the server, the server registers the user phone as a username and sends the application for that user.

The user installs the application on the mobile by answering the security question asked and entering password. The security question helps the user to get back or reset his/her password incase it is forgotten.

During this process, the password and the security text will be saved on the server's database for future use.

The user will have different options on the application that s/he gets: Send all contacts, Write and send, Retrieve, Change password, and Reset password.

The user uses one of those options, for example; if a user wants to send all contacts to the server, s/he can use the option "send all contacts" and this will send all contacts on the mobile phone to the server.

In this case the system checks if the backup is processed again. That means previously saved contacts are checked to avoid redundancy and only the new (non-existing) ones are backed up. This helps phone users that don't have good knowledge on the technology to backup easily using only a single menu so that even if to backup one new contact, s/he can select "send all" and the system will check which is new to take backup.

This process has its own disadvantage and it is recommended not to use it if the user is sure which contact is new. If the user wants to send by writing, s/he can use the option "write and send". With this option the user has a chance to write name contact or text that s/he wants to backup.

If the user wants to retrieve data saved on the server, s/he can use the option "retrieve", which leads the user to enter his/her password to check that the requester is an authorized user. If the password is correct, then the data saved will be displayed as a list on the user's phone.

The application always uses the user's number as a user name so that the user is not expected to enter username. This helps all users to be safe that no one can see their data even if someone can know the password of the other, because s/he has to get the SIM card too.

In some cases, mobile users may forget their passwords due to complexity of the password or for different reasons. For this purpose, there is an option which says "reset password" on the menu. This option helps the user to reset his/her password using the security s/he entered during registration.

Resetting is done by changing the password which was previously saved to a constant number "123456", so that after resetting the user can change the password to the password s/he wants.

This process can only be done if the user is able to remember the answer s/he entered during registration as a security question.

4.2 Security Issue

The system is intended to backup data for storage or due to fear of data loss. Through these activities, the user should be free to send any of his/her data to the server without any fear of security that s/he is going to face. As designers we are responsible to worry about how the data is moving from the phone to the server and also how the data is kept on the server.

The first part that needs to secure users' data is to integrate user phone and password.The user is not expected to enter his/her phone number to the system. Phone number is registered as user name and this is retrieved by the system from the SSID number of the SIM card. This helps the user to be safe about his/her data because even if someone knows the password it is impossible to retrieve other's data because the SIM also must be there, since retrieving needs both user name and password.

The password and the keyword have also to be secured. For this, MD5 is used. MD5 hashing is better because it is not an encryption algorithm instead it is a hashing algorithm so that there is no way to decrypt back. This keeps user password safe and unknown by any means [15].

5. Conclusion and Future work

Through this research attempt has been made to design and develop a mobile backup system. A number of tasks were done in order to make the work successful. Review of related literatures was one of the most important tasks which enabled us to get good understanding of the problem and technologies available so far.

After having a relevant information on the existing scenario regarding mobile backup system, attempt has also been made to collect requirements and model using different modeling techniques like use case and flowcharts. Following the development of the prototype, the testing process exhibits the validity of the concepts and the design proposed.

From the application designed, we concluded that most mobile phones can have a backup system so that the user can send contacts and other data.

Since there are scope limitations on the work, further enhancement is recommended. As it is clearly stated in different parts of this paper, the solution designed has some limitations like platform dependency and synchronization. Based on these, we recommend the following as future work:

- Platform independence: There are lots of mobile operating systems. It is better to design a system to fit in all operating systems so that any phone user can use the application.
- Design an application which backs up multimedia data as well.
- Add more functionalities, for example, synchronization, which is a way of returning backup data to the original place where they are taken.
- The application can request the user to send the data to database when the user saves new contacts.

References

[1] http://www.ethionet.et, last accessed on June 10, 2012.

[2] www.mobyko.com/, last accessed on June 18, 2012.

[3] Dashwire.com/, last accessed on June 18, 2012.

[4] www.gizmodo.com/, last accessed on June 18, 2012.

[5] web.orange.co.uk/p/contacts/home, last accessed on June 15/2012

[6] en.wikipedia.org/wiki/Mobile_phone, last accessed on June 15, 2012.

[7] Peter Holt, "Mobile Technology for Social Transformation", Nimbus Consulting Ltd., September 2010

[8] http://www.allaboutsymbian.com/reviews/item/Rseven-nline_mobile_backupsync.php, last accessed on June 18, 2012.

[9] Harald Welte, "Anatomy of Contemporary GSM Cellphone Hardware", April 16, 2010.

[10] Rabindranath Dutta and Richard Scott, "Automated Backup of Wireless Mobile Device Data onto Gateway Server while Device is Idle", 2002.

[11] Liren Chen, Jack Streenstra, and Kirk S. Taylor, "Peer to Peer Distributed Backup System for Mobile Devices", 2010.

[12] Tom Frencel and Suavek Zajac, "Mobile Access to Backup and Recovery Services", 2012.

[13] Robert Meadows, Jonatan Salcedo, and Garrett Larson, "Mobile Phone Data Backup System", 2007.

[14] http://www.webopedia.com/TERM/M/mobile_phone.html, last accessed on June 18, 2012.

[15] Ronald Ashri, Steve Atkinson, Danny Ayers, Marten Haglind, Bill Ray, Rob Machin, Richard Taylor, and Chanoch Wiggers, "Professional Java Mobile Programming".

[16] http://pogue.blogs.nytimes.com/2012/08/09/how-to-make-your-lost-phone-findable/, last ccessed on Feb 6, 2013.

[17] http://www.lovelysms.com/mobile-phone-health-issues.htm//, lLast accessed on Feb 7, 2013.

[18] http://www.smartfuzz.com/ online mobile contact backup system, last accessed on Feb 7, 2013.

[19] Battery Life Measurement and Current Consumption Technique, Version 6.3, 25th May 2011.

[20] SIM Card Reader, SIM Card Backup Device, www.alibaba.com, last accessed February 18, 2013.

[21] Bhart Welingkar and Jiji Nair, "Data Backup for a Mobile Computing Devices", 2008.