International Journal of Computer Applications (0975 – 8887)
Volume 57– No.22, November 2012

Mobile Client's Access Mechanism for Location based Service using Cell-ID

Gurjeet Kaur
M.Tech Student
Computer Science Department
S.B.S State Technical Campus,
Ferozepur, India

Monika Sachdeva
Associate Professor
Computer Science Department
S.B.S State Technical Campus,
Ferozepur, India

Navdeep Singh
B.Tech Student
ECE Depatrment
B.B.S.B Engineering
College,Fatehgarh Sahib, India

ABSTRACT
Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. A location-based service is a service that determines the location of a mobile device and uses this to provide functionalities and information specific to that location. With the growth of the importance and of the audience of location-based services, questions of security and privacy are brought forward. As services are being built on top of this technology, the number of parties increases significantly, and the possibility of a malicious insider (or a misbehaving insider) emerges. The extent to which the parties care to trust each other has reduced, and trust amongst the various parties can no longer be assumed by a location-based service. An attacker may try to steal a service (e.g., claiming to be a client to get free internet access), service providers may gain of private information. There should be a proper authentication mechanism between client and server to access the services. By considering some important factors like Cost, Energy Efficiency, we have proposed an Access Mechanism in which mobile Phone Users will send request for some services from server. Firstly Location Verification is done; server verifies the User's Mobile Phone's location against authorized location. After User/Device Authentication is done, server checks User/Device Identification. If both conditions are true, server will grant access to the users for services and resources.

Keywords
Location Based Services, Cell-ID, IMEI number, IMSI number, Android, LAC

1. INTRODUCTION
Cell-Id is an id assigned to every BTS. GSM device will only know which cell it is connected to. The Area covered by each cell depends on radius of each BTS that will limit the area down to some extent. Determining how useful cell id as location method is for different sorts of areas will be beneficial for cell id software solutions in general. There are portable devices exists that uses Context Aware Systems. When it comes to its usefulness in rural areas no field test have been found, and it will be most interesting to know if there are any practical use of cell positioning in such areas. Accordingly, if location by cell id works in most regions, this data can be used by software installed on these smart phones. In dense city areas a large number of GSM cell phone towers are within reach at any given time but there are some drawbacks of GPS System, large buildings can block out a straight course to any satellites used for positioning. Since GPS systems use four satellites to perform an advanced triangulation, it will be useless if any of the required satellites are hidden behind a large object. For the exact same reason GPS does not work inside buildings. When an area is covered by cells, the number of cells will depend of several factors. The most obvious element will be usage. A region with many users will most probably have more cells to serve customers than a more sparsely populated would.

• In mid-sized towns the density of GSM cell phone towers can be to some extent lower, but the overall advantage of GPS could be improved. In rural regions the density of GSM cell phone towers can be so low that it is probably not usable in large areas. GPS could be the only positioning method in these cases. In large cities the density of GSM cells will probably be so high that an accurate location can be calculated. It will not be as accurate as GPS, but it will be able to give a good enough location, and even work indoors.

2. LITERATURE REVIEW
2.1 Location Based Services
Location Based Services (LBS) are information services that provide users with customized contents, such as the nearest restaurants/hotels/clinics, retrieved from a dedicated spatial database based on the user's current location. The LBS can obtain user's geographical position/location by making use of technologies such as Cell-ID, Global Positioning System (GPS), triangulation/triliteration etc. LBS not only serve individual mobile users, but also play important role in public safety. The role of Location Based Services is to retrieve the information directly related to the location of the user at the time of making the request.

3. EXISTING CELL-ID MECHANISM
3.1 Cell –Id
A GSM Cell ID (CID) is a generally unique number used to identify each Base transceiver station (BTS) or sector of a BTS within a Location area code (LAC) if not within a GSM network. In some cases the last digit of CID represents cells' [1]. This is simplest, cheapest and easiest mobile positioning system to implement. This is an inherent feature of all cellular systems, minimal changes to existing systems needed. No changes to networks or handsets and allows positioning services to be offered today at extra cost.

3.2 Cell Coverage Area Co-Ordinate (Cell ID)
Positioning Service will receive a request for location. After this the serving BTS ID is resolved from the Mobile Network and the service will look for the corresponding co-ordinates from the Network Database. When the correct co-ordinates

have been found the location service is delivered to the MS. The system block diagram is presented in the next figure.

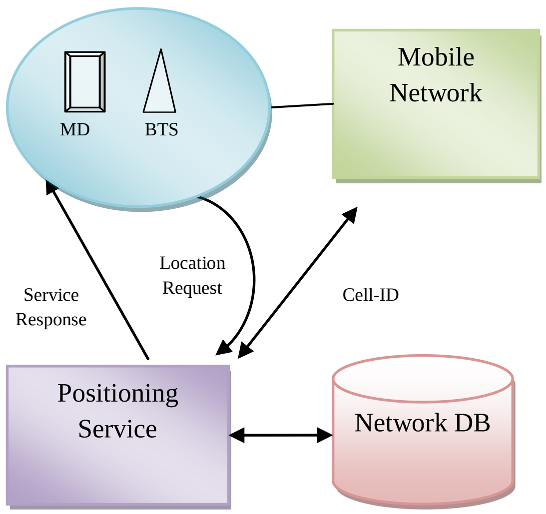


Fig:1 Existing Cell-ID based System

4. ANDROID PLATFORM

Android is a platform for mobile device developed by Google. It provides a complete set of software development: operating system, tools and APIs necessary to begin developing applications [2].

Android SDK was released by Open Handset Alliance in the month of November of the year 2007. Android is actually developed using the kernel of Linux 2.6 and the highlighting features of Android include the following [3]:

4.1 Components of Android App Development

The basic components of an Android application include Activity, Broadcast Receiver, Service, and Content Provider. Each of these which when used for any application has to be declared in the AndroidManifest.xml. The user interface of the component is determined by the Views. For the communication among these basic components we use Intents and Intent filters which play crucial role during app development [4].

4.1.1 Activity

An Activity is, fundamentally, an object that has a lifecycle. An Activity is a chunk of code that does some work; if necessary, that work can include displaying a UI to the user. It doesn't have to, though - some Activities never display UIs. Typically, we will designate one of our application's Activities as the entry point to our application [5].

4.1.2 Broadcast Receiver

Broadcast Receiver is yet another type of component that can receive and respond to any broadcast announcements.

4.1.3 Service

A Service is a body of code that runs in the background. It can run in its own process, or in the context of another application's process, depending on its needs. Other components "bind" to a service and invoke methods on it via remote procedure calls. An example of a Service is a media player; even when the user quits the media-selection UI, she probably still intends for her music to keep playing. A Service keeps the music going even when the UI has completed.

4.1.4 Content Provider

Content Provider is a data storehouse that provides access to data on the device; the classic example is the Content Provider that's used to access the user's list of contacts. Our application can access data that other applications have exposed via a Content Provider, and we can also define our own Content Providers to expose data of our own.

4.1.5 Intents

Intent is a simple message object that represents an "intention" to do something. For example, if our application wants to display a web page, it expresses its "Intent" to view the URI by creating an Intent instance and handing it off to the system. The system locates some other piece of code (in this case, the Browser) that knows how to handle that Intent, and runs it. Intents can also be used to broadcast interesting events (such as a notification) system-wide. There are two types of intents namely implicit and explicit intents. Implicit intents have no specified component where as Explicit intents do specify the component.

4.1.6 AndroidManifest.xml

The AndroidManifest.xml file is the control file that tells the system what to do with all the top-level components (specifically activities, services, intent receivers, and content providers described below) we have created. For instance, this is the "glue" that actually specifies which Intents our Activities receive.

4.1.7 Views

A View is an object that knows how to draw itself to the screen. Android user interfaces are comprised of trees of Views. If we want to perform some custom graphical technique (as we might if we're writing a game, or building some unusual new user interface widget) then we would create a View.

4.1.8 Notification

A Notification is a small icon that appears in the status bar. Users can interact with this icon to receive information. The most well-known notifications are SMS messages, call history, and voicemail, but applications can create their own. Notifications are the strongly-preferred mechanism for alerting the user of something that needs their attention.

5. Gaps in Existing Work

(Mathkour, 2010) proposed and developed a GPS-based Mobile Service Locator System [6] to help individuals in different walks of life, find addresses and locate their services of interest using their mobile devices. This approach is realized by specialized handsets, which require special soft- or hardware to calculate their positions. A mobile device with GPS would be a handset based method.

- GPS based system is not accurate in some places like underground, in the buildings or inaccurate due to atmospheric conditions. Accuracy depends on the number of visible satellites, Obstacles like buildings and trees can deflect the signal, causing your position on the GPS screen to be off by as much as 100 feet. Atmospheric conditions may also affect GPS accuracy.

- Because the GPS receiver has high power consumption, the mobile terminals require higher battery capacity.

- GPS does not work indoor or when satellites are in shadow. Set-up time can be quite long, many minutes in the worst case;

- A client device allowing the user to request certain services on the bases of his/her location. In which communication is done through an SMS sent using the SIM of the handset to the cell phone provider that is not cost effective.

- Section 7 will explain in detail about our proposed work in which we have used Cell-ID based system .GPS based systems have some disadvantages we used in our thesis together with cell-ID based system because for different types of services at different times, it may be better to use one method over another.

- Cell-ID positioning is simple and economic. It is very fast to calculate the location information. It does not require any upgrade of handsets or network equipments, but since the handset can be anywhere within a cell, accuracy depends on cell size.

- It estimates the location of a mobile terminal indoors, in a building or underground locations etc.

6. Importance of user's location verification and Identity Verification

With the increase in the growth of wireless networks and sensor and mobile devices, we are moving towards an age of ubiquitous computing where location information will be an integral part of many applications. Researchers [7] have described how the use of location information can make applications more secure. For instance, a user should be able to control or fire a missile from specific high security locations only. Verifying the location information in addition to the checks that are performed by traditional methods of authentication and access control will improve the security of the underlying application. Location information, however, can also be misused causing a breach of privacy and security. For example, information about the location of a user can compromise his privacy. If a malicious user knows about the location information of a person, he/she can infer the activities being performed by that person. Protecting the confidentiality, integrity, and availability of location information is of utmost importance.

7. OUR PROPOSED ACCESS MECHANISM BETWEEN MOBILE CLIENT AND PHP SERVER

7.1 Objectives of Proposed Work

To Use best Positioning techniques that have following characteristics:

- Cost Effective
- Energy Efficient
- Higher Accuracy level
- Locality depends upon situation. (Either urban rural)

- To use the cost effective Communication network.
- To develop a secure Authentication Mechanism for location based services. The focus is on the authentication mechanism for LBS. Figure 2 shows UseCase of authentication mechanism for LBS.

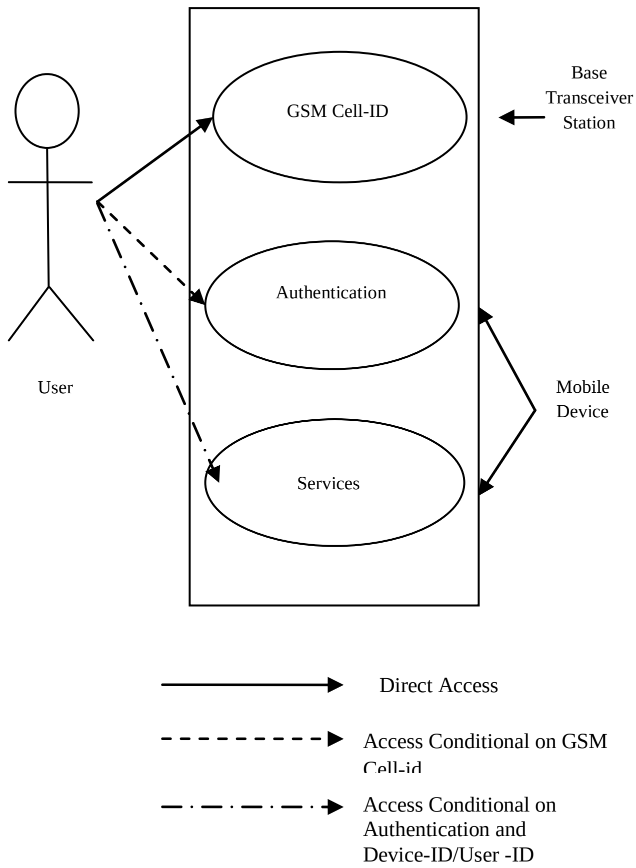


Fig. 2 The Proposed USECASE

7.2 Using cell-ID

In order to implement the location-based service system with cell identifier Positioning Service will receive a request for location. Each BTS broadcasts both the LAI and the Cell-ID to its cells.

The Mobile Station is always receiving these broadcast messages; thus, it always knows its Cell-ID. After this the serving BTS ID is resolved from the Mobile Network and the service will look for the corresponding co-ordinates from the Network Database. When the correct co-ordinates have been found the location service is delivered to the MS. Hence, the MS is assumed to be located at the BTS coordinates independently of its actual position within the cell [8]. Figure 3 shows our cell-ID based mechanism architecture. Once cell-ID and LAC are identified, data is sent via GPRS to the PHP server. Then the server crosschecks this with a list containing authorized coordinates or Cell IDs before allowing the user to attempt the second form of authentication. After this step the application request for IMEI/IMSI number from SIM. The SIM card consists of mobile particular information such as SSN (SIM Serial Number), IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), LAI (Location Area Identity) and Ki (Authentication Key). This research uses only IMEI/IMSI code to identify the device and identify the person who registered to use that device. After that, Application will send encrypted IMEI and IMSI number via GPRS to PHP server using POST method of HTTP protocol and server again crosschecks this with a list containing authorized IMEI/IMSI number in Database. Upon location verification using Cell-

ID/LAC and user authentication using IMEI/IMSI, the services are accessible to the user. Figure 4 shows the flow of information between Mobile Client and PHP server.

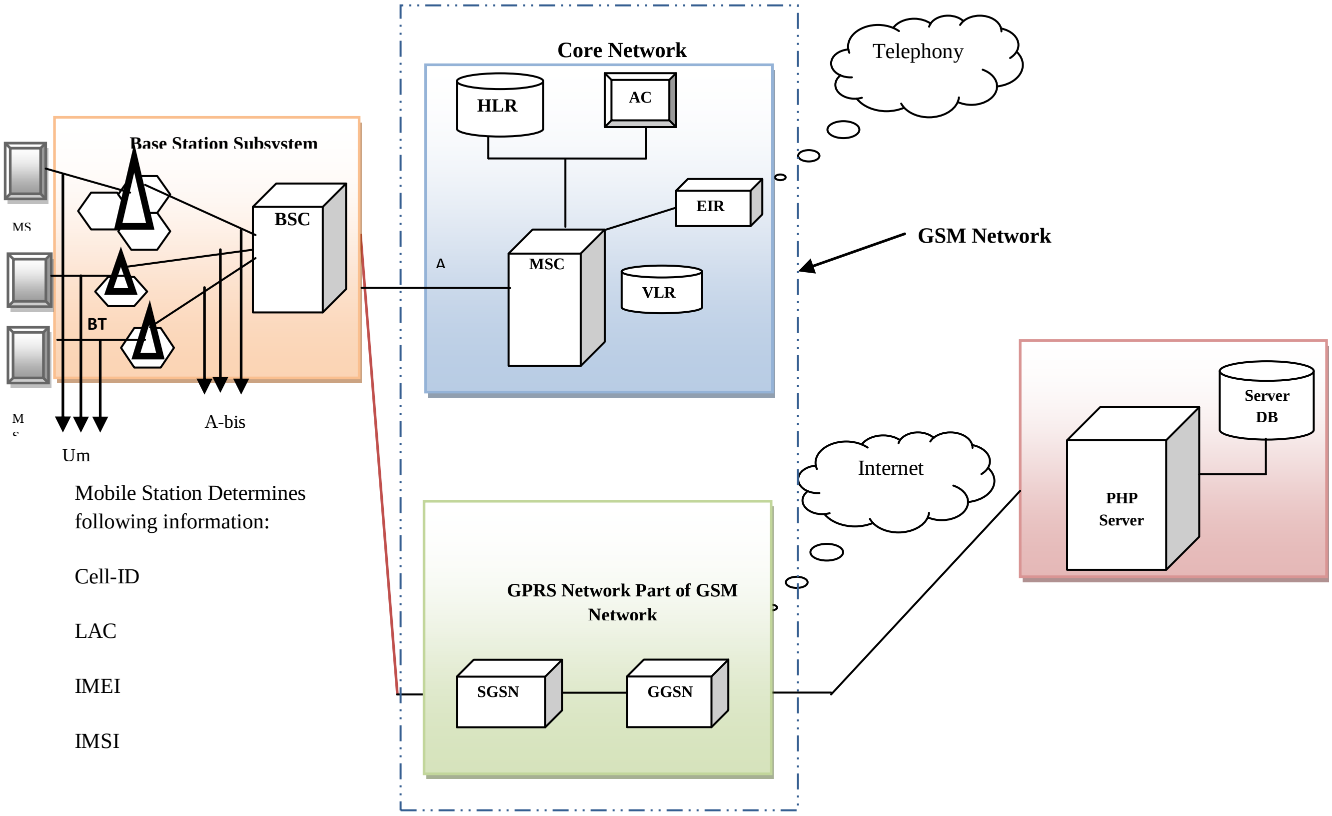


Fig. 3 Architecture of Cell-Id based system

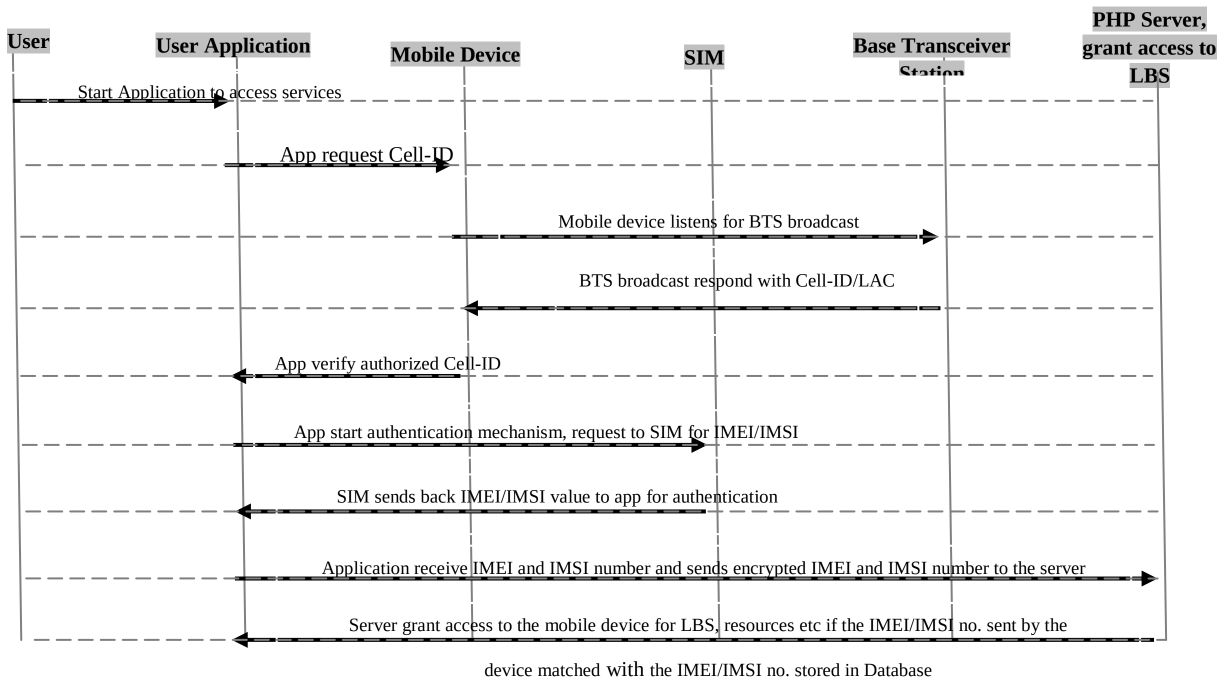


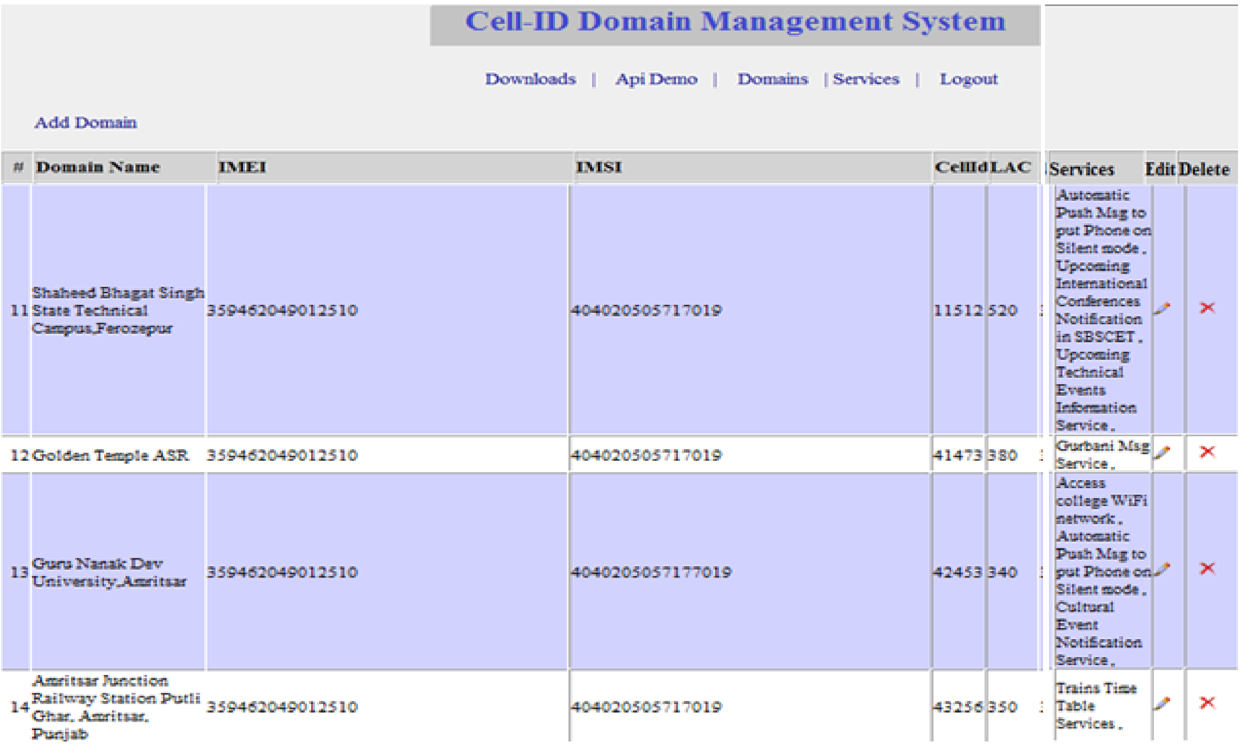
Fig. 4 Cell-Id Based System Flow Chart

8. PHP SERVER

We have Database at Server side which contains all the necessary information about client's device that is IMEI number, client's ID that is IMSI number, Location information like Cell-ID, Location Area Code. On the bases of above information, Database will grant access to some Services.

We can add the necessary information that is Location information, Device information and User information in given columns. In figure 7 shows the domain information and available Services for the restricted domains and figure 8 shows comlete Domain Management System that have various columns : Domain Name ,IMEI number, IMSI number, Cell-ID, LAC, and Services.

Fig. 7 Cell-ID Domain Management System



#	Domain Name	IMEI	IMSI	CellId	LAC	Services	Edit	Delete
11	Shaheed Bhagat Singh State Technical Campus,Ferozepur	359462049012510	404020505717019	11512	520	Automatic Push Msg to put Phone on Silent mode , Upcoming International Conferences Notification in SBSCET , Upcoming Technical Events Information Service ,		
12	Golden Temple ASR	359462049012510	404020505717019	41473	380	Gurbani Msg Service ,		
13	Guru Nanak Dev University,Amritsar	359462049012510	4040205057177019	42453	340	Access college WiFi network , Automatic Push Msg to put Phone on Silent mode , Cultural Event Notification Service ,		
14	Amritsar Junction Railway Station Putli Ghar, Amritsar, Punjab	359462049012510	404020505717019	43256	350	Trains Time Table Services ,		

Fig.8 Cell-ID Domain Management System

In Figure 9 we have various fields that will help us to check the errors. This is only for testing purposes.If we want to test the Cell-ID Domain Management System , we have to enter the information in given field for which we want to give or restrict the access of Mobile Client.Fig 10 shows IMEI and IMSI number testin.After pressing Check button we receive JSON String that shows 0 errors and massege "imei and imsi numbers exists. If we got 1 2 or 3 errors in JSON String that means System is not in good working condition.

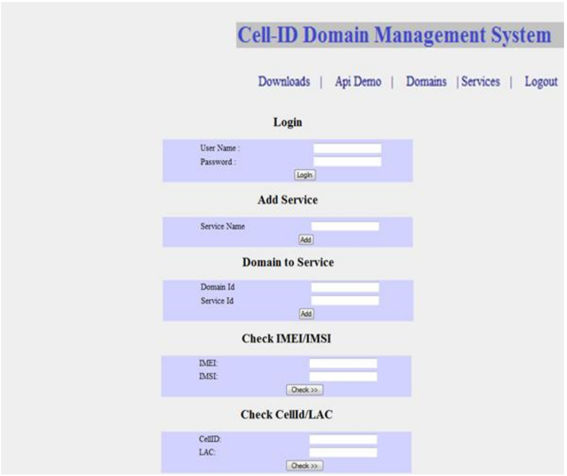


Fig.9 Cell-ID Domain Management System

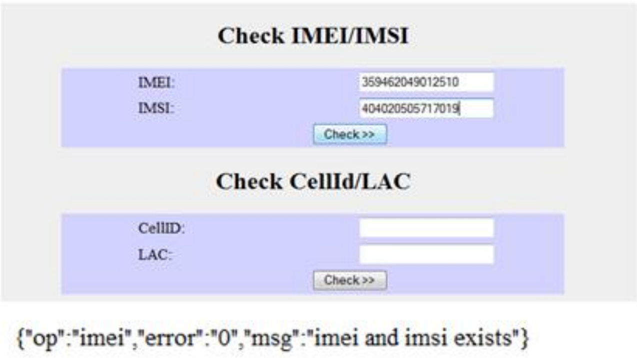


Fig.10 Cell-ID Domain Management System

9. RESULT AND DISCUSSION

9.1 CIDActivity

In the Main activity CIDActivity , first option is to present the user with the current network information, such as the Cell ID and Location Area Code (LAC). The LAC in this case is for testing purposes only. The Cell ID, if one is available, will be displayed in the proper format; otherwise the application will notify the user there is no connection.

Android contains two packages containing classes that allow the programmer to obtain network information, such as the Cell ID. These packages are android.telephony and android.telephony.gsm. Each contains the required classes of android.telephony.TelephonyManager and android.telephony.gsm.GsmCellLocation, classes respectively. Activity must request services of the phone to access this network data. This is done so by:TelephonyManager tm = (TelephonyManager) getSystemService(*TELEPHONY_SERVICE*);

This allows access to the following class and an instantiation of it to be used for data retrieval:
GsmCellLocation loc = (GsmCellLocation) tm.getCellLocation();
The remaining portions of this first function in the activity consist of displaying this data to a TextView for the user. The second portion of the activity is whether or not to allow the user to advance to the authentication mechanism. The application should only allow this to occur if the user is connected to an authorized Cell ID. The list of authorized Cell IDs is written into the code at server side application. These IDs will be cross-referenced when the user depresses the "Send CellID/Lac" button to compare the current Cell ID to the list. If there is a match, then the user will be directed to the User/DeviceIdentificationActivity, otherwise the activity will terminate. The following is the example the "ID" is a constant representing where the true value would be checked:

```
TelephonyManager tm = (TelephonyManager) getSystemService(TELEPHONY_SERVICE);
GsmCellLocation loc = (GsmCellLocation) tm.getCellLocation();
cellID = loc.getCid();
lac = loc.getLac();
```

The only requirement in the manifest file is the course location access permission.
Figure 10 and figure 11 shows CellidActivity that display cell-id of nearest BTS and Location Area Code (LAC).

Fig.10: CellIDActivity **Fig. 11: CellIDActivity**

9.2 UserDeviceIdentificationActivity

This activity only contains a button with a notification tied to it. The architecture ties this to the authentication mechanism that is discussed below.

```
String imei = tm.getDeviceId();
String imsi =tm.getSubscriberId();
```

Figure 13 shows IMEI and IMSI numbers.

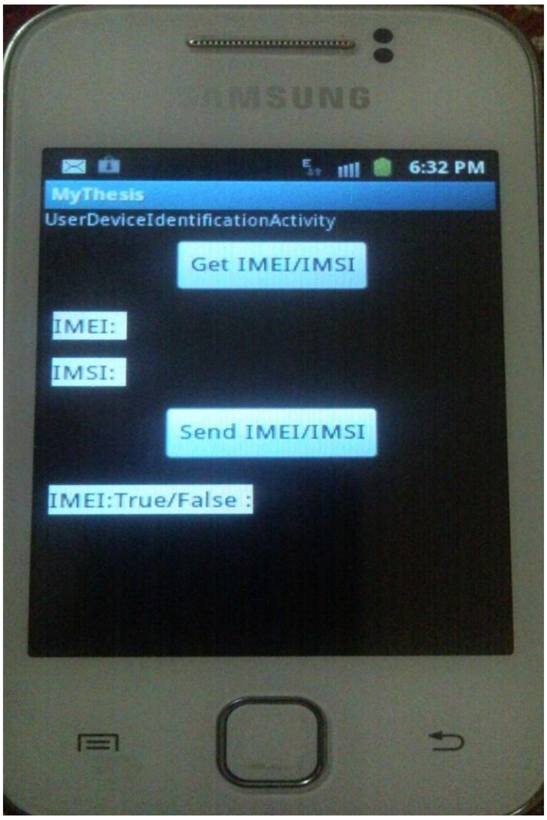


Fig:12:UserDeviceIdentificationActivity

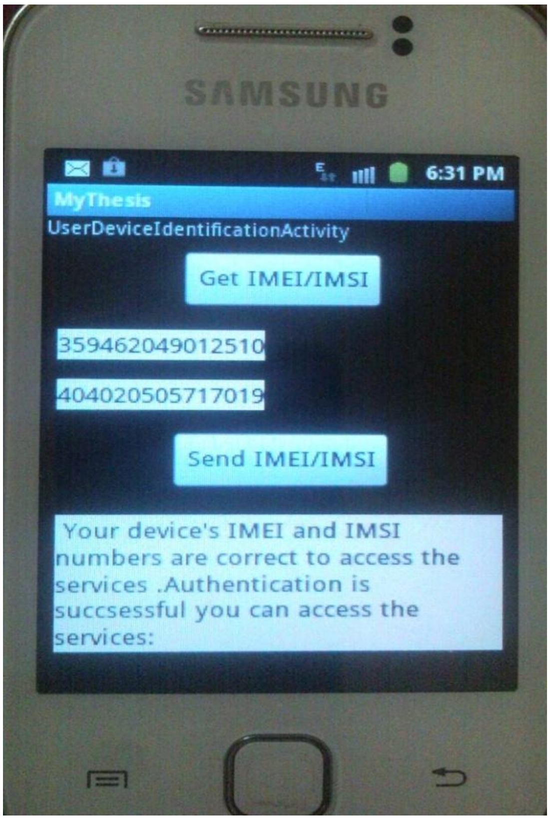


Fig.13: UserDeviceIdentficationActivity

9.3 Comparison of existing system and proposed system

Table 1 shows the comparison of existing system and our proposed system.

Table 1 Comparison of Existing system and proposed system

Conditions Based On	Existing System	Proposed System
Location Technique	GSM Cell-ID	GSM Cell-ID
Authentication Mechanism	User Name and Password	IMEI and IMSI number
Communication method to transmit required information	SMS	GPRS
Cost of Communication Method (Monthly Pack Airtel)	75 INR	98 INR
Number of Requests can be sent	2700	25600
Limitation	200 Smses/Day	No limitation

In existing systems researchers used Username and password.

By knowing username and password an attacker may try to steal a service (e.g., claiming to be a client to get free internet access) and users may lie about their whereabouts (e.g. to lower taxes due in a road pricing scheme).

Due to above reasons we have used International Mobile Subscriber Identity for user's identity and International Mobile Equipment Identity for Mobile Device's identity.

Airtel provide us monthly Services, in SMS service, 2700 Local & National SMSes in INR 75 but we can send limited number of SMS/Day (200 SMS/Day).Another Service that is GPRS Service in which Airtel provide 1GB in 98 INR [9].

In our experiment one request uses 0.04 MB and we have 1024 MB and we can send 25600 requests.

10. CONCLUSION

This paper proposes an Access Mechanism between Mobile Client and PHP Server for Location Based Services allow personnel, such as first responders and military members, to securely access and manage valuable resources and applications under certain conditions. At the same time it prevents others, who are unauthorized, access to the same resources and applications. The proposed architecture is divided in to two main components: Location Verification, Device/User Identification.

The first component is the location-verification application. This is an Android application that can check the Cell ID of the BTS to which the MCD is connected, or both. The application crosschecks this with a list containing authorized coordinates or Cell IDs before allowing the user to attempt the second form of authentication.

The second component is User and Device identification application. This component can only be accessed after being properly validated by the location verification application. In this component we have used IMEI number for Device identification and IMSI number for User identification. On the bases of IMEI/IMSI number, server will grant the access for services to the authorized users. Our Cell-ID technique is more energy efficient in terms of consumption of Mobile Device's battery power than GPS. We have used GPRS for data transfer instead of SMS. This SMS based system is neither efficient nor cost effective. In most countries the cost of GPRS is cheaper than SMS by a factor of 20 to 100. To send required information from Mobile client to Server we prefer GPRS. Table 1 shows the results that GPRS is most suitable and cost effective communication method between Mobile Client and Server.

11. FUTURE WORK

We have proposed a secure authentication mechanism in which we used Device id (IMEI) number and subscriber identity (IMSI) number. In our proposed work every time users request for services from server, they have to send the IMEI and IMSI number along with location information. There are possibilities various attacks on IMEI and IMSI number by attackers. An attacker may try to steal a service (e.g., claiming to be a client to get free internet access), service providers may gain of private information on user's movements (e.g., determine your preferred shopping areas), and users may lie about their whereabouts (e.g. to lower taxes due in a road pricing scheme). The information flow between client and server should be securely managed. We will compare different encryption techniques and choose the best encryption technique to encrypt the information before sending it to the PHP Server. We will choose one that is more secure and cost effective in terms of encryption time and battery usage.

12. REFERENCES

[1] Cell-ID: Available at http://en.wikipedia.org/wiki/Cell_ID

[2] S. Sukaphat, "*Creating of Mobile Search System for Traffic Inquiry*", Proc. 10th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2009),IEEE, 2009, pp. 417 - 420, doi: 10.1109/SNPD.2009.73.

[3] Meier Reto*,(2010) " Professional Android 2 Application Development",*Wrox, 247_264, 2010

[4] Haseman Chris, (2008) "*Android Essentials"*, firstPress, 9_17, 2008

[5] Steele J., To N., Conder S., Darcey L. (2012) "*The Android Developer's Collection*", Addison- Wesley Professional, 30A_40A, 2012.

[6] Hassan I. Mathkour A "*GPS-based Mobile Dynamic Service Locator System "* 2210-8327 ª 2011 King Saud University. Production and hosting by Elsevier B.V. All rights reserved. Peer review under responsibility of King Saud University. doi:10.1016/j.aci.2011.05.003

[7] Denning Dorothy E, MacDoran Peter F.*"Location-based authentication: grounding cyberspace for better security".* In: Proceedings of the computer fraud and security. Elsevier Science Ltd;February 1996.)

[8] Emiliano Trevisani, Cell-ID location technique, limits and benefits: an experimental study, Proceedings of the Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2004)1550-6193/04 $20.00 © 2004 IEEE

[9] http://www.airtel.in/applications/xm/MobilePrepaidTariffTab.jsp?CIRCLE=1&CIRCLENAME=Punjab&ID=1563&SERVICENAME=SMS%20PACK%20RC%2075&link=S