Implementation of Secure Authentication Mechanism for LBS using best Encryption Technique on the Bases of performance Analysis of cryptographic Algorithms

Gurjeet Kaur[1], Monika Sachdeva[2]
[1]Department of Computer Engineering,S.B.S State Technical Campus, Ferozepur,India
gurjeetrandhawa4@gmail.com
[2]Department of Computer Engineering,S.B.S State Technical Campus, Ferozepur,India
monika.sal@rediffmail.com

ABSTRACT

Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. 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. In this paper we have proposed an Authentication 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. The information flow between client and server should be securely managed. The security of transmitted data over a wireless channel aims at protecting the data from unauthorized intrusion.Encryption algorithms, which play a main role in information security systems, consume a significant amount of computing resources and battery energy, which are very limited because usage time of a mobile device is constrained by its most critical resource – battery. High energy consumption has a direct impact on the battery life, and, consequently, on the duration and extent of the user's mobility. Thus, the reduction of energy consumption of a portable system is of the primary importance. We have compared the encryption algorithms to encrypt the User/Device information before sending it to server. Numerical results obtained through simulation are compared on the bases of throughput of various Encryption Algorithms. Encryption time is used to calculate the throughput of an encryption scheme. Increased throughput results in decrease of power consumption. The results are shown with respect to key size variation. It has been observed that AES 128 bit encryption Algorithm is better solution for our application.

KEYWORDS

Location Based Services, GPS, Mobile Network, IMEI, IMSI,Android

1. INTRODUCTION

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. Location based services (LBS)

DOI : 10.5121/ijsptm.2012.1602

is becoming one of the most promising and challenging market for various multinational mobile companies [1] [2]. 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. Therefore, accessing the service from a different physical location will provide a different response. It is possible to automatically trigger Location Based Services when the mobile device is at a particular location. These services can also originate in the user's mobile device itself in order to satisfy location-based requests like finding areas of interest, checking traffic conditions, finding our friends, vehicles, resources, machines and emergency requests. 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. This decrease of trust needs to be balanced. The dependency on trust can be replaced by adequate authentication mechanism. In this fashion, there is a desire to shift from needing trust towards using security controls. Making this shift possible is currently the focus of research in location-based services.

In this paper we have proposed an authentication mechanism for location based services. . 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 either check GPS coordinates or the Cell ID of the BTS to which the MD 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 (International Mobile Equipment Identity) number for Device identification and IMSI (International Mobile Subscriber Identity) number for User identification. On the bases of IMEI/IMSI number, server will grant the access for services to the authorized users.

2. AUTHENTICATION

While the foregoing technical considerations provide constraints on the technical provision of the proposed solutions, issues such as security and privacy hold the key to take-up of the services. Authentication is most important part of secure communication in any network. On the basis of this, Bishop provides the following definition: "*Authentication is the binding of an identity to a subject*" [3]. The relation between an identity and a subject that acts on behalf of an entity is also implicitly contained in the definition of authentication given by (Pfleeger, 2007): "*Authentication is basically a means of providing or verifying a previously given identity*"[4].

3. RELATED WORK

Researchers have explored the use of various sensors in mobile devices to provide context data. Schmidt, et al., 1999 developed a framework for considering various contextual features, including human factors and physical environment factors. Human factors include information about the user (e.g. habits, emotional state, biophysical conditions), social environment (co-location of others, social interaction), and the user's tasks (what they are doing at the moment). Physical environment factors include the physical conditions at the moment (such as light, temperature, noise.), infrastructure (surrounding resources such as computers or phones that might be used) and, of course, location (including absolute location and relative location). Applications of such data can range from changes in the system's output depending upon context (e.g. notifications or alerts may be contingent on whether others are around), to simple interface improvements (e.g. turning up the volume in noisy environments, or providing a backlight on the screen in low light conditions).Some of the research on context-aware computing has quite direct implications for e-commerce. First, much of the research has been completed in indoor environments, using such location and context detection technologies as infrared, ultrasound, and low power radio [5] [6]. Hence, it has the potential to fill in an important gap in the coverage afforded by GPS. Research within location-tracking in indoor environments has been conducted for over a decade. Early work such as the Active Location Badge system[6] uses infra-red technology but other sensor technologies have been explored as well [7].

Urs Hengartnera et al.(2006) presented a distributed, context-sensitive access-control architecture that avoids privacy violations.Their discussion revealed that access rights should not be publicly available and that constraints should be kept restricted, otherwise running the access-control algorithm can become complex. In particular, constraints should involve either a subject being granted an access right or an entity issuing an access right [8].

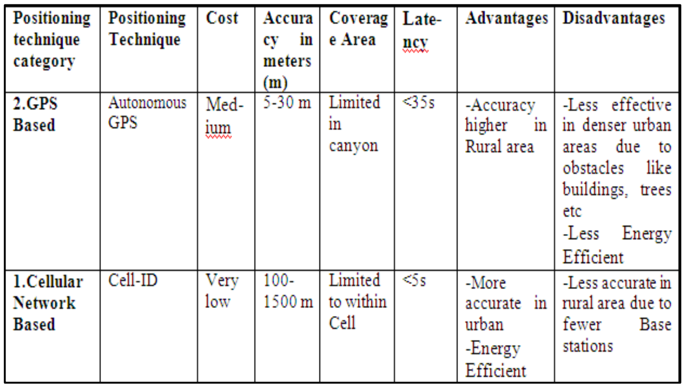
The use of location information can be used for enhancing the security of an application, and it can also be exploited to launch attacks. For critical applications, such as the military, a formal model for location-based access control is needed that increases the security of the application and ensures that the location information cannot be exploited to cause harm.

Indrakshi Ray et al. (2006) propose MAC that shows how the mandatory access control (MAC) model can be extended to incorporate the notion of location. They also show how the different components in the MAC model are related with location and how this location information can be used to determine whether a subject has access to a given object. This model is suitable for military applications consisting of static and dynamic objects, where location of a subject and object must be considered before granting access [9].

YoungHoon Yu et al.(2009) model the ontology with consideration of the user's position and the available time and implement a knowledge base using this ontology. The ontology also has information about shops for recommendations and personal profiles of users. A user can manage the information through the user interface module. This approach of collective intelligence is an effective implementation of LBS and should provide the most recent information. We test our system under the assumption that the user, who wants to watch a movie, is in a specific area. To recommend a list of theatres and movies to the user, our system executes an inference procedure with information on the starting time of movies, the current time and current position of the user, information on movies and theatres, and the user profile.[10]

Sasivimon Sukaphat(2011) presents a software development on Android Platform which applies cell identifier method for improving the accuracy of indoor localization. The objective of this research is to provide a detectable system, "Mobile Detective", for tracking and finding clues of lost mobiles.GPS may not be suitable for tracking lost mobiles. In order to solve this problem, cell identifier which indicates mobile device position by using station base information is introduced in this research. The location tracking process is run as background process by using Android service and it automatically repeats sending this information in an interval of time. The results from this process composed of position and mobile's particular information: SIM code and IMEI (International MobileEquipment Identity), are sent from the lost mobile to the recipient[11].

Table1. Comparison of GPS and GSM Cell-ID Technique



Positioning technique category	Positioning Technique	Cost	Accuracy in meters (m)	Coverage Area	Late-ncy	Advantages	Disadvantages
2.GPS Based	Autonomous GPS	Med-ium	5-30 m	Limited in canyon	<35s	-Accuracy higher in Rural area	-Less effective in denser urban areas due to obstacles like buildings, trees etc -Less Energy Efficient
1.Cellular Network Based	Cell-ID	Very low	100-1500 m	Limited to within Cell	<5s	-More accurate in urban -Energy Efficient	-Less accurate in rural area due to fewer Base stations

4. RELATED WORK 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.
- To compare different Encryption techniques and choose energy efficient technique to secure the sensitive data communicated in LBS.

5. PROPOSED ARCHITECTURE AND DESIGN

This chapter includes detail of implementation of the new approach. The main objective of the research is to develop and propose a new scheme, an authentication mechanism for LBS. The proposed scheme is based on two approaches: Cell-ID approach and GPS approach. We have used both positioning techniques alternatively because of their advantages and disadvantages in particular locality, situation. To achieve the research objective successfully, we have developed a USE CASE shown in figure 1.

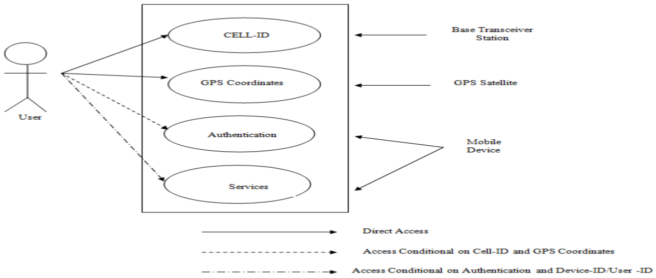


Figure1. Proposed USE CASE

In this section, we describe an architectural overview of our proposed system. The mobile terminals are assumed to possess a GPS receiver and the capability to determine the ID of the GSM cell they are currently located within. This paper proposes architecture to 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.

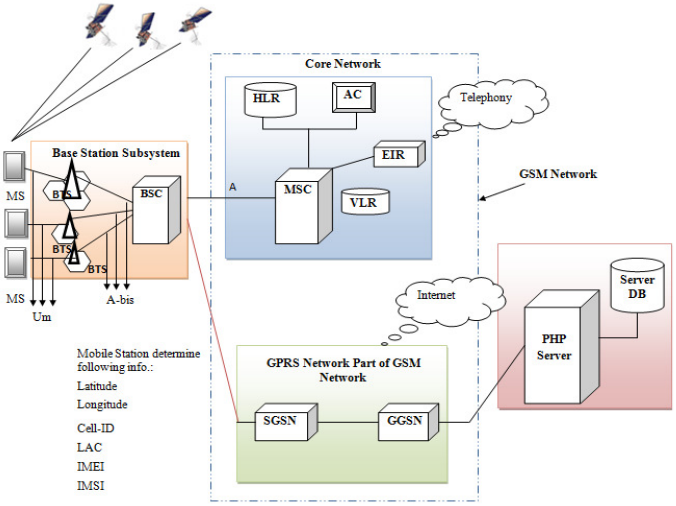


Figure 2. Architectural Overview

Figure 2 presents an architecture contains two major components: the location-verification application, user authentication mechanism and secure structure that contain the valuable resources and applications. The first component is the location-verification application. This is an Android application that can either check GPS coordinates or the Cell ID of the BTS to which the MS 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 the User/Device Identification. This component can only be accessed after being properly validated by the location verification application. In this second component device's International Mobile Equipment Identity number (IMEI) is used for Device Identification and International Mobile Subscriber Identity number (IMSI) is used for Subscriber or user Identification.

5.1 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. An MS 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.[15].Figure 3 shows flow of information. Once cell-ID and LAC are identified, the php server side application 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 to PHP server using POST method of HTTP protocol and 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.

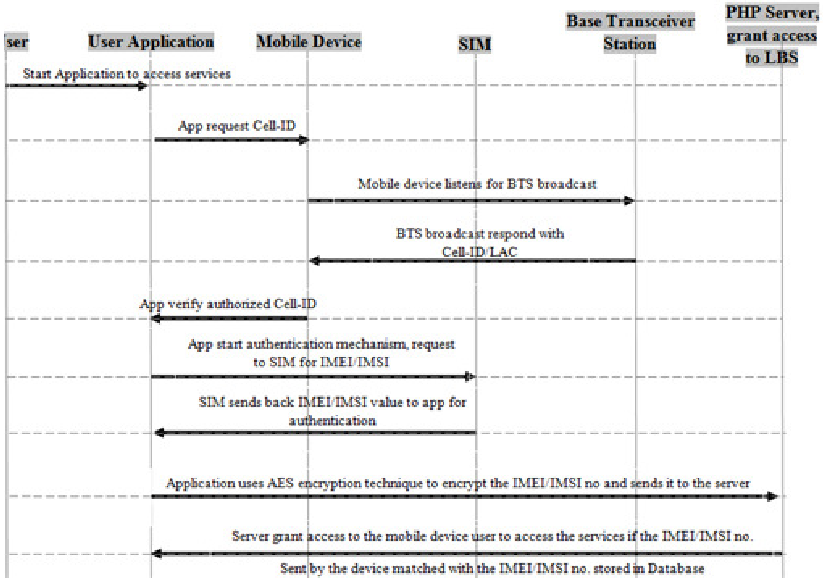

ser
User Application
Mobile Device
SIM
Base Transceiver Station
PHP Server, grant access to LBS
Start Application to access services
App request Cell-ID
Mobile device listens for BTS broadcast
BTS broadcast respond with Cell-ID/LAC
App verify authorized Cell-ID
App start authentication mechanism, request to SIM for IMEI/IMSI
SIM sends back IMEI/IMSI value to app for authentication
Application uses AES encryption technique to encrypt the IMEI/IMSI no and sends it to the server
Server grant access to the mobile device user to access the services if the IMEI/IMSI no.
Sent by the device matched with the IMEI/IMSI no. stored in Database

Figure 3. Flow Chart for Cell-Id Based System

5.3 Using GPS Based System

GPS stands for Global Positioning System, and is a way of locating a receiver in three dimensional spaces anywhere on the Earth, and even in orbit about it. In this scenario when user will start the application, application will send request to the mobile device that has built-in GPS receiver. Figure 4 shows flow of information. Once GPS receiver receives the GPS signal and determine location information which is latitude and longitude. After this step mobile device will send these co-ordinates to PHP server where these co-ordinates, Latitude and Longitude will be crosschecked with a list containing authorized coordinates. After this in authentication mechanism, 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 to PHP server using POST method of HTTP protocol and 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.

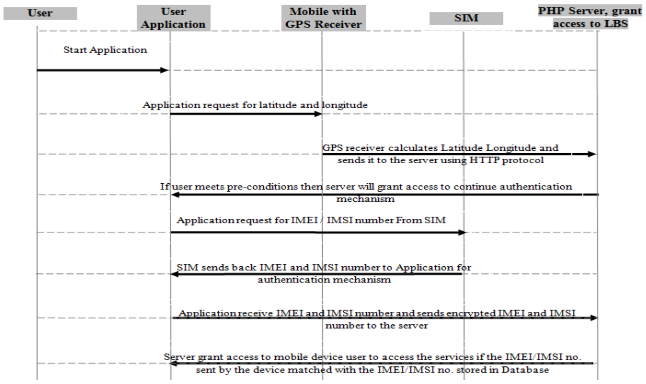
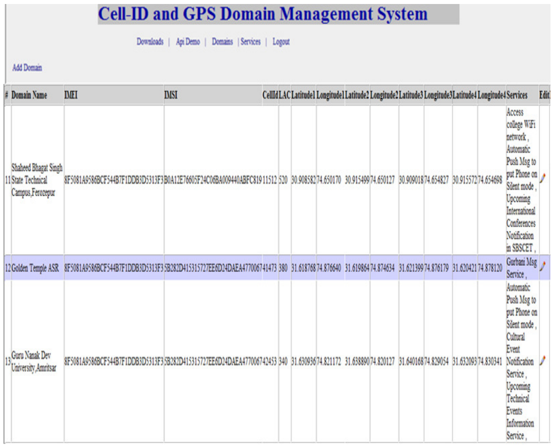

User
User Application
Mobile with GPS Receiver
SIM
PHP Server, grant access to LBS
Start Application
Application request for latitude and longitude
GPS receiver calculates Latitude Longitude and sends it to the server using HTTP protocol
If user meets pre-conditions then server will grant access to continue authentication mechanism
Application request for IMEI / IMSI number From SIM
SIM sends back IMEI and IMSI number to Application for authentication mechanism
Application receive IMEI and IMSI number and sends encrypted IMEI and IMSI number to the server
Server grant access to mobile device user to access the services if the IMEI/IMSI no. sent by the device matched with the IMEI/IMSI no. stored in Database

Figure 4. Flow chart of GPS Based System

Figure 5 shows Cell-ID and GPS Domain Management System. User can edit the information for particular Device, particular Location of user, and Services for users in this Database.



Cell-ID and GPS Domain Management System

Downloads | Api Demo | Domains | Services | Logout

Add Domain

#	Domain Name	IMEI	IMSI	CellId	LAC	Latitude1	Longitude1	Latitude2	Longitude2	Latitude3	Longitude3	Latitude4	Longitude4	Services	Edit
11	Shaheed Bhagat Singh State Technical Campus,Ferozepur	8F5081A9586BCF544B7F1DDB3D5313F3	B0A12E76605F24C06BA009440ABFC819	11512	520	30.908582	74.650170	30.915499	74.650127	30.909018	74.654827	30.915572	74.654698	Access college WiFi network , Automatic Push Msg to put Phone on Silent mode , Upcoming International Conferences Notification in SBSCET ,	✎
12	Golden Temple ASR	8F5081A9586BCF544B7F1DDB3D5313F3	5B282D415315727EE6D24DAEA4770067	41473	380	31.618768	74.876640	31.619864	74.874634	31.621399	74.876179	31.620421	74.878120	Gurbani Msg Service ,	✎
13	Guru Nanak Dev University,Amritsar	8F5081A9586BCF544B7F1DDB3D5313F3	5B282D415315727EE6D24DAEA4770067	42453	340	31.630936	74.821172	31.638890	74.820127	31.640168	74.829054	31.632093	74.830341	Automatic Push Msg to put Phone on Silent mode , Cultural Event Notification Service , Upcoming Technical Events Information Service ,	✎

Figure 5. Database of Authorised Users conataining Nessesary Information

6. ANDROID AND ITS SUPPORT FOR LBS

The Android system is perhaps the most promising candidate of an open platform and operating system for mobile devices beside the iPhone and its SDK. Android is based on the Linux kernel and the application software is written in Java with the help of the Android SDK, a set of development tools which can be seamlessly integrated into the Eclipse IDE via the Android Developer Tools (ADT) plugin. The Android SDK contains two optional APIs and one important class bearing potential reference to LBS. Optional means that a given handset may not support them fully depending on to its hardware features. These APIs are the *Wi-Fi APIs* and the API for Location-Based Services.

The API for LBS is Android’s primary support for building location-based services. It provides the ability to obtain the phone’s location from a location provider such as GPS or A-GPS and is designed to be open for other location based systems which may come online. It contains two packages: android.location for managing such location providers and getting standard – and Reverse Geocoding through the Geocoder class. The other package is com.google.android.maps for drawing and controlling well integrated Google Maps overlays. Accessing and noticing of the phone’s current and possibly changing CellID and other important connection parameters such as data connection state or signal strength is provided by the class android.telephony.PhoneStateListener .Figure 6 shows Android application named MyThesis.

We have created an application that can two alternative options to calculate the position of Mobile device or Mobile Client. The options are Get Latitude Longitude using GPS and Get Cell-ID , LAC using GSM Network. Figure 7 shows transition from GPS Activity to UserDeviceIdentificationActivity. And Figure 8 shows transition from Cell-ID Activity to UserDeviceIdentificationActivity.

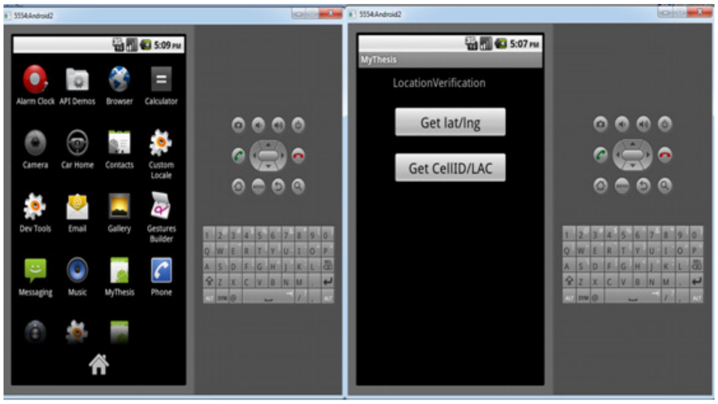
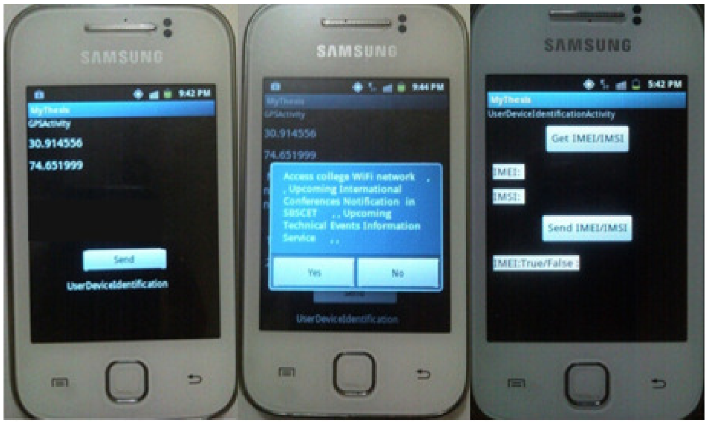


Figure 6. LBS Application(MyThesis)

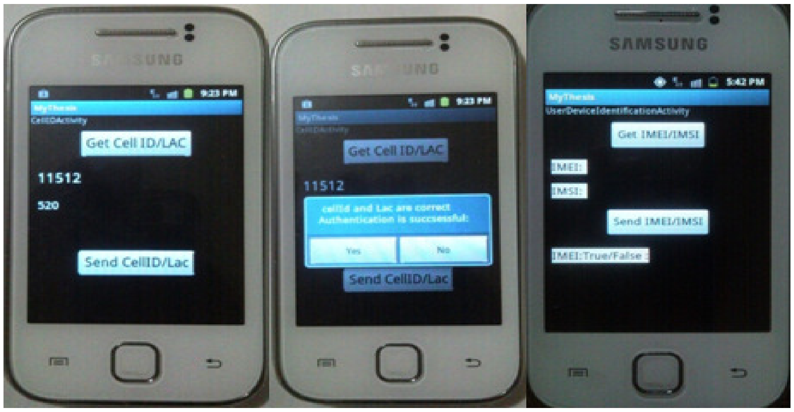


30.914556

74.651999

Access college WiFi network , Upcoming International Conferences Notification in SBSCET , , Upcoming Technical Events Information Service , ,

Figure 7 GPS Activity and UserDeviceIdentification Activity



```
11512
520
```

```
11512
cellId and Lac are correct
Authentication is successful:
```

Figure 8. Cell-ID Activity and UserDeviceIdentification Activity

7. PRIVACY CONCERNS IN LOCATION BASED SERVICES

Location determining technologies will continue to expand in use and it is very important for the technologies to adapt to the technological and social needs, desires, and expectations of users and to the needs of society as a whole. Within the broader domain of tracking technologies, location-based services (LBS) are a subset of capabilities that allow users to access information relative to their own physical location. The personal location information generated by such technologies is at risk of being misused or abused unless protection capabilities are built into the design of such systems [12].

In order for location-based services to function properly, the location of the customer's cellular telephone must be identified. Along with all the benefits and convenience the location based service has provided, there are many privacy issues and concerns regarding this kind of technology.

Information that users used in the location based services is considered as very personal and critical information for many reasons. Users' information included in the location based services consisted with four major components:

- Users' identity information.
- Users' location information - the location coordinates.
- The context of the location based services.

In Authentication Mechanism we have used device's IMEI and IMSI number along with the location information. IMEI and IMSI numbers are unique numbers assigned to the device and subscriber. The necessity for secured mobile terminal identification increases with the growing terminal functionality and applications. It is well known that the current terminal identity IMEI in GSM system is not secure at all, as it is not a verifiable entity. The signalling information element confidentiality feature is the property that a given piece of signalling information which is exchanged between MSs and base stations is not made available or disclosed to unauthorized individuals, entities or processes. The following signalling information elements related to the user are protected whenever used after connection establishment:

- International Mobile Equipment Identity (IMEI);
- International Mobile Subscriber Identity (IMSI);

We have used best encryption algorithm on the bases of comparison of different encryption techniques to protect IMEI and IMSI number. We have proposed a Location Based System in which client device reads the current position of the object using GPS and Cell-ID positioning techniques, the data is sent via GSM/ GPRS service from the GSM network towards a web server using the POST method of the HTTP protocol. In mobile or wireless communication, the air interface is the radio-based communication link between the mobile station and the active base station. In GSM/UMTS, the various UTRA standards are air interfaces, and are also (but not exclusively) referred to as "access modes". Following are the important points that describe the need of confidentiality and authenticity of any user or subscriber.

7.1 Subscriber Identity Authentication

This is basically the authentication of the subscriber identity (IMSI/TMSI) by the network. This property both protects the providers from unauthorized use of their network, and protects the subscribers from communicating with an attacker impersonating an actual subscriber. If an authentication fails the specific MS is denied access to the PLMN.

Cryptography ensures that the message should be sent without any alterations and only the authorized person can be able to open and read the message. A number of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography- Symmetric and Asymmetric. This paper presents a detailed study of most of the symmetric encryption techniques with their advantages and limitations over each other.

8. PROBLEM DESCRIPTION

Cryptography came into existence due to the four fundamental problems exists while communication. They are Security, Authentication, Non Repudiation and Integrity Control. Consider the problem of a person wants to buy service from service provider on the web. User uses some unique numbers that is IMEI and IMSI for authentication. When IMEI and IMSI number is transmitted over the network for LBS then security is a big concern for the buyer. On the other hand the vendor has to be sure that the IMEI and IMSI numbers are of legitimate user. So cryptography plays here a very important role of authenticating the identity of the buyer. Assuming the vendor accepts the transaction, how can they prove that you really did order the item and won’t claim it wasn’t you when the bill comes due? This is the non repudiation problem. Finally after the transaction, how can the vendor and buyer be sure that our communication is not being altered by any malicious interceptor?

Encryption is the process of converting the original plain text into non readable format. There are various encryption techniques exist in the cryptography such as DES, Triple DES, AES etc. But the problem arises in choosing the encryption technique is to select the algorithm with better key length. The second difficulty is to make choice on the implementation of cryptosystem or protocol.

Cryptography is used for securing information stored in mobile devices. Usage time of a mobile device is constrained by its most critical resource – battery. The user must be aware of the energy consumption characteristics of the applications and services he/she uses on the mobile device [13]. Encryption algorithms, which play a main role in information security systems, consume a significant amount of computing resources and battery energy, which are very limited. High energy consumption has a direct impact on the battery life, and, consequently, on the duration and extent of the user's mobility. Thus, the reduction of energy consumption of a portable system is of the primary importance [14].

The design of crypto algorithms typically does not account for physical constraints such as limited battery energy. Therefore, the primary challenge in providing security in mobile devices is minimizing energy consumption and maximizing security [15]. Scalable features such as scalable key establishment protocols and scalable authentication schemes, in which different security, performance and energy trade-offs are enabled for different application scenarios are especially desirable [16].

Here we evaluate cipher strength (the number of bits in the key used to encrypt data) of AES and Rijndael crypto algorithms versus energy consumption in mobile devices aiming to find an energy efficient combination of crypto algorithm parameters for different user application scenarios and energy consumption strategies. As energy consumption awareness is highly important in mobile devices, we must ensure required functionality, data security level and reasonable use of energy at the same time. Empirically we can predict that cryptography with a longer key will ensure higher levels of security at the cost of higher energy consumption.

However, block size also has influence, because larger blocks will require more encryption rounds. Energy consumption also depends on the application scenario, e.g., if the user only encrypts data on a mobile device but decrypts its elsewhere, the energy/cipher strength trade-off will differ from the scenario, when a user encrypts/decrypts data on a mobile device only. Therefore, in order to use crypto algorithms energy-efficiently one needs to understand the relationships between energy consumption and encryption parameters. Once these relationships are understood well then it is possible to optimize energy consumption vs. security requirement or vice-versa.

A conventional encryption scheme has five major parts: Plaintext, Encryption Algorithm, Secret Key, Cipher text, and Decryption Algorithm [17]. In such a scheme, it is essential for secure communication that the sender and receiver have a way to exchange secret keys in a secure manner. Symmetric key encryption is faster than public key encryption since public key encryption places heavier computational load than symmetric key encryption [18]. Examples of commonly used symmetric-key encryption algorithms are: DES (Data Encryption Standard), TripleDES/3-DES, AES/Rijndeal. Table 1 compares these algorithms where AES seems to be the better algorithm. AES supports key sizes of 128 bits, 192 bits, and 256 bits, in contrast to the 56-bit keys offered by DES, a predecessor of AES [17] .

8.1 Brief Definitions Of The Most Common Symmetric Encryption Techniques Are Given As Follows:

8.1.1 DES

(Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size). Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [19].

8.1.2 TDES

TDES is an enhancement of DES. It is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [19].

8.1.3 AES

AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. it encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices [20]. Also, AES has been carefully tested for many security applications.

8.2 Effect of Cryptography Algorithms On Executable File Based On Varying Key Size

The results are carried out using two simulations Androsa FileProtecter. Using this simulations Encryption throughput can be determined.The encryption throughput can be determined by calculating the total plaintext encrypted on total encryption time of various encryption algorithms. Increased throughput results in decrease of power consumption. The results are shown with respect to key size variation.

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. Different packet sizes are used in this experiment for the AES-256, AES-192, AES-128, DES-64 and TDES-192 algorithms.

The encryption time is recorded for all the encryption algorithms. The average data rate is calculated for AES-256, AES-192, AES-128, DES-64 and TDES-192 algorithms based on the recorded data. The formula used for calculating average data rate is

$$AvgTime = \frac{1}{Nb}\sum_{I=1}^{Nb}\frac{Mi}{ti}(Kb/s)$$

Equation1. Average Time of Encryption

Where
AvgTime = Average Data Rate (Kb/s)
Nb = Number of Messages
Mi=Message Size (Kb)
Ti=Time taken to Encrypt Message Mi

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated using the following Formula

$$Throughput = \frac{Tp}{Et}$$

Equation2. Throughput

Tp= Total Plain text
Et= Encryption time
It is very important to calculate the throughput time for the encryption algorithm to known better performance of the algorithm.

Table 1 Time Consumption (Encryption) for .doc files

.doc file	Time in Millisecond				
Input Size(Kb)	AES(256)	AES(192)	AES(128)	DES(64)	TDES(192)
30	32	24	16	28	22
64	61	59	48	66	53
107	110	105	94	115	98
525	180	173	161	185	166
906	300	270	201	310	220
1680	1240	1190	1120	1250	1140
AvgTime	**320.5**	**303.5**	**273.333**	**325.666**	**283.1666**
Throughput	**10.333**	**10.912**	**12.117**	**10.169**	**11.696**

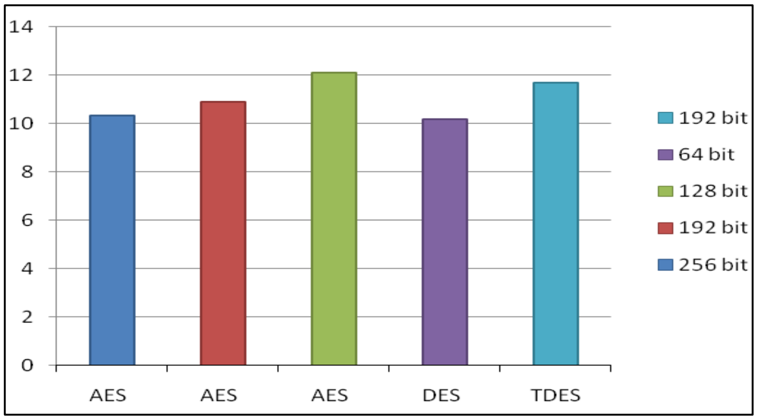


Fig 9.Time Consumption (Encryption) of .doc file

Figure 9 shows the result based on the throughput of the encryption with different packet size. It shows the throughput is high for AES-128 bit when compared to that of AES-256,AES-192,DES-64,TDES. As the throughput value is increased, the power consumption of the encryption technique is decreased. So from the experiment it proves that AES-128 bit encryption algorithm consumes less power for encrypting the .doc file than others.

Table 4 Time Consumption (Encryption) for .pdf files

.pdf file	Time in Millisecond				
Input Size(Kb)	AES(256)	AES(192)	AES(128)	DES(64)	TDES(192)
1057	2590	1960	1660	2250	2010
3043	2980	2580	2050	2670	2300
5283	3930	3540	3240	3680	3390
7915	4850	4500	4180	4620	4350
8819	5860	5300	5100	5770	5240
12071	5790	5320	4820	5650	4980
AvgTime	**4333.333**	**3866.666**	**3508.333**	**4106.666**	**3711.666**
Throughput	**8.812**	**9.876**	**10.884**	**9.299**	**10.288**

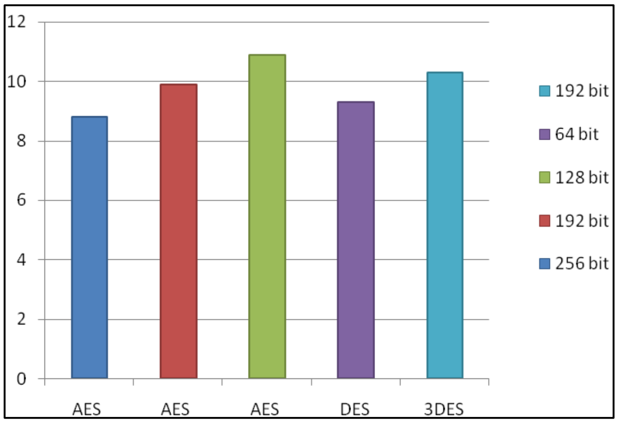


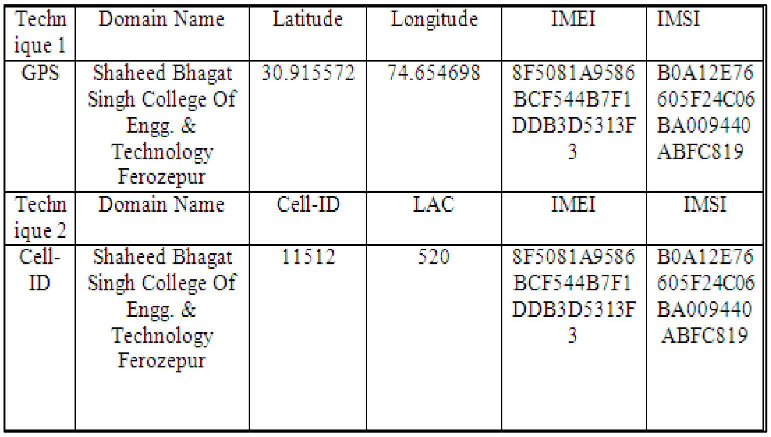
Fig10. Time Consumption (Encryption) of .pdf file

Figure 10 shows the result based on the throughput of the encryption with different packet size. It shows the throughput is high for AES-128 bit when compared to that of AES-256,AES-192,DES-64,TDES. As the throughput value is increased, the power consumption of the encryption technique is decreased. So from the experiment it proves that AES-128 bit encryption algorithm consumes less power for encrypting the .pdf file than others.

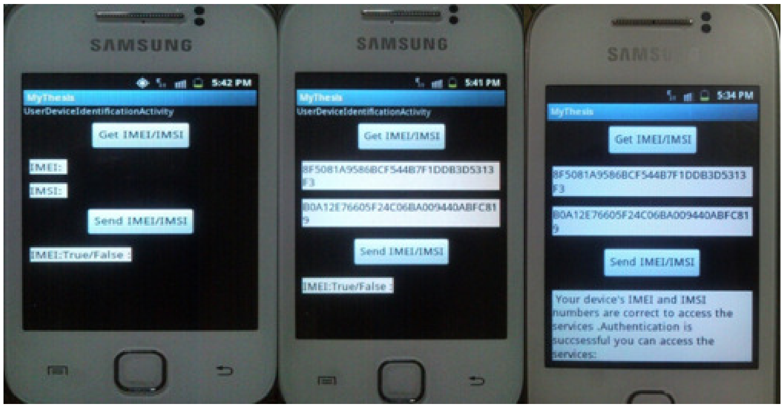
9. RESULTS AFTER APPLYING ENCRYPTION

On the bases of comparison between various techniques we have chosen the best encryption technique. We have applied AES 128 bit encryption algorithm to protect the sensitive information. Figure 10 shows encrypted IMEI number and IMSI number.when we click the button Send IMEI/IMSI, Application will send encrypted IMEI and IMSI number to PHP server using POST method of HTTP protocol and crosschecks this with a list containing authorized IMEI/IMSI number in Database. As we can see in figure 10 that our IMEI/IMSI numbers are valid and application shows a message on mobile screen “Your IMEI and IMSI numbers are correct to access the services. Authentication is successful”.

Table 2 Set of Data Obtained from this Android Application



Technique 1	Domain Name	Latitude	Longitude	IMEI	IMSI
GPS	Shaheed Bhagat Singh College Of Engg. & Technology Ferozepur	30.915572	74.654698	8F5081A9586 BCF544B7F1 DDB3D5313F 3	B0A12E76 605F24C06 BA009440 ABFC819
Technique 2	Domain Name	Cell-ID	LAC	IMEI	IMSI
Cell-ID	Shaheed Bhagat Singh College Of Engg. & Technology Ferozepur	11512	520	8F5081A9586 BCF544B7F1 DDB3D5313F 3	B0A12E76 605F24C06 BA009440 ABFC819



8F5081A9586BCF544B7F1DDB3D5313F3

B0A12E76605F24C06BA009440ABFC819

Your device's IMEI and IMSI numbers are correct to access the services .Authentication is succsessful you can access the services:

Figure 11. UserDeviceIdentification Activity (Encrypted information using AES-128 bit encryption Technique)

10. CONCLUSIONS

This paper proposes an Authentication Mechanism 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 either check GPS coordinates or the Cell ID of the BTS to which the Mobile Device is connected, or both. The server side 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.

We have addressed a problem of security of sensitive information. To protect sensitive information we need best encryption technique because mobile device is constrained by its most critical resource – battery. The user must be aware of the energy consumption characteristics of the applications and services he/she uses on the mobile device. In order to consume less energy and power, it will be better to replace the algorithms that consume more energy, modification in the algorithms and to implement new design of algorithms. On the bases of comparison between various techniques we have chosen the best encryption technique. We have compared two encryption techniques with varying key size that are AES-256, AES-192, AES-128, DES-64 and TDES-192.results obtained are based on the throughput of the encryption with different packet size. It shows that the throughput is high for AES 128 bit when compared to that of AES-256, AES-192, DES-64 and TDES-192. As the throughput value is increased, the power consumption of the encryption technique is decreased. So from the experiment it proves that AES 128 bit encryption algorithm consumes less power for encrypting the text than that of AES.We have applied AES 128 bit encryption algorithm to protect the sensitive information for this android application. Overall it is identified that AES-128 bit can be used in circumstances where there is need for high security and performance aspects.

REFERENCES

[1] Shu Wang, Jungwon Min and Byung K. Yi (2008). Location Based Services for Mobiles:Technologies and Standards, *IEEE International Conference on Communication (ICC) 2008*,Beijing, China

[2] I.K.Adusei, K. Kyamakya and F. Erbas (2004). Location-Based Services: Advances and Challenges. *Canadian Conference on Electrical and Computer Engineering (CCECE).*

[3] Bishop Matt,(2003) "*Computer Security*". Addison-Wesley, August 2003.

[4] Pfleeger, P. Charles and Pfleeger, S., Lawrence. *Security in Computing*. Prentice Hall, 4 editions, 2007.

[5] Albrecht Schmidt(1999), There is more to context than location,computer & Graphics, volume 23,issue 6,December 1999 ,pages 893-901,http://dx.doi.org/10.1016/S0097-8493(99)00120-X,

[6] Roy Want , The Active Badge Location System (1992),Journal ACM Transaction on Information System(TOIS) Volume 10 Issue 1,jan.1992,pages 91-102, ACM New York,NY,USA, doi>10.1145/128756.128759

[7] Mike Hazas1 and AndyWard2, A Novel Broadband Ultrasonic Location SystemIn *Proceedings of UbiComp 2002: Fourth International Conference on Ubiquitous Computing*, Lecture Notes in Computer Science volume 2498, pages 264.280, G¨oteborg, Sweden, September 2002. © Springer-Verlag.

[8] Urs Hengartnera,_, Peter Steenkisteb a David R. " Avoiding privacy violations caused by context-sensitive services" Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada b Departments of Computer Science and Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA Pervasive and Mobile Computing 2 (2006) 427–452

[9] Indrakshi Ray, Mahendra Kumar " Towards a location-based mandatory access control model" Department of Computer Science, Colorado State University, Fort Collins, CO 80523, USA computers & security 25 (2006) 36 – 44

[10] YoungHoon Yu, JiHyeok Kim, Kwangcheol Shin *, Geun Sik Jo " Recommendation system using location-based ontology on wireless internet: An example of collective intelligence by using 'mashup' applications" School of Computer and Information Engineering, Inha University, 253 Yonghyun-dong, Nam-gu, Incheon (402-751), Republic of KoreaExpert Systems with Applications 36 (2009) 11675–11681

[11] Sasivimon Sukaphat " An Implementation of Location-Based Service System with Cell Identifier for Detecting Lost Mobile"Computer Science Program, Faculty of Science, Srinakharinwirot University, Bangkok 10110, Thailan*d* Procedia Computer Science 3 (2011) 949–953

[12] Onsrud, H.J. (2001). "*Contract Approach to Addressing Privacy in the Use of Location Based Services*". Center for Spatially Integrated Social Science: LBS Specialist Meeting, Santa Barbara, CA.

[13] Tiliute D. E. Battery management in wireless sensor networks // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 4(76). – P. 9–12. Baums A. Energy consumption optimization in hard realtime system CMOS processors // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 4(68). – P. 19–22.

[14] Baums A. Energy consumption optimization in hard realtime system CMOS processors // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 4(68). – P. 19–22.

[15] Chandramouli R. Battery power-aware encryption. // ACM Transactions on Information and System Security (TISSEC), 2006. – Vol. 9. – No. 2. – P. 162-180.

[16] Dumčius A., Gužauskas N. Mixed Data Encryption System // Electronics and Electrical Engineering. – Kaunas: Technologija, 2002. – No. 6(41). – P. 12–15.

[17] Joan Daemen, Rijmen Vincent, (1999) "*AES Proposal: Rijndael*", Belgium pp 1-45 csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

[18] Wikipedia, http://www.wekipedia.org.

[19] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks."I BM Journal of Research and Development, May 1994, pp. 243 -250.

[20] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

Authors

Gurjeet Kaur was born in Pehowa, Haryana, on December 1, 1986.Gurjeet kaur received her Bachelor degree *in* Computer Science *and* Engineering from Adesh InstituteOf Engineering & Technology,Punjab,India.Currently she is doing Master's in Computer Science & Engineering from Shaheed Bhagat Singh State Technical Campus,Ferozepur,Punjab,India. Her research interests are inthe area of Telecommunication Networks (GSM–Security),Location Based Services.Miss Gurjeet Kaur is member of UACEE and SDIWC.

Monika Sachdeva has done B.Tech computer science and engineering from National Institute of Technology NIT, Jalandhar in 1997. She finished her MS software systems from BITS Pilani in 2002. Currently she is a PhD student in Department of Computer Science and Engineering from Guru Nanak Dev University, Amritsar,Punjab,India.