ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

SaFe-Tracker: A Privacy System for Continuous Location-Based Services

Athira Mohanan, Archana P.S

M-Tech Student [Cyber Security], Sree Narayana Gurukulam College of Engineering Ernakulam, India

ABSTRACT: In today's fast moving life, services based on location has very much important. Location Tracking is become very popular in the modern era. The Technology is helpful for the parents who wants to be aware of where their children are. Nowadays, the crime and its impact are at its highest pitch and parents concern for their children's safety is undoubtedly true. In this scenario, the children are also not giving a single hand to their parents to ensure their security, so the parent's worries are genuine. Fast moving life services based on location has very much importance in every one's life. As the trend is of smart phones, iphones, tablets etc, it is very important for the mobile user to have the location based services. Location based service can be elaborate as the services which uses the users geographical location which consist of X and Y coordinates, which is generated by GPS which acts as positioning device. In this paper we propose an application that provides options to track the location of second party through their smart phones. The application maintains log file which contains user's current location and update the location to the server with in a unique interval, also that details are store in the data sever in an encrypted manner for the concerned party.

KEYWORDS: GPS; LBS; Location Privacy; Cryptography; Database Security

I. INTRODUCTION

In this modern world, it is very easy for a person to know his/her location with the help of devices having GPS facility. When the user's location is provided to location based services (LBS), it is possible to user to know all location dependent information like location of friends or Nearest Restaurant, whether or traffic conditions. The massive use of mobile devices pave the way for the creation of wireless networks that can be used to exchange information based on locations. When the exchange of location information is done amongst untrusted parties, the privacy of the user could be in harmful. Existing protocol does not work on many different mobile devices and another issue is that, Location Server (LS) should provide misleading data to user. In recent years there has been a dramatic increase in the number of mobile devices querying location servers for information about POIs. Among many challenging barriers to the wide deployment of such application, privacy assurance is a major issue.

Location-based services (LBS) require users to continuously report their location to a potentially untrusted server to obtain services based on their location, which can expose them to privacy risks. Unfortunately, existing privacy-preserving techniques for LBS have several limitations, such as requiring a fully-trusted third party, offering limited privacy guarantees and incurring high communication overhead. Mobile security testing is becoming an urgent and important research subject due to the explosive increase of mobile app downloads and mobile users. Now, location-based function services in mobile apps not only enhance mobile user experience, but also bring new challenges and issues in software testing and data security. This paper focuses on location-based testing issues, attack prevention for mobile apps, and proposes a new tracking and searching model and method to address these needs. Location-based services (LBS) require users to continuously report their location to a potentially untrusted server to obtain services based on their location, which can expose them to privacy risks. Unfortunately, existing privacy- preserving techniques for Location-based services (LBS) have several limitations, such as requiring a fully-trusted third party, offering limited privacy guarantees and incurring high communication overhead. An increased number of intruders in mobile networking make this research a relevant one.

Privacy is a serious security threat that can be extremely harmful to both businesses and consumers in the mobile environment. The location based attack can be performed either using mobile networks or database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to discovering the nearest ATM machine, gas station, hospital, or police station. There are

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

increasing mobile phone users worldwide. So location technologies can be currently used by wireless carrier operators to provide a good forecast of the user location. Now a days, number of users are use location based services which can provide location-aware information. A lot of research has been done on privacy preserving. But no one gave absolute guarantee of user's data and query. Basically when user used specific location based service or registered for that, then LBS can provide number of other services like delivery coupons or other marketing information to customer who is in a specific geographical area. Nowadays, there are number of user takes advantage of location based services and graph is increasing.

II. RELATED WORK

The first solution to the problem was proposed by Beresford [6], in which the privacy of the user is maintained by constantly changing the user's name or pseudonym within some mix-zone. It can be shown that, due to the nature of the data being exchanged between the user and the server, the frequent changing of the user's name provides little protection for the user's privacy. A more recent

Investigation of the mix-zone approach has been applied to road networks [18]. They investigated the required number of users to satisfy the unlinkability property when there are repeated queries over an interval. This requires careful control of how many users are contained within the mix-zone, which is difficult to achieve in practice[13].LBS problems old days introduced in a new method which presents a preliminary investigation on the privacy issues involved in the use of location-based services. It is argued that even if the user identity is not explicitly released to the service provider, the geo-localized history of user-requests can act as a quasi-identifier and may be used to access sensitive information about specific individuals [1].

A complementary technique to the mix-zone approach is based on k-anonymity [3], [2], [5].The concept ofk-anonymity was introduced as a method for preserving privacy when releasing sensitive records [13]. This is achieved by generalization and suppression algorithms to ensure that a record could not be distinguished from (k − 1) other records. The solutions for LBS use a trusted anonymiser to provide anonymity for the location data, such that the location data. As more user information becomes available with the fast growth of Internet applications, e.g., social networks, attackers have the ability to construct users' personal profiles. This gives rise to new challenges and reconsideration of the existing privacy metrics, such as kanonymity. A new metrics to measure users' query privacy taking into account user profiles[2]., However location knowledge is often perceived as personal information. While a number of privacy-preserving models and algorithms have taken shape in the past few years, there is an almost universal need to specify one's privacy requirement without understanding its implications on the service quality[14].Location-based queries are quickly becoming ubiquitous. However, traditional search engines perform poorly for a significant fraction of location-based queries, which are nonfactual (i.e., subjective, relative, or multidimensional). As an alternative, we investigate the feasibility of answering location-based queries by crowd sourcing over Twitter. More specifically, they developed the effectiveness of employing location-based services (such as Foursquare) for finding appropriate people to answer a given location-based query. Findings give insights for the feasibility of this approach and highlight some research challenges in social search engines[10].

An important privacy issue in location based services (LBS) is to hide a user's identity and location while still providing quality location based services. A user's identity can be easily hidden through anonymous Web browsing services. However, a user's location can reveal a user's identity. Also, they argue that ensuring the server does not reveal more data than what is queried is important at the same time. They propose an efficient two-level solution based on two cryptographic protocols: PIR and oblivious transfer. Our solution is a general-purpose one and can use either a two-level PIR [2] or it can use a combination of PIR and oblivious transfer. Their approach provides privacy for the user/client, does not use a trusted party or anonymizer, is provably privacy-preserving, and when compared to previous approaches ensures that the server reveals as minimum data as is required, and the data that is released by the server is as fine-grained or precise as possible[9].

Another method for avoiding the use of a trusted anonymiser is to use 'dummy' locations [7], [11]. The basic idea is to confuse the location of the user by sending many random other locations to the server, such that the server cannot distinguish the actual location from the fake locations.

This incurs both processing and communication overhead for the user device. The user has to randomly choose a set of fake locations as well as transmitting them over a network, wasting bandwidth. We refer the interested reader to Krumm [13]. Existing protocol method, Oblivious Transfer Phase purpose of this protocol is for the user to obtain one and only one record from the cell in the public grid P, shown in Fig. 4. We achieve this by constructing a 2-dimensional

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

oblivious transfer, based on the ElGamal oblivious transfer [21], using adaptive oblivious transfer proposed by Naor et al. [22]. Generally speaking, PIR schemes allow a user to retrieve data (bit or block) from a database, without disclosing the index of the data to be retrieved to the database server [20]. Ghinita et al. used a variant of PIR which is based on the quadratic residuosity problem [23].

This idea was extended to provide database protection [7][11], [13]. This protocol consists of two stages. In the first stage, the user and server use homomorphic encryption to allow the user to privately determine whether his/her location is contained within a cell, without disclosing his/her coordinates to the server. In the second stage, PIR is used to retrieve the data contained within the appropriate cell. So that the encryption scheme used for the data base security by the Diffi-Hellman schema [4]with public key cryptosystem. Finally the year of 2014 continuous location based problems and encryption security also challenge in modern mobile world. Finally new problem in LBS that Only a few privacy-preserving techniques have been proposed for continuous LBS [15], [13][14]. These techniques rely on a TTP to continuously expand a cloaked area to include the initially assigned k users. These techniques not only inherit the drawbacks of the TTP model, but they also have other limitations. (1) Inefficiency. Continuously expanding cloaked areas substantially increases the query processing overhead. (2) Privacy leakage. Since the database server receives a set of consecutive cloaked areas of a user at different timestamps, the correlation among the cloaked areas would provide useful information for inferring the user's location. (3) Service termination. A user has to terminate the service when users initially assigned to her cloaked area leave the system.

III. PROPOSED SYSTEM

This work is designed for the parents and children/ women safety purpose. Both must have a smart phone that supports the GPS and internet. We proposed a solution intend to develop an application which tracks the mobiles location and also search the location zones. SaFe-Tracker, as the word expansion indicates it includes that the mobile tracking application for the Mobile devices with the help of GPS/internet technology.

A. *System Architecture of SaFe-Tracker:*

The proposed architecture avoided the trusted third party server. So that it is help to overcome limitations of the existing privacy preserving techniques for LBS, such as requiring a fully-trusted third party, offering limited privacy guarantees and incurring high communication overhead. The, safe-tracker will update each of tracking location of the currents users in a limited interval. A continuous range query is defined as keeping track of the POIs within a user specified distance range of the user's current location (xu, yu) for a certain time period. That location details are also encrypted (latitude and longitude of location details and digits) by the help of SHA-1.

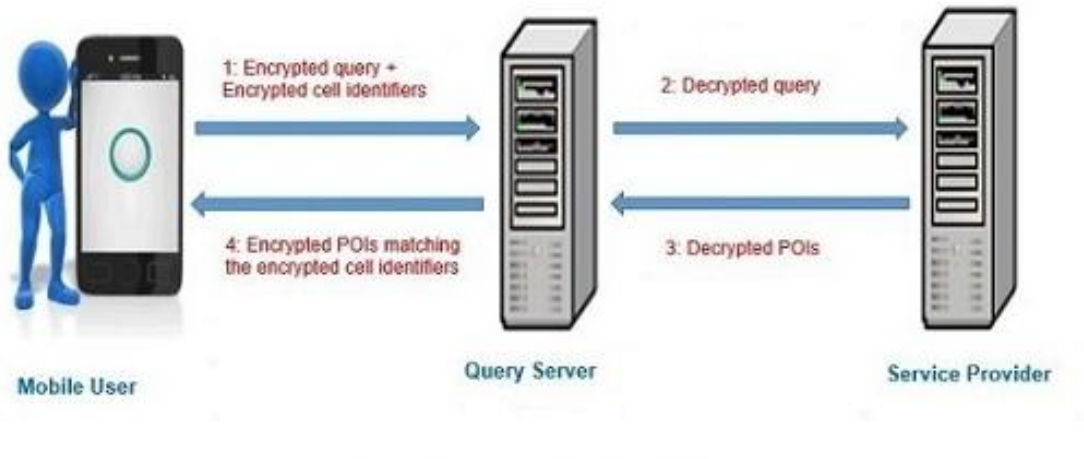

Fig.1. System Architecture of SaFe-Tracker

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

The SaFe-Tracker system consists of:

- The mobile User
- Query server (Qs)
- Service provider (sp).

First the mobile user acts as a user interface for the LBS. The user (parent/child) side which acts as a server for the system but actually it is not a server. The mobile user basically uses a smart phone owned by either the parent or the child. By using this app a general mobile user can track any person such as child, an elder, a friend, women or a neighbour etc. GPS /internet services to be enabled in the mobile user's phone for the app functioning.

The purpose of the query server (QS) is to establish and maintain the communication between the location server/ mobile service provider (SP) and the mobile user. Query server (QS) also performs the role of a data base server.

- app execution steps:

Step1. Install application.
Step2. Sign up {new user registration)
Step3. Enter username, password, email id and phone number
Step4. Sign in
Step5. Select the option to search location or else tracking
Step6. If tracking is set then add the tracking device phone number
Step7. The application checks for updates from the GPS at regular intervals
Step8. If the current location view is shown in the map (tracking person map plotting)
Step9. If the current location updates we need to see then showing the grid view (list of location name, time, date)
Step10. Storing the data to could server/database server and exit.

For communicating between mobile user and query server we propose a new protocol called SaFe-Tracker Protocol. The detailed explanation of this protocol is given in the next section.

B. *SaFe-Tracker Protocol:*

The SaFe-Tracker protocol using the encryption and decryption methods together, it helps to achieve the secure cryptosystem features. The high level overview of the SaFe-Tracker protocol is shown in fig.2.

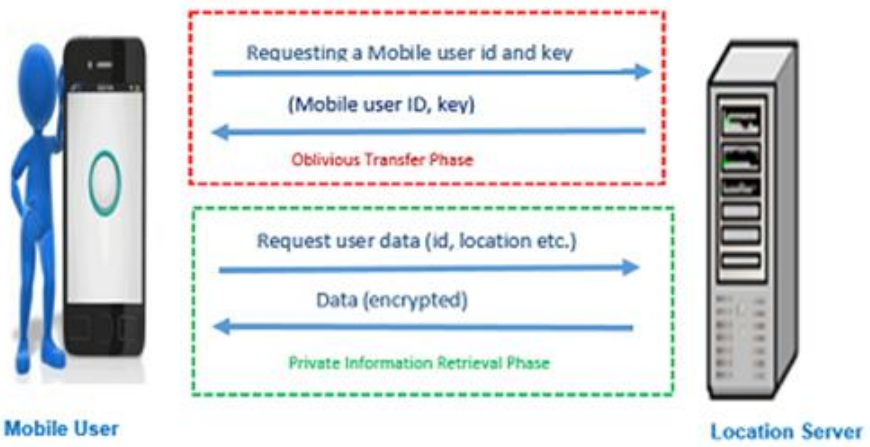

Fig.2. High Level Overview of the SaFe-Tracker Protocol

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

This protocol is organized as two stages. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR (Private Information Retrieval phase), to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage.

The proposed Protocol method consists of following stages:

- Prior to first stage: Initialization phase run by the Server.
- First stage (Oblivious transfer phase): User determines his location and owner's cell-ID and symmetric key.
- Second stage (Private Information Retrieval phase): User executes PIR, retrieve the appropriate block in the private grid. Then the user can decrypt corresponding private info using symmetric key.

IV. SECURITY FEATURES AND ADVANTAGES

The various security features and advantages of our SaFe-Tracker app is discussed in this section.

A. *SaFe-Tracker app Security Features:*

- The application maintains a log file which is sent (via mail) to the concerned party for which all days they were tracked (showing the users that day records).
- The application will ask to the concerned party to fill the details like concerned party contact details, email id, mobile number, username and password etc, at the time of user registration.
- The application is hidden to the end user (eg child), so the user will not be able to see the application and it keeps on working at the background.
- User entering into this application is given an option for connecting to the database so as to verify the location updates. Information is then delivered at the right time in the right place to the right person.
- This application provides facility to installing and uninstalling the application in android device through pass codes only. The installation pass code (eg is â000â) and un- installation pass code (eg â111â).
- When there are the absence of GPS/internet service provider, generates the easy way to track the location of the second party by sending hidden code/location via SMS

B. *Advantages of SaFe-Tracker:*

- Data will be encrypted and stored in the data base server with the symmetric key encryption schema with the SHA-1 algorithm.
- The app can trace single/multiple user at same time and also can search the locations.
- Helps to plot the location map view and location list view.

V. SIMULATION RESULTS

The SaFe-Tracker project is implemented in the Android (lolipop-google nexus4) and JAVA(web)language with the support of the could-platform and SQL. The usability of this system is simpler so that authentication will not be a burden anymore. The time taken to obtain the result after the scanning process is much lower so entire process can be finished within limited time. The latest growing technology can easily adopt such integrated authentication methods.

When the project is getting executed, it is redirect firstly to the home page. It contains username, password, login and sign-up these for options for the user to access the application. This home page includes the options for getting a new user account, to download the smart phone application, to get login into the system. The process of application mainly starts from here and its shown in Fig.3.

When the home page displayed, then the user need to do the sign up/in to use the app. First the user is a new one, he/she must need to register their details like username, password, and mobile no and email id etc. After completion of registration, user can sign-in and perform next stage.(shown in Fig.4)User can enter his username and password in order to login in to his home page. After successful login, he/she will be redirected to his/her own home page which contains the location textbox and Enter tracking person's mobile number.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

After successful login, he/she will be redirected to his/her own home page which contains the location textbox and Enter tracking persons mobile number. When we putting the PLUS(+) symbol button its will redirect to the tracking persons location details, shown in Fig.5

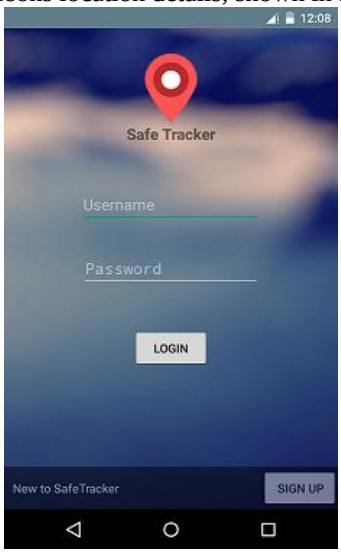

Fig.3. Home Page of SaFe-Tracker.

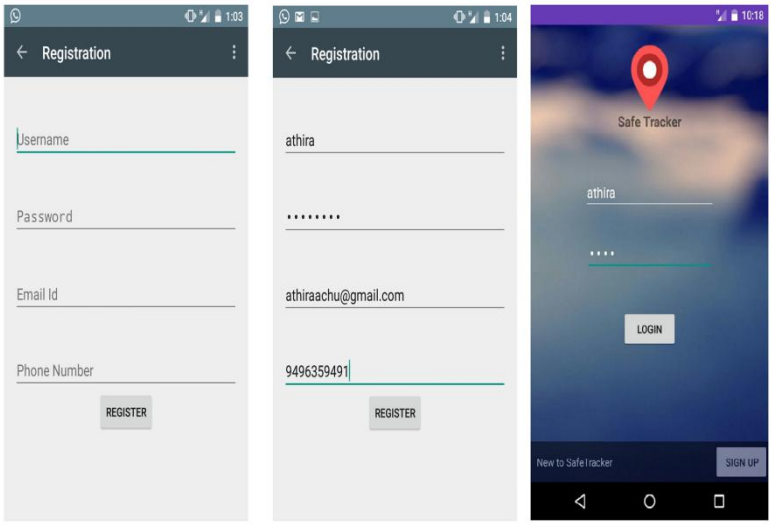

Fig.4. SaFe-Tracker New User Sign-up and Sign-in.

After Tracking it provides to plot the location map view and location list view. The primary objective of our app system is to track the person and plot the location on real time system like Google map (shown in fig.6)

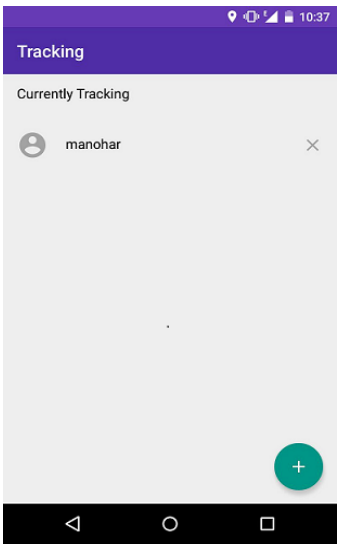

Fig.5. SaFe-Tracker User Tracking.

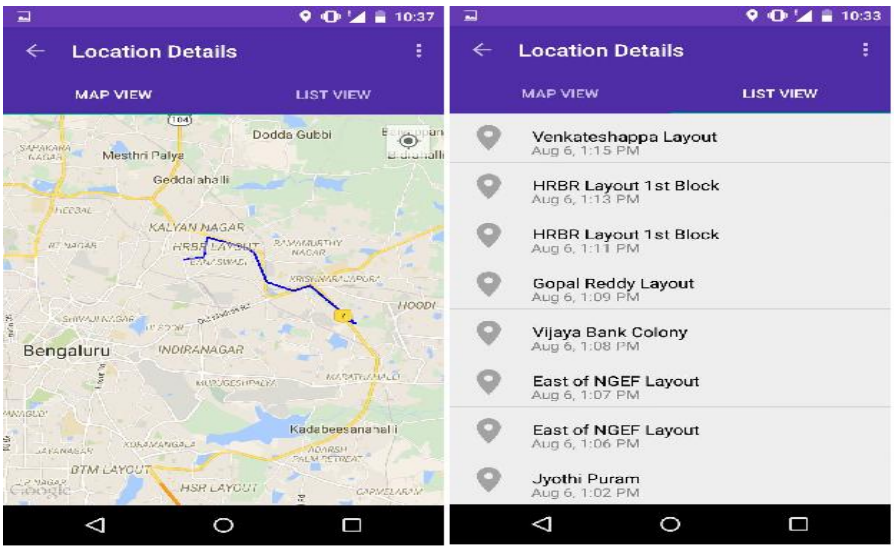

Fig.6. SaFe-Tracker Location Tracking(Map/grid view).

VI. CONCLUSION AND FUTURE WORK

The aim of the SaFe-Tracker app is to develop a low cost solution for GPS based SaFe tracking system. This SaFe-Tracker app can apply to various domains of the industrial and personal use just by using the very common mean, for example mobile with android enabled. It successfully implemented and provides a simple layout for ensuring the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

user (eg: childs/women) safety all the while he/she is by his/her own. The main objective of the system is to track the current location of the person which has an android enabled mobile by extracting the longitude and latitude of that target person. The primary objective of our system is to track the person and plot the location on real time system like Google map. Location-based services need high security, so this SaFe-Tracker app is best suitable for continuous LBS. As an extension to this work, we can develop the SaFe-Tracker app for ios, Microsoft and Blackberry.

REFERENCES

1. C.Bettini,X.Wang And S.Jajodia, "Protecting Privacy Against Location Based Personal Identification", in Proc. 2nd VDLB Int. Conf. SDM, W.Jonker and M. Petkovic, Eds.Trondheim, Norway, 2005
2. X. Chen and J. Pang, "Measuring Query Privacy in Location-Based Services",2nd ACM CODASPY, San Antonio, TX, USA,1, 2012
3. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private InformationRetrieval", J. ACM, vol. 45, no. 6, pp. 965981, 1998
4. T. ElGamal, " A Public Key Cryptosystem And a Signature Scheme Basedon Discrete Logarithms ",IEEE Trans. Inform. Theory, vol. 31, no. 4,pp. 469472, Jul, 2005
5. C. Gentry and Z. Ramzan, "Single-database Private Information RetrievalWith Constant Communication Rate ", ICALP, L. Caires, G. Italiano,L. Monteiro, C. Palamidessi, and M. Yung, Eds., Lisbon, Portugal, pp.803815, LNCS 3580, 2005
6. A. Beresford and F. Stajano, "Location privacy in pervasive computing,"IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar.2003.
7. Jianliang Xu, Xueyan Tang, Haibo Hu and Jing Du, " Privacy-ConsciousLocation-Based Queries in Mobile Environments", Parallel and DistributedSystems, IEEE Transactions on, Volume: 21, Issue: 3 Pages:313 - 326, DOI: 10.1109/TPDS.2009.65, 2010.
8. Goncalves M, Torres D and Perera G, " Making RecommendationsUsing Location-Based Skyline Queries", Database and Expert SystemsApplications (DEXA), 2012 23rd International Workshop on , DOI:10.1109/DEXA.2012.44, 2012.
9. Vishwanathan R and Yan Huang, "A Two-Level Protocol to Answer PrivateLocation-Based Queries", GeoInformatica, vol. 15, no. 14, pp. 128,2009.
10. 10] Bulut M.F, Yilmaz, Y.S and Demirbas M, "Crowdsourcing Location Based Queries ", Pervasive Computing and Communications Workshops(PERCOM Workshops), IEEE International Conference, 2011.
11. Swapnil Ramesh Jadhav, "A Survey on Privacy Preserving and ContentProtecting Location Based Queries",IJRITCC, 2014.
12. Elabd E and Hacid, "Concurrent Queries in Location Based Services",IEEE, Reliability and Security (ARES), Ninth International Conferenceon, 2014.
13. Russell Paulet,Md. Golam Kaosar, Xun Yi, and Elisa Bertino, "Privacy-Preserving and Content-Protecting Location Based Queries ", Conf. Computerand Comm. Security,IEEE , 2014.
14. Dewri and Thurimella, " Exploiting Service Similarity for Privacy inLocation-Based Search Queries", Parallel and Distributed Systems, IEEETransactions, 2014.
15. Roman Schlegel, Chi-Yin Chow, Qiong Huang and Duncan S, " User-Defined Privacy Grid System for Continuous Location-Based Services ",DOI 10.1109/TMC.2388488, IEEE Transactions on Mobile Computing ,2015.
16. A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "ProvidingKanonymity in Location Based Services", SIGKDD Explor. Newsl., vol.12,pp. 310y, 2010.
17. U.S. Census Bureau, "TIGER", http://www.census.gov/geo/www/tiger.
18. B. Palanisamy and L. Liu, "MobiMix: Protecting location privacywith mix-zones over road networks," in Proc. ICDE, Hannover,Germany, 2011, pp. 494–505.
19. Android Developers, developer.android.com/training/basics.
20. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Privateinformation retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998.
21. M. Bellare and S. Micali, "Non-interactive oblivious transfer andapplications," in Proc. CRYPTO, 1990, pp. 547–557.
22. M. Naor and B. Pinkas, "Oblivious transfer with adaptivequeries," in Proc. CRYPTO, vol. 1666, Santa Barbara, CA, USA,1999, pp. 791–791.
23. E. Kushilevitz and R. Ostrovsky, "Replication is not needed:Single database, computationally-private information retrieval,"in Proc. FOCS, Miami Beach, FL, USA, 1997, pp. 364–373.
24. (2011, Jul. 7) Openssl [Online]. Available:http://www.openssl.org/
25. V. Shoup, (2011, Jul. 7). Number thoery library [Online]. Available:http://www.shoup.net/ntl/