Securing Privacy and Content Using Android Location Based Queries

Mr.C.Rajmohan, Iswarya V, Logeswari S, Nivetha M, Padmashree C

Department of Information Technology, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India

Abstract:

The privacy preserving and content-protecting method are used as a solution to one of the location-based query problems. The problem are: a user wants to query a database of a particular location's data, known as Points Of Interest (POI), and does not want to reveal his/her location to the server due to privacy ;the location server of the data, does not want to distribute their data to all the users. The location server desires to have some control over its data, since the data is its asset. Previous solutions have used a trusted anonymiser to address privacy, but introduced the impracticality of trusting a third party. More recent solutions have used homomorphic encryption to remove this weakness. Briefly,the user submits his/her encrypted coordinates to the server and the server would determine the user's location homomorphically, and then the user would acquire the corresponding record using Private Information Retrieval techniques. We propose a major enhancement upon this result by introducing a similar two stage approach, where the homomorphic comparison step is replaced with Oblivious Transfer to achieve a more secure solution for both parties. The solution we present is efficient and practical in many scenarios. We also include the results of a working prototype to illustrate the efficiency of our protocol.[2] The Android testing framework, an integral part of the development environment, provides an architecture and powerful tools that help you test every aspect of your application at every level from unit to framework.

1 INTRODUCTION

A Location based service (LBS) is an information service generally accessed by mobile devices such as, mobile phones, GPS devices and operating through a mobile network. A LBS can offer many services to the users based on the geographical position of their mobile device. The services provided by the LBS are typically based on a point of interest database[1]. The user can get response for LBQ by retrieving the point of interest(POI) from the database server. The number of mobile devices querying location servers for information about POIs has been increased in past few years. Among many challenging barriers for such application, privacy assurance for the end-user is a major issue[19]. For instance, users may feel hesitant to disclose their locations to the LBS, because it may be possible for a location server to learn who is making a certain query by linking these locations with a residential phone book database, since users are likely to perform many queries from home.

During the process of transmission the users should not be allowed to discover any information for which they have not paid. It is thus crucial that the solutions to be devised the address and the privacy of the users issuing queries, but also prevent users from accessing content to which they do not have authorization[16]. A novel protocol is proposed for the LBS. our protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid.It contains ID and associated symmetric key for the cipher block of data in the private grid. In the second stage, the user executes an efficient PIR , to retrieve the appropriate cipher block data in the private grid.Then it is decrypted using symmetric key.

2.RESEARCH METHOD

The LBS are based on two users such as:(i)user who request for location data;(ii) the location server(LS) who fetch the POI from the database.

1.Requirement Definition

Analyzes based on similar application and determines the necessary features in the application to be included.Features that are needed for user as are follows:

a.User Register

The registration form is used for the user registration through which the user can get accessed to the service provided by the LBS.The user register the information to get logged-in.The information of the users are stored by the admin.

b.Log-in Method

The user can log-in using the username and password that are registered in the user registeration. It allows the user to access the service using the username and password.

c.Add-Detail

The category for the location data will be provided for the user in the list and user can select the category for which the data are needed.

d.Category Details

The details of the selected category should be provided to locate the location of that place. The POI of a particular user is based on the location and descriptions that are provided by the user.

2.System and Software design

System design is the process of planning a new system to complement or altogether replace the old system. The purpose of the design phase is the first step in moving from the problem domain to the solution domain. The design of the system is the critical aspect that affects the quality of the software. System design is also called top-level design. The design phase translates the logical aspects of the system into physical aspects of the system.

The users in our model use some location-based service provided by the location server *LS*. Each record describes a POI, giving GPS coordinates to its location (*xgps, ygps*), and a description or name about what is at the location.[12] We assume that the mobile service provider *SP* does not interfere with the communications between the user and the location server. This means that the mobile service provider does not collude with the location server to attack the privacy of the user.

As a consequence of this assumption, the user is able to either use GPS (Global Positioning System) or the mobile service provider to acquire his/her coordinates. Since we are assuming that the mobile service provider *SP* is trusted to maintain the connection, we consider only two possible adversaries. One for each communication direction.

We consider the case in which the user is the adversary and tries to obtain more than he/she is allowed. Next we consider the case in which the location server *LS* is the adversary, and tries to uniquely associate a user with a grid coordinate.

a.Global initialisation

A user *u* from the set of users *U* initiates the protocol process by deciding a suitable square cloaking region CR, which contains his/her location.[5] All user queries will be with respect to this cloaking region. The user also decides on the accuracy of this cloaking region by how many cells are contained within it, which is at least the minimum size defined by the server.

b. Input design

Input design is one of the most important phases of the system design. Input design is the process where the input received in the system are planned and designed, so as to get necessary information from the user, eliminating the information that is not required[17]. The aim of the input design is to ensure the maximum possible levels of accuracy and also ensures that the input is accessible that understood by the user.

The input design is the part of overall system design, which requires very careful attention. If the data going into the system is incorrect then the processing and output will magnify the errors.

c.Output design

The output design is the most important and direct source of information to the user. The encoding time and file size for both the fractal as well as fast fractal technique are shown in output screen. The comparison of both techniques is done and the PSNR value is calculated. The reconstructed image is also displayed in the output screen.

Output from the computer system is required to communicate the result of processing to the user and to provide permanent copy of these results for later consultation. While designing the output, the type of output format, frequency etc has been taken into consideration. Output designed to simply generate an output of the process whether it was successful or not.

3.Implementation and unit testing

Implementation is the process of converting a new or revised system design into an operational one. The implementation is the final and important phase. It involves ser training, system testing and successfully running of developed proposed system. The user tests the developed system and changes are made according to their needs. The testing phase involves the testing of developed system using various kinds of data.

An elaborate testing of data is prepared and the system is tested using that test data. The corrections are also noted for future use. The users are trained to operate the developed system. Both the hardware and software securities are made to run the developed system successfully in future.Education of user should really have taken place much earlier in the project when they were being involved in the investigation and design work[18]. Training has to be given to the user regarding the new system.

Unit testing is the testing of an individual unit or group of related units. It falls under the class of white box testing. It is often done by the programmer to test that the unit he/she has implemented is producing expected output against given input.

4.Integeration and System testing

System testing is the testing to ensure that by putting the software in different environments (e.g., Operating Systems) it still works. System testing is done with full system implementation and environment. It falls under the class of black box testing.

When the individual components are working correctly and meeting the specified objectives, they are combined into a working system[21]. This integration is planned and co-coordinated so that when a failure occurs, there is some idea of what caused it.

In addition, the order in which components are tested, affects the choice of test cases and tools. This test strategy explains why and how the components are combined to test the working system. It affects not only the integration timing and coding order, but also the cost and thoroughness of the testing.

a.Bottom-up Integration

One popular approach for merging components to the larger system is bottom-up testing. When this method is used, each component at the lowest level of the system hierarchy is tested individually[21]. Then, the next components to be tested are those that call the previously tested ones. This approach is followed repeatedly until all components are included in the testing.

Bottom-up method is useful when many of the low-level components are general-purpose utility routines that are invoked often by others, when the design is object-oriented or when the system is integrated using a large number of stand-alone reused components.

b.Top-down Integration

Many developers prefer to use a top-down approach, which in many ways is the reverse of bottom-up. The top level, usually one controlling component, is tested by itself. Then, all components called by the tested components are combined and tested as a larger unit. This approach is reapplied until all components are incorporated.

A component being tested may call another that is not yet tested, so we write a **stub,** a special-purpose program to stimulate the activity of the missing component. The stub answers the calling sequence and passes back the output data that lets the testing process continue.

For example, if a component is called to calculate the next available address but that component is not yet tested, then a stub is created for it, that may pass back a fixed address which allows only testing to proceed. As with drivers, stubs need not be complex or logically complete.

c.Big-bang Integration

When all components are tested in isolation, it is tempting to mix them together as the final system and see if it works the first time. Many programmers use the big-bang approach for small systems, but it is not practical for large ones.

In fact, since big-bang testing has several disadvantages, it is not recommended for any system. First, it requires both stubs and drives to test the independent components. Second, because all components are merged at once, it is difficult to find the cause of any failure. Finally, interface faults cannot be distinguished easily from other types of faults.

5.Android Testing

The Android testing framework, an integral part of the development environment, provides an architecture and powerful tools that help you test every aspect of your application at every level from unit to framework.

The testing framework has these key features:

i).Android test suites are based on JUnit. You can use plain JUnit to test a class that doesn't call the Android API, or Android's JUnit extensions to test Android components. If you're new to Android testing, you can start with general-purpose test case classes such as AndroidTestCase and then go on to use more sophisticated classes.

ii).The Android JUnit extensions provide component-specific test case classes. These classes provide helper methods for creating mock objects and methods that help you control the lifecycle of a component.

iii).Test suites are contained in test packages that are similar to main application packages, so you don't need to learn a new set of tools or techniques for designing and building tests.

iv).The SDK tools for building and tests are available in Eclipse with ADT, and also in command-line form for use with other IDEs. These tools get information from the project of the application under test and use this information to automatically create the build files, manifest file, and directory structure for the test package. v).The SDK also provides monkeyrunner, an API for testing devices with Python programs, and UI/Application Exerciser Monkey, a command-line tool for stress-testing UIs by sending pseudo-random events to a device.

This document describes the fundamentals of the Android testing framework, including the structure of tests, the APIs that you use to develop tests, and the tools that you use to run tests and view results. The document assumes you have a basic knowledge of Android application programming and JUnit testing methodology.

a.Active testing and Service testing

Activity testing is particularly dependent on the Android instrumentation framework. Unlike other components, activities have a complex lifecycle based on callback methods; these can't be invoked directly except by instrumentation. Also, the only way to send events to the user interface from a program is through instrumentation.

This document describes how to test activities using instrumentation and other test facilities. The document assumes you have already read testing fundamentals, the introduction to the Android testing and instrumentation framework.

The activity testing API base class is Instrumentation testcase, which provides instrumentation to the test case subclasses you use for Activities.

For activity testing, this base class provides these functions:

i).Lifecycle control: With instrumentation, you can start the activity under test, pause it, and destroy it, using methods provided by the test case classes.

ii).Dependency injection: Instrumentation allows you to create mock system objects such as Contexts or Applications and use them to run the activity under test. This helps you control the test environment and isolate it from production systems. You can also set up customized Intents and start an activity with them. iii).User interface interaction: You use instrumentation to send keystrokes or touch events directly to the UI of the activity under test.

Service Testing

Android provides a testing framework for Service objects that can run them in isolation and provides mock objects. The test case class for Service objects is Servicetestcase. Since the Service class assumes that it is separate from its clients, you can test a Service object without using instrumentation.

This document describes techniques for testing Service objects. If you aren't familiar with the Service class, please read the services document. If you aren't familiar with Android testing, please read testing fundamentals, the introduction to the Android testing and instrumentation framework.

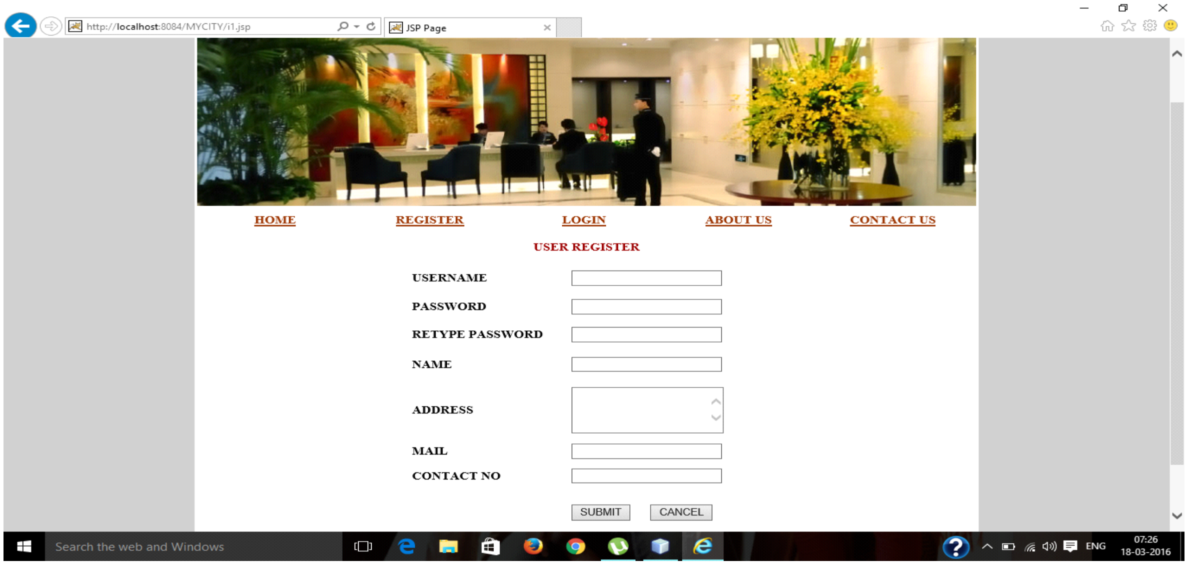
6.operation and maintenance

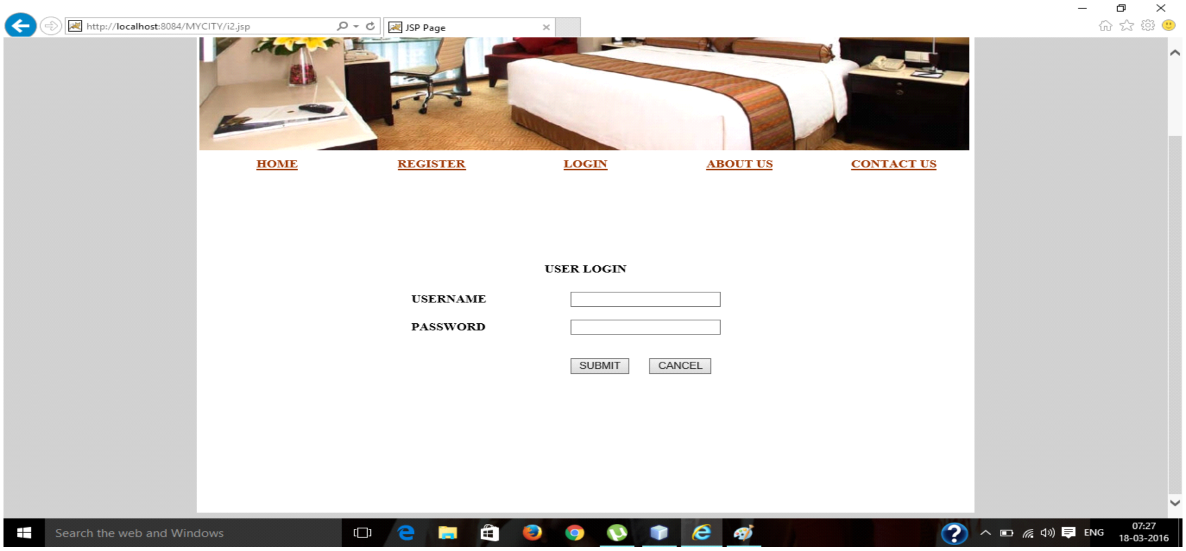
After doing integration into one whole system, if there is any changes or reparations needed then the previous phases can be back.

3. EXPECTED RESULTS

3.1 Application Screenshot

Below are several screenshots of location based service that are provided for user as web application.



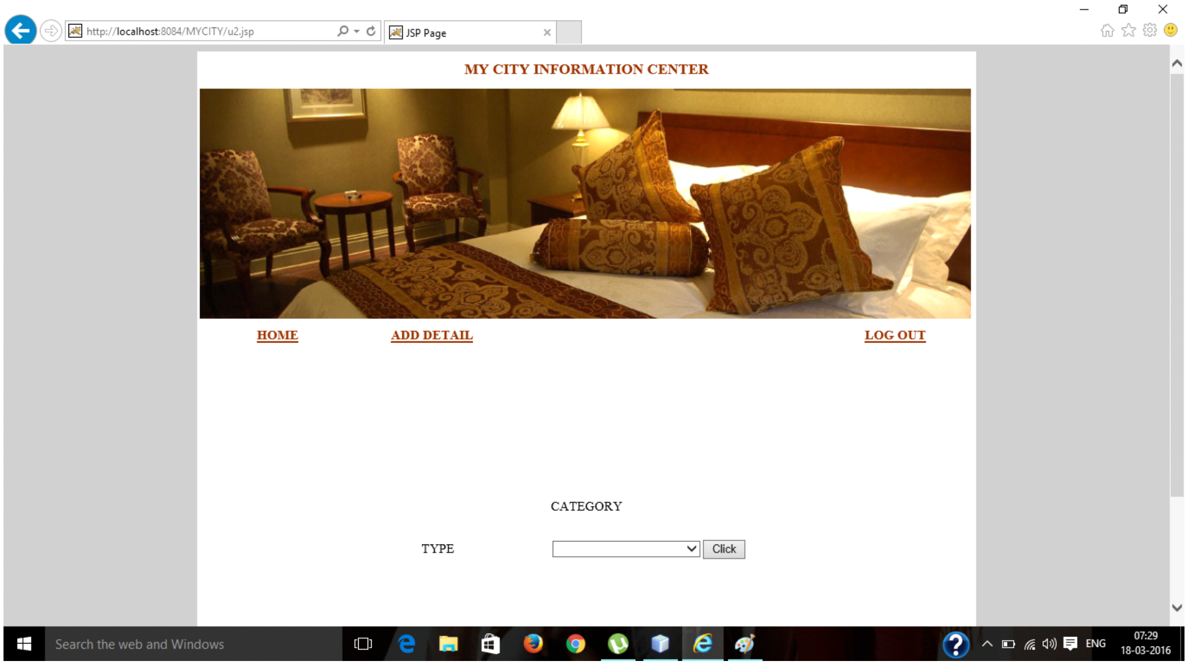


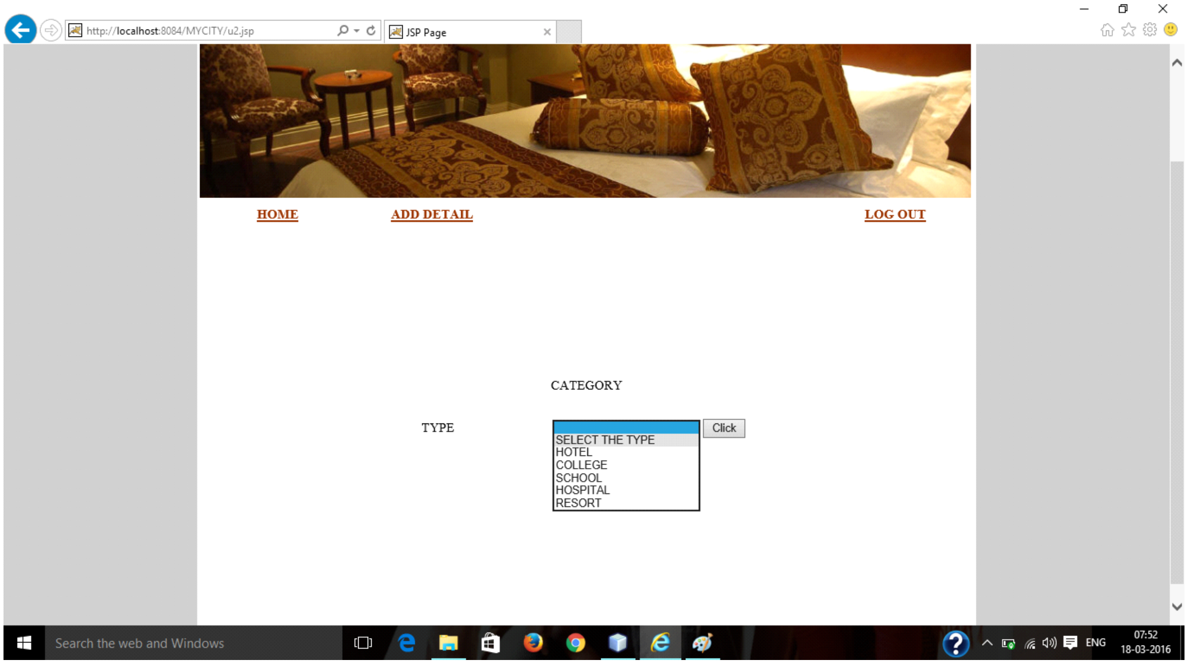
The registration form is used for the user registration through which the user can get accessed to the service provided by the LBS.The user register the information to get logged-in.The information of the users are stored by the admin.

The user can log-in using the username and password that are registered in the user registeration. It allows the user to access the service using the username and password.

3.2 Categories of Locations

The user can add location to their POI database by selecting the categories and adding the data information about that particular location.


http://localhost:8084/MYCITY/u2.jsp
JSP Page
MY CITY INFORMATION CENTER
HOME
ADD DETAIL
LOG OUT
CATEGORY
TYPE
Click
Search the web and Windows
ENG
07:29
18-03-2016

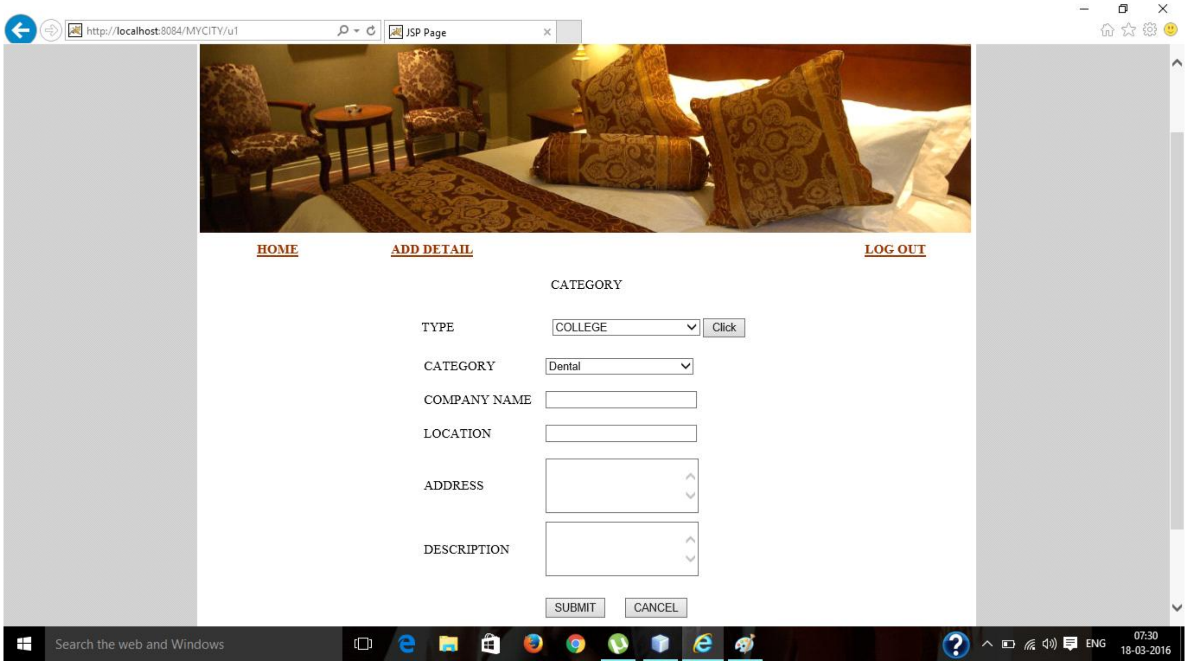

http://localhost:8084/MYCITY/u2.jsp

JSP Page

CATEGORY

TYPE

SELECT THE TYPE
HOTEL
COLLEGE
SCHOOL
HOSPITAL
RESORT


http://localhost:8084/MYCITY/u1

JSP Page

CATEGORY

TYPE: COLLEGE

CATEGORY: Dental

COMPANY NAME

LOCATION

ADDRESS

DESCRIPTION

After the categories were selected by the user, the type of location i.e, for example the college category consists of types like medical,dental,engineering,arts etc....,. Then the description for the location will be provided by the admin and while the location address is given, the lattitude and longitude of the location will be generated. the location can be viewed through using mobile devices.

4.CONCLUSIONS AND SUGGESTIONS

4.1 conclusions

The Location based Service(LBS) provides the user with the POI database from the database server and are retrieved by the location server using the novel protocol to protect the location data as well as the user's location infiormation, although, the location server(LS) tracks the transformation of location data, the users loaction cannot be found by other devices. The privacy of the user and the location data are preserved by using cryptographic method to avoid data loss.

4.2 suggestions

Future work will involve testing the protocol on many different mobile devices. The mobile result we provide may be different than other mobile devices and software environments. Also, we need to reduce the overhead of the primality test used in the private information retrieval based protocol. Additionally, the problem concerning the LS supplying misleading data to the client is also interesting. Privacy preserving reputation techniques seem a suitable approach to address such problem. A possible solution could integrate methods. Once suitable strong solutions exist for the general case, they can be easily integrated into our approach.

5.REFERENCES

[1] (2011, Jul. 7) *Openssl* [Online]. Available: http://www.openssl.org/
[2] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," in *Proc. CRYPTO*, 1990, pp. 547–557.
[3] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.
[4] 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, pp. 185–199, LNCS 3674.
[5] X. Chen and J. Pang, "Measuring query privacy in location-based services," in *Proc. 2nd ACM CODASPY*, San Antonio, TX, USA, 2012, pp. 49–60.
[6] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *J. ACM*, vol. 45, no. 6, pp. 965–981, 1998.
[7] M. Damiani, E. Bertino, and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations," *Trans. Data Privacy*, vol. 3, no. 2, pp. 123–148, 2010.
[8] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proc. 3rd Int. Conf. Pervasive Comput.*, H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp.
243–251, LNCS 3468.
[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.
[10] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proc. ICDCS*, Columbus, OH, USA, 2005, pp. 620–629.
[11] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in *Proc. ICALP*, L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung , Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.
[12] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in *Proc. Adv. Spatial Temporal Databases*, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644.
[13] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," *GeoInformatica*, vol. 15, no. 14, pp. 1–28, 2010.
[14] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in *Proc. ACM SIGMOD*, Vancouver, BC, Canada, 2008,pp.121-132
[15] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacypreserving matching of spatial datasets with protection against background knowledge," in *Proc. 18th SIGSPATIAL Int. Conf. GIS* , 2010, pp. 3–12.
[16] M. Gruteser and D. Grunwald, "Anonymous usage of locationbased services through spatial and temporal cloaking," in *Proc.1st Int. Conf. MobiSys*, 2003, pp. 31–42.

[17] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," in *Proc. 9th Int. Conf. UbiComp*, Innsbruck, Austria, 2007, pp. 372–390.
[18] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in *Proc. 1st Int. Conf. SecureComm*, 2005, pp. 194–205.
[19] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries,"*IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 12, pp. 1719–1733,Dec. 2007.
[20] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proc. Int. Conf. ICPS*, 2005, pp. 88–97.
[21] J. Krumm, "A survey of computational location privacy," *Pers Ubiquitous Comput.*, vol. 13, no. 6, pp. 391–399, Aug. 2009.
[22] 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.
[23] L. Marconi, R. Pietro, B. Crispo, and M. Conti, "Time warp: How time affects privacy in LBSs," in *Proc. ICICS*, Barcelona, Spain,2010, pp. 325–339.
[24] S. Mascetti and C. Bettini, "A comparison of spatial generalization algorithms for lbs privacy preservation," in *Proc. Int. Mobile Data Manage.*, Mannheim, Germany, 2007, pp. 258–262.
[25] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in *Proc. VLDB*, Seoul, Korea, 2006, pp. 763–774.
[26] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in *Proc. CRYPTO*, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791–791.
[27] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. EUROCRYPT*, vol. 1592, Prague, Czech Republic, 1999, pp. 223–238.
[28] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino, "Privacypreserving and content-protecting location based queries," in *Proc. ICDE*, Washington, DC, USA, 2012, pp. 44–53.

BIOGRAPHIES

C.Rajmohan received the **M.Tech** degree in Information Technology from the Manonmaniam Sundaranar University, Tirunelveli, India. Currently doing **Ph.D** in Anna University, India. His research interest includes wireless communication Data mining, Soft Computing

C.Padmashree Currently doing **B.Tech.** in Information Technology in Sri Ramakrishna Engineering College,Coimbatore, India.

V.Iswarya Currently doing **B.Tech.** in Information Technology in Sri Ramakrishna Engineering College, Coimbatore, India.

S.Logeswari Currently doing **B.Tech.** in Information Technology in Sri Ramakrishna Engineering College, Coimbatore, India.

M.Nivetha Currently doing **B.Tech.** in Information Technology in Sri Ramakrishna Engineering College, Coimbatore, India.