PRIVACY PROTECTION IN LOCATION-BASED SERVICES THROUGH A PUBLIC-KEY PRIVACY HOMOMORPHISM

Asst.Prof. Girish Kumar.D[1], Sneha Raman.T[2], Vinayashree.P[3], Sushmitha.V.Shetty[4]
Dept. of Computer Science, BITM College, Ballari, Karnataka, India

Abstract: Location-Based Services (LBS) can be accessed from a variety of mobile devices to obtain value added information related to the location of the user. Most of the times, these services are provided by a trusted company like a telecommunications company. However, the massive use of mobile devices form a strong way for the creation of ad hoc wireless networks that can be used to exchange information based on locations. In the latter case, these LBS could be provided by an untrusted party. Sending the location to an untrusted LBS provider could put the privacy of the user in to danger. In this topic we propose a original technique to guarantee the privacy of users of LBS. Our technique consists of several modules, but the highest degree of security is achieved thanks to the use of a public-key privacy homomorphism. Unlike the existing approaches, our proposal does not need any trusted third party to anonymise the users and only makes use of a public-key infrastructure.

I. INTRODUCTION

Location-Based Services (LBS) allow users to receive highly personalised information. These services can be accessed by using a variety of mobile devices that can utilise a plethora of localisation technologies. Mobile devices have become ubiquitous and services related to the current position of the users are growing fast. Some examples of these LBS are tourist information service, router planners, emergency assistance, etc. For a given user of LBS, sending her location could put her privacy in jeopardy. An LBS basically consists of an LBS provider delivering location-based in- formation and a set of users asking for this information. Mobile devices have a variety of ways for determining their approximate location. Thus, we assume in this paper that the utilised devices have this capability (i.e. they can determine their longitude and latitude). In this scenario, a user u asks the LBS provider P for some information by sending in the form of message {IDu,query,long,lat}. Upon this request, P seeks the desired information in its database and returns an appropriate answer to u. Note that, if u sends her exact location to an untrusted LBS provider Pu, it can misbehave because it can relate the real location 'longitude, latitude' with the unique identifier of u, IDu, for instance: (i) Pu is able to know if u is in front of certain shops or places, so it can flood her with undesired advertisements; (ii) Pu can track u so it knows where she has been and when; (iii) Pu can send the identifier of u along with her location to a spammer, and the later can send undesired location-based advertisements to the user.

II. EASE OF USE

2.1 Purpose of Document

This paper gives an overview about how existing solution make use of the K-Anonymity algorithm for the Privacy Protection. In this kind of solutions Mobile device will get his nearby companion's location though Bluetooth and then with this location, he will calculate a centroid. The centroid is sent to LBS for location based advertisements. By doing in this way LBS will not know exact location of the user, only it knows approximate location, so LBS services are not affected and user privacy is protected.

2.2 Scope for development of this paper

Any Mobile user who collects companion location, may leak the exact location, in that case privacy is compromised. When mobile user requests for companion location, each companion encrypts his location information using Homomorphic encryption and send to mobile user. Mobile user also encrypts his location information using Homomorphic encryption, which may provide the privacy to the user data.

2.3 Modules of the system

A. LBS

LBS: Location based services (LBS) are services offered through a mobile phone and take into account the device's geographical location. LBS typically provide information or entertainment.

B. LOCATION COLECTOR

Location Collector: this module receives the location request from the companion and centroid is calculated

C. CENTROID CALCULATOR

Centriod calculator: Centroid is calculated using encrypted locations and then value is decrypted to get actual centroid.

D.MOBILE USER

Mobile User: when mobile user requests for companion location, each companion encrypts his location information using Homomorphic encryption and send to mobile user. Mobile user also encrypts his location information using Homomorphic encryption.

2.4 Existing System

Existing solution is based K-Anonymity based Privacy Protection. In this solution. Mobile device will get his nearby companion's location though Bluetooth and then with this location, he will calculate a centroid. The centroid is sent to LBS for location based advertisements. By this way
LBS will not know exact location, only it knows approximate, so LBS services are not affected and user privacy is protected.

2.5 Limitations of Existing system

If the Mobile user who collects companion location leaks the exact locations then the privacy is not provided.

2.6 Proposed System with Benefits

In this proposed solution, when mobile user requests for companion location, each companion encrypts his location information using Homomorphic encryption and send to mobile user. Mobile user also encrypts his location information using Homomorphic encryption. Centroid is calculated using encrypted locations and then value is decrypted to get actual centroid. In this way privacy is protected even if mobile user leaks the companion location.

III. SYSTEM REQUIREMENTS AND SPECIFICATIONS

3.1 Functional Requirements

Functional Requirement defines a function of a software system and how the system must behave when presented with specific inputs or conditions. These may include calculations, data manipulation and processing and other specific functionality. In this system following are the functional requirements:-

- Send advertise request
- Send location request to companion
- Calculate centroid
- View advertise response

Non Functional Requirements

Non functional requirements are the requirements which are not directly concerned with the specific function delivered by the system. They specify the criteria that can be used to judge the operation of a system rather than specific behaviors. They may relate to emergent system properties such as reliability, response time and store occupancy. Non functional requirements arise through the user needs, because of budget constraints, organizational policies, the need for interoperability with other software and hardware systems or because of external factors such as:-

1. Product Requirements
2. Organizational Requirements
3. User Requirements
4. Basic Operational Requirements

3.2.1 Product Requirements

Portability: Since the software is developed in java it can be executed on any platform for which the JVM is available with minor or no modifications.

Correctness: It followed a well-defined set of procedures and rules to compute and also rigorous testing is performed to confirm the correctness of the data.

Ease of Use: The front end is designed in such a way that it provides an interface which allows the user to interact in an easy manner.

Modularity: The complete product is broken up into many modules and well-defined interfaces are developed to explore the benefit of flexibility of the product.

Robustness: This software is being developed in such a way that the over all performance is optimized and the user can expect the results within a limited time with utmost relevancy and correctness. Java itself possesses the feature of robustness, which implies the failure of the system is negligible.

3.2.2 Organizational Requirements

Process Standards: IEEE standards are used to develop the application which is the standard used by the most of the standard software developers all over the world.

Design Methods: Design is one of the important stages in the software engineering process. This stage is the first step in moving from problem to the solution domain. In other words, starting with what is needed design takes us to work how to satisfy the needs.

The design of the system is perhaps the most critical factor affecting the quality of the software and has a major impact on the later phases, particularly testing and maintenance. We have to design the product with the standards which has been understood by the developers of the team.

3.2.3 User Requirements

- The user must be able to visualize Graphical User Interface Window.
- The user must be able to configure all the parameters with neat GUI.

3.2.4 Basic Operational Requirements

The customers are those that perform the eight primary functions of systems engineering, with special emphasis on the operator as the key customer. Operational requirements will define the basic need and, at a minimum, will be related to these following points:-

Mission profile or scenario: It describes about the procedures used to accomplish mission objective. It also finds out the effectiveness or efficiency of the system.

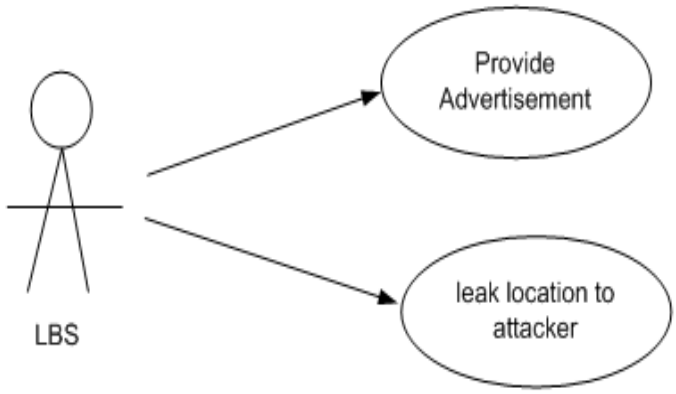
Performance and related parameters: It points out the critical system parameters to accomplish the mission

Utilization environments: It gives a brief outline of system usage. Finds out appropriate environments for effective system operation.

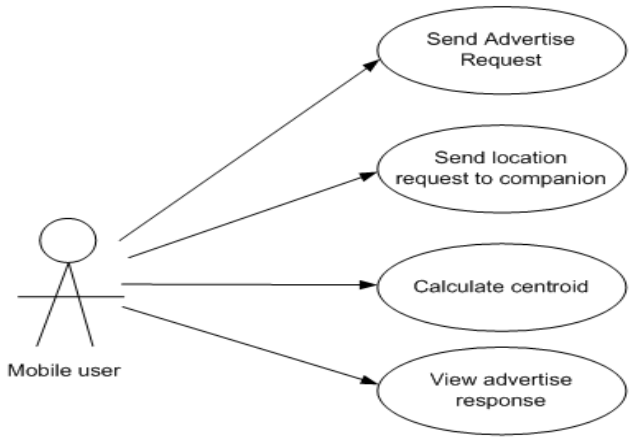
Operational life cycle: It defines the system lifetime.

IV. SYSTEM DESIGN

4.1 Use Case Diagram

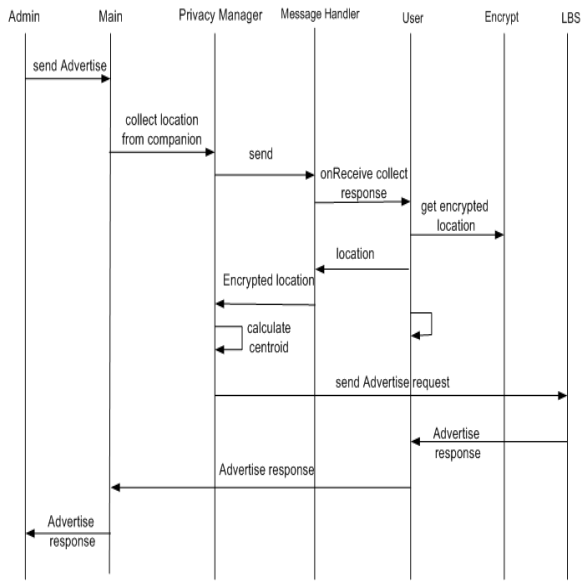


Use Case Diagram for LBS

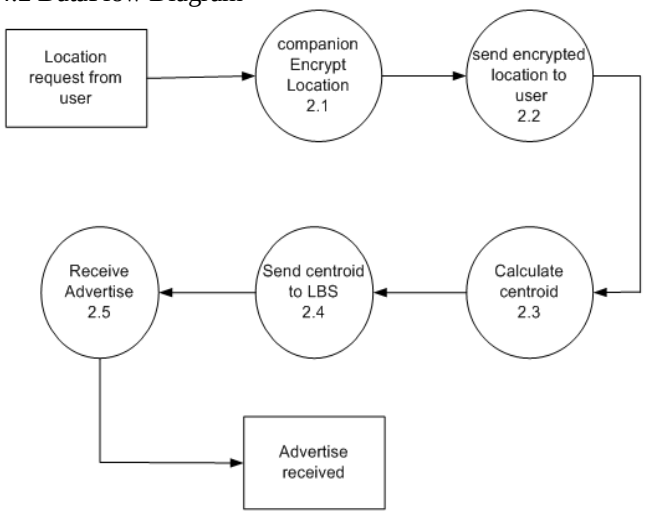


Use Case Diagram for Mobile User

4.2 Sequence Diagram



4.2 DataFlow Diagram



V. CONCLUSION

Our project is based on a public-key privacy homomorphism it averts the use of a trusted third party. Our method relies on a basic scheme, consisting in the computation of the average location of a set of k users, and improves it in the sense that it guarantees the location privacy of the users and the location exchange among them by using a public-key privacy homomorphism. Proposed algorithm solves the privacy aspects related to LBS.

Future work includes improving the proposed method to allow static users to take part in several anonymity procedures and studying different collusion scenarios, with more than one user colluded with the LBS provider.

REFERENCES

[1] Domingo-Ferrer, J., Seb´e, F., Solanas, A.: A polynomial-time approximation to op- timal multivariate microaggregation. In: Computer and Mathematics with Applica- tions (in press, 2007)

[2] Gedik, B., Liu, L.: A Customizable k-Anonymity Model for Protecting Location Privacy (2004)

[3] Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In: Proceedings of the First International Confer- ence on Mobile Systems, Applications, and Services, pp. 31–42 (2003)

[4] Mokbel, M.F.: Towards Privacy-Aware Location-Based Database Servers. Interna- tional Workshop on Privacy Data Management, PDM (April 2006)

[5] Okamoto, T., Uchiyama, S.: A new public-key cryptosystem as secure as factoring. Lecture notes in computer science, pp. 308–318

[6] Bertino, E., Cheng, R., Zhang, Y., Prabhakar, S.: Preserving user location privacy in mobile data management infrastructures. In: Proceedings of Privacy Enhancing Technology Workshop (PET) (2006)

