ISSN 2395-1621

Effect on Location Privacy Preservation Level by Time varying Population Density

[#1]Nawale Prajakta P., [#2]Kolekar Rutumbhara B., [#3]Saptarshi Priyanka S.
[#4]Alhat Shubhangi B.

[1]prajakta2194@gmail.com
[2]rutumbarakolekar1992@gmail.com
[3]priyanka103.saptarshi@gmail.com
[4]shubatul5@gmail.com

[#1234]Student, Department of Computer Engineering
BSIOTR, Wagholi, Pune

ABSTRACT

We evaluated the impact of the time-varying distribution of population density on location based service level in an experiment. We used a people flow data set of the user generated area to obtain the time-varying distribution of population density and user location. The results demonstrate that the adversary is able to estimate user locations more correctly and more confidently by considering the time-varying distribution of population density. We also found a problem in terms of large dispersion of the location privacy preservation level between regions. We also provide the Location based service to user requested in case of emergency like, if someone request for the nearest mall, hospital etc., that also we provide to the user. A location privacy preservation level criterion is difficult to satisfy. By the simulation results, Considering the time-varying distribution of population density is effective for estimation of user location and degrading the performance of location privacy preservation mechanisms.

Keywords: **Location based query, LBS, population density, time-varying distribution, K-nearest.**

ARTICLE INFO

Article History

Received: 2nd December 2016

Received in revised form :

2nd December 2016

Accepted: 5th December 2016

Published online :

5th December 2016

I. INTRODUCTION

Location-based systems are rapidly used in modern society by mobile device with positioning system (GPS) receivers. Location based service (LBS) provides different services based on users' locations, e.g., local searches, route navigation, and location-based social networks. In participatory sensing systems, a large number of people send sensing data with their location information. In order to use these kinds of services, the users have to transmit geographical information such as latitude and longitude coordinates to the LBS providers. Personal information, such as home, workplace, behaviour pattern, and health state, is easily inferred from the location information. We defined location privacy as the ability to prevent other parties from learning one's current or past location. In order to use LBSs safely, a mechanism to preserve location privacy without degrading the quality of services as much as possible is required. Location based services (LBS) form a large class of applications in modern day mobile systems.

These applications utilize the positioning capabilities of a mobile device to determine the current location of the user.

Project Objective:

1. This system becomes automated calculating the location details.
2. Increased adulteration in consumables can be prevented.
3. Cost effective approach, Time saving approach.
4. This system helps to maintain the data properly.
5. This system is very accurate, simple and low power consumption, which is used for the real time applications.

II. LITERATURE SURVEY

"Local differential perturbations: Location privacy under approximate knowledge attackers", In this paper method based on location to address such adversaries. Different methodology used Location privacy, differential privacy, query approximations. [1]

"Identifying important places in people's lives from cellular network data", he proposes a new algorithm to identify important locations. We test this algorithm on arbitrary cellphone users, including those with low call rates, and find that we are within 3 miles of ground truth for 88% of volunteer users. Further, after locating home and work, he achieve commute distance estimate that are within 1 mile of equivalent estimates derived from government census data. Finally, he perform carbon footprint analyses on hundreds of thousands of anonymous users as an example of how data and algorithms can form an accurate and efficient underpinning for policy and infrastructure studies.[2]

"Privacy-Preserving and Content-Protecting Location Based Queries", he propose a major enhancement upon previous solutions by introducing a two stage approach, where the first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties. The solution he present is efficient and practical in many scenarios. he implement our solution on a desktop machine and a mobile device to assess the efficiency of our protocol. he also introduce a security model and analyse the security in the context of our protocol. Finally, he highlight a security weakness of previous work and present a solution to overcome it.[3]

"Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey" this paper surveyed the state-of-the-art in cryptography-based solutions for achieving privacy-preservation in LBS services. Specifically, he categorized current research into three groups, based on the trust assumptions between parties involved in LBS schemes. [4]

"Pseudo-Location Up-dating System for Privacy-Preserving Location-Based Services" he proposed a privacy-preserving system, called 3PLUS, which was TTP-free, and improved users' location privacy by employing a pseudo-location updating scheme for LBSs. By following three steps, buffer initialization, pseudo-locations swapping and pseudo-locations uploading, users can achieve k-anonymity to protect their location privacy.[5]

III. EXISTING SYSTEM

In a straight-forward setup, location-based services have many trust assumptions amongst the involved parties. However, some of the parties may be honest while still being interested in learning confidential information, and others can have reasons to cheat where possible. We proposed Location-based services or LBS refer to a set of applications services in order to provide services based on that information. They also open a new area for developers and service providers to develop and provide value-added services: advising clients of nearest hospital, hotel, helping the users to find nearby shopping malls.

IV. PROPOSED SYSTEM

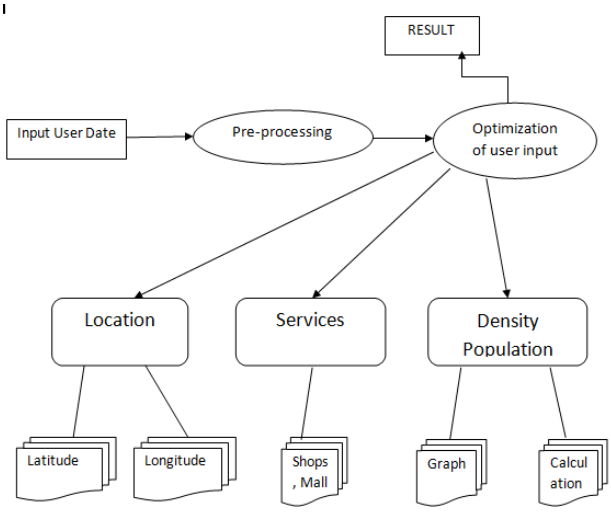

Fig 1. System architecture

Modules: -

User Module:
User can authorize login access. He can update all personal information. He also cans authority to send request to admin for getting the LBS service in case of emergency.

LBS:

LBS is the providing the services for requesting the user which are stored the server.

Admin Module:

Admin is the authorized person, he check all the user activity records as well as profile. He also send the services info to user.

V. ALGORITHM

1. K-anonymity Algorithm

It is the One approach for protecting the identity of individuals when releasing or sharing sensitive location related data is to anonymize it. A popular approach for data anonymization is k-anonymity. The most common implementations of k-anonymity use transformation

techniques such as generalization, global recoding, and suppression. A relation is said to satisfy k-Anonymity property if every count in the frequency set is greater than or equal to k.

• Database – a table with n rows (records) and m columns (attributes)

• Alphabet of a Database (£) – the range of values that individual cells in the database can take.

•Suppression – can replace individual attributes with a *

• Generalization – replace individual attributes with a broader category

2. Obfuscation Method

This method is used to hide the information about user's location .
This technique deliberately degrades the quality of user's location for protection purpose.
It performs slightly altering, substituting or generalizing location to avoid reflection of user's original position.

VI. CONCLUSION

By above experimental evaluation time varying distribution of population density is effective method for estimation of user location. Location privacy preservation mechanism is not enough able to maintain the privacy of user's location. We evaluated the dispersion of the location privacy preservation level between regions, the uncertainty of estimating user location, and the correlation coefficient between the location privacy preservation level and population density.

REFERENCES

[1] R. Dewri, “Local differential perturbations: Location privacy under ap-proximate knowledge attackers,”Mobile Computing, IEEE Transactions on, vol. 12, no. 12, pp. 2360–2372, 2013.

[2] S. Isaacman, R. Becker, R. C´ aceres, S. Kobourov, M. Martonosi, J. Rowland, and A. Varshavsky, “Identifying important places in people’s lives from cellular network data,” in Pervasive computing. Springer, 2011, pp. 133–151.

[3] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino, ”Privacy-Preserving and Content-Protecting Location Based Queries,” ieee trans-actions on knowledge and data engineering, may 2014.

[4] Emmanouil Magkos, ”Cryptographic Approaches for Privacy Preser-vation in Location-Based Services: A Survey,” International Journal of Information Technologies and Systems Approach, 2011.

[5] NIU Ben, ZHU Xiaoyan, CHI Haotian, LI Hui, ”Pseudo-Location Up-dating System for Privacy-Preserving Location-Based Services,” National Key Laboratory of Integrated Networks Services, Xidian University, Xian 710071, China.

