SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 251–257

ISSN No: 2454-9614

Identification of Fake Location Based Service Providers Using Secure Abstraction of Top-K Query Processing

P. Shyamala, D. Deepa*

Department Of information technology, Bannari Amman Institute of Technology, Sathyamangalam , Tamilnadu, India.

*Corresponding Author: P. Shyamala

E-mail: shyamala.se14@bitsathy.ac.in

Received: 10/11/2015, Revised: 13/12/2015 and Accepted: 07/03/2016

Abstract

A novel distributed system for cooperative location based information generation and sharing is predicated on the expansion of net capable and position aware mobile devices and permits the mobile users to share with others their expertise with all types of points of interests (POI). The target is to get a much better understanding of the user and neutral needs associated with secure location sharing systems, as well as the expectations, concerns, rights and obligations of the person being placed. To contribute the general public dialogue regarding location privacy, it introduces security in social location based services and placement sharing systems can forestall abuse and build a positive awareness in society concerning location based services. The situation based mostly information generation and sharing for distributed system allows a secure process that allows the users to verify credibility and correctness of the question result for untrusted location exploitation novel schemes. The power to search out the geographical location of the mobile device and supply services supported that location information by Location chase services that square measure supported different parties chase the user's location and Position aware services that suppose the device's information of its own location.

Reviewed by **ICETSET'16** *organizing committee*

1. Introduction

Location based services provider measure services offered through a mobile phone and take under consideration the device's location. LBS generally give info or diversion. As a result of LBS measure for the most part of the mobile user's location, the target of the service provider's system is to see wherever the user is. To specify the mobile user's location, one methodology involves mistreatment the mobile phone network, the present cell ID will be used for distinctive the bottom transceiver station that the phone is human action with. Once that's determined, the sole issue left is to purpose the placement of the BTS. Alternative systems use GPS satellites. This methodology proves correct than the mentioned and square measure currently created easier by sensible phones.

The abstraction computing is to understand it's usually declared potential across disciplines geographic informatics must convey a transparent image of GIS and connected technologies square measure smart for. This image should concentrate on information contents and user queries, instead of on information formats (raster and vector) and system commands, which dominate the present image of GIS. It ought to be a worth proposition that's across application domains, like reducing all abstract information. Similarly, abstraction analysis reduces abstraction information basically to merchandise of random purpose processes. Within the absence of a transparent however image of abstraction info and computing, several potential users still believe that GIS is primarily accustomed build and store maps.

2. Problem Statement

This work is most identified with information outsourcing, for which it can just review representative schemes because of space constraints. The system of information outsourcing was initially presented, in which an information proprietor outsources its information to an outsider administration supplier who is responsible of noting the information inquiries from either the information proprietor or different clients. As a rule, there are two security concerns in information outsourcing: information protection and question integrity. A bucketization methodology was proposed, to empower proficient reach inquiries over scrambled information, which was recently enhanced and the novel systems for multidimensional extent inquiries over encoded information.

First, individual LBSPs regularly have little information sets including POI audits. This would to a great extent influence the helpfulness and in the long run impede the more common utilization of spatial top-k question administrations. A main purpose behind restricted information sets at individual LBSPs is that individuals tend to leave surveys for the same POI at one or at most just a couple LBSPs' sites which they frequently visit.

Second, LBSPs may alter their information sets by deleting a few surveys or including fake audits and return customized inquiry results for the eateries that are willing to pay or against those that decline to pay. Regardless of the possibility that LBSPs are not pernicious, they may return unfaithful question results affected by different assaults, for example, the Sybil attack whereby the same attack can submit numerous fake surveys for the same POI.

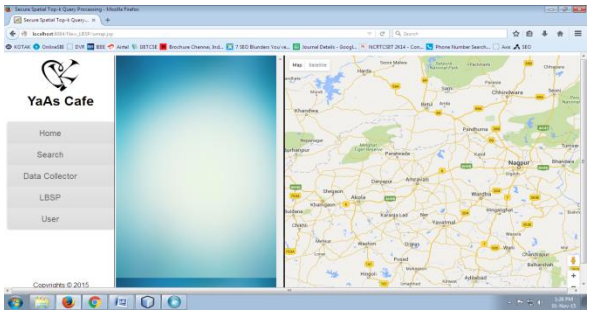
3. Experimental Work

Merkle hash tree is for creating chaining ordered POIs in every zone. It allows efficient and secure verification of the content of large data sets. Allow to verify any kind of data stored, handled, transferred in and between the computer.

Top-K query is to return the k highest ranked answer or data sets quickly and efficiently. The reason for using Top-K query is to minimize the cost metric that is associated with the retrieval of all data sets and to maximize the quality of the data set, that allows the users, not overwhelmed with irrelevant results.

3.1 Location Based Service Provider

Location Based Services Provide Modules provide a general class of computer program-level services that use location data to control features. As such LBSP is an information service which uses information on the geographical position of the mobile device. LBSP are used in a variety of contexts, such as health, indoor object search, entertainment, work, personal life, etc. LBSP include services to identify a location of a person or object, such as discovering the nearest Shopping mall or the where about of a location. Adding location information is carried out under the LBSP using the Google-Map Latitude and Longitude. The locations will be added based on the latitude and longitude of the exact location in Google-API.



3.1.1 Geolocation

He latitude and longitude coordinates of a particular location is the identification of the real-world geographic location of an object, such as a radar source, mobile phone or Internet-connected computer terminal. It refer to the practice of assessing the location, or to the actual assessed location and closely related to the use of positioning systems but may be distinguished from it by a greater emphasis on determining a location (e.g. a street address) rather than just a set of geographic coordinates.

```
// Function of Location based service identifier
function codeLatLng() {
var input = document.getElementById('latlng').value;
var latlngStr = input.split(',', 2);
var lat = parseFloat(latlngStr[0]);
var lng = parseFloat(latlngStr[1]);
var latlng = new google.maps.LatLng(lat, lng);
geocoder.geocode({'latLng': latlng}, function (results, status) {
if(status== google.maps.GeocoderStatus.OK) {
if (results[1]) {
map.setZoom(11);
```

```
marker = new google.maps.Marker({
position: latlng,
map: map
});
```

3.2 Query Processing

The LBSP purchases the data sets of interested POI categories from the data collector. For every POI category selected by the LBSP, the data collector returns the original data set D, the signatures on Merkle root hashes, and all the intermediate results for constructing the Merkle hash tree. Alternatively, the data collector can just return the first two pieces of information and let the LBSP itself perform a onetime process to derive the third piece in the same way as the date collector.

In particular, the user issues the ath snapshot top-k query at time

$$t_a = \begin{cases} 0 & \text{if a=1} \\ min(t_{a-1} + \Delta t, t_u, T) & \text{otherwise} \end{cases}$$

Where Δt is his personal parameter determining the lowest frequency at which snapshot queries are issued, and tu denotes the time when the first POI in the current top-k POIs moves out of the query region.The user issues two consecutive snapshot top-k queries at locations X and Y with query regions R1 and R2, respectively

$$\tau_i = \begin{cases} \tau_{b,i} \text{ ; if zone i only overlaps with } R_b \\ \tau_{a,i} \text{ ; if zone i only overlaps with } V_{a \to b} \\ \max(\tau_{b,i}, \tau_{a,i}) \text{ ; if zone i overlaps with both } R_b \text{ and } V_{a \to b} \end{cases}$$

Where $\tau b,i$ and $\tau a,i$ are the number of POIs in zone i.

$\tau i = The\ auxillary\ set\ of\ zone\ i$

$Rb = The\ region\ of\ ath\ snapshot\ query$

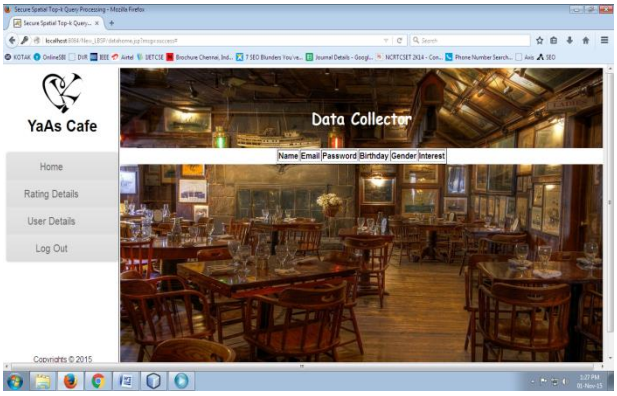
$Va \to b = The\ verification\ region$

$\Delta t = The\ delay\ between\ two\ consecutive\ snapshot\ queries$

3.3 Query Result Verification

The user verifies the authenticity and correctness of the query result, which can be done via a small plug-in developed by the data collector and installed on the web browser. For authenticity verification, the user checks if every piece of information in the query result can lead to the same Merkle root hash matching the data collector's signature. Specifically, the user first determines which of the above five cases belongs to based on its message format. And then derives the indexes for all related POIs. To perform correctness verification, the user first checks if

zones I encloses the query region R. If so, it proceeds with the following verifications in accordance with the aforementioned correctness condition used in query processing.



4. Proposed System

In propose system, three novel schemes to tackle the test for encouraging the handy sending and wide utilization of the imagined framework. The key thought of our plans is that the information gatherer pre-registers and verifies some assistant data about its information set, which will be sold along with its information set to LBSPs. To reliably answer a top-k inquiry, a LBSP need give back the right top-k POI information records and in addition appropriate proper authenticity and correctness proofs constructed from authenticated clues. The authenticity proof permits the query client to affirm that the inquiry come about just comprises of real information records from the trusted information gatherer's information set, and the rightness verification empowers the client to confirm that the returned top-k POIs are the one to fulfilling the inquiry.

The initial two schemes, both target preview top-k questions yet vary in how authenticated hints are pre-processed and how authenticity and correctness proofs are developed and confirmed and also the related correspondence and calculation overhead.

The third scheme, based upon the first scheme, acknowledges productive and verifiable moving top-k questions. The adequacy and proficiency of our schemes are completely analyzed and evaluated.

4.1 System Architecture

Location Based Services provides information about the position of a device or a user,often offered as a service via various means of media. The position can be combined with spatial information so as to integrate an LBS system with Geographical Information Systems or other location dependent information. The quality of the services provided by the LBSs depends on the utilized architecture that would support differentiated service levels, each of which guarantees a specific Quality of Service.

The design of a LBSs system focuses on the degree of accuracy in targeting a user's location. A number of geo-location technologies promise an accurate pinpointing of an object or person's position on earth. The range of coverage and scalability of applications, the degree of service quality that can be established and maintained at a reasonable cost, and the careful alignment of the overall technology costs. Systems that determine the location of a mobile user can be tracking or positioning. In the case a sensor network determines the location the term that is used is tracking. Otherwise, if the mobile system determines the location itself, the term positioning is used.

5. Conclusion

A novel distributed system for cooperative location-based information generation and sharing. It projected three novel schemes to modify secure top-k question process via un-trusted LBSP for fostering the sensible preparation and wide use of the visualized system. This schemes support each photograph and moving top-k queries, that modify users to verify the genuineness and correctness of any top-k question result. The efficacious and potency of our schemes area unit completely analyzed and evaluated through careful simulation studies. The projected platform itself wherever push and pull LBS services are often integrated on a singular visual portal; this is often done by shaping and victimization metaphysics and alternative reasoning to make sure ability at the appliance layer among several LBS service suppliers. The abstraction domain metaphysics matching application wont to integrate the fashioning symbols of the many suppliers with some extensions to be in dire straits standards to incorporate the attributes of the map symbols with the abstraction information.

References

[1] R. Zhang, Y. Zhang, and C. Zhang, "Secure Top-k Query Processing via Untrusted Location-Based Service Providers," Proc. IEEE INFOCOM '12, Mar. 2012.
[2] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "SybilGuard: Defending against Sybil Attacks via Social Networks," IEEE/ ACM Trans. Networking, vol. 16, no. 3, pp. 576-589, June 2008.
[3] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks," IEEE/ACM Trans. Networking, vol. 18, no. 3, pp. 885-898, June 2010.
[4] H. Hacig€um€us, S. Mehrotra, B. Iyer, "Providing Database as a Service," Proc. IEEE 18th Int'l Conf. Data Eng. (ICDE), Feb. 2002.
[5] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "Query Integrity Assurance of Location-Based Services Accessing Outsourced Spatial Databases," Proc. Int'l Symp. Advances in Spatial and Temporal Databases, July 2009.
[6] H. Hacig€um€u¸s, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model,"

Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD'02), pp. 216-227, 2002.

[7] B. Hore, S. Mehrotra, and G. Tsudik, "A Privacy-Preserving Index for Range Queries," Proc. 30th Int'l Conf. Very Large Data Bases (VLDB'04), pp. 720-731, Aug. 2004.

[8] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure Multidimensional Range Queries over Outsourced Data," The VLDB J., vol. 21, no. 3, pp. 333-358, 2012.

[9] E. Shi, J. Bethencourt, H. Chan, D. Song, and A. Perrig, "Multi-Dimensional Range Query over Encrypted Data," Proc. IEEE Symp. Security and Privacy (S&P'07), pp. 350-364, May 2007.

[10] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE 30th Int'l Conf. Distributed Computing Systems (ICDCS'11), June 2011.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. *IEEE INFOCOM*, Apr. 2011.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Access Control in Cloud Computing," Proc. IEEE INFOCOM'10, Mar. 2010.

[13] H. Pang and K.-L. Tan, "Verifying Completeness of Relational Query Answers from Online Servers," ACM Trans. Information and System Security, vol. 11, no. 2, pp. 1-50, Mar. 2008.