IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 16-19

Spatial Technology for POI Cognition and Image Localization

Priti S. Netam[1], Jagdish Pimple[2]
*[1]*Student, Department of computer science and engineering, Nagpur Institute of technology, Nagpur*
Priti15891@gmail.com[1]
[2]*Professor, department of computer science and engineering, Nagpur institute of technology, Nagpur*
pimplejagdish@gmail.com[2]

Abstract: *In this paper location based information generation and sharing is considered which becomes increasingly more popular due to the explosive growth of internet capable and location aware mobile devices. The system consist of data collector, data contributor, location based service provider by using google maps and system users.The data collector gathers all the information from data contributor while user fire query to perform spatial top-k query which ask for POI in certain region & finding the highest k rating for interested POI attribute. In practice, LBSPs are untrusted and may return fake query results for various bad motives eg. In favor of POIs willing to pay. Three novel schemes are used for user to detect fake query result and moving top-k query result as push to cultivate the helpful arrangement and utilization of the projected framework. The affectivity and productivity of schemes area unit analyzed and evaluated.*

Keywords: *Location based service provider (LBSP), Point-of-interest (POI), Data collector and contributor.*

I. Introduction

The touchy development of internet and location based area aware mobile devices and surge in social media organization use are cultivating cooperative data age and sharing on a phenomenal scale. All most all smart phones have cellular data/ Wi-Fi internet access and can always acquire location via pre-installed positioning software. Also growing popularity of social network. It is very easy to share their reviews or experiences with others or with all kinds of points-of-interest (POIs) such as bar, restaurants, grocery stores, coffee shops and hotels. Meanwhile, it becomes commonplace for people to perform various spatial Poi queries at online location based service provider (LBSPs) such as Google maps and yelps. As probably, the most familiar types of spatial queries ask for POIs in certain region with the highest k rating for a given POIs attribute. For example, one many search for the best five stars hotel with the least précising within his budget.

II. Related Problems

There are two essential drawbacks with current top-k query service. First, individual LSBPs often have very small Data set for comparing POI reviews. This would largely affect on use of spatial top-k query services. The data set at individuals LBSP may not cover all the hotels within the search radius. Additional some hotels being closed after that this services may receives divers rating so user get confused by very different query results from different LBSP for the same query. Second, in data collector may modify their data sets by deleting some reviews or adding take reviews and return fake query results in favor of hotels that are willing to pay or against those that refuse to pay. To introduce some trusted data collectors as central hubs for collecting POI reviews is a good solution. Such centralized data collection also makes it much easier and feasible for data collector to pay sophisticated defence to filter out fake reviews from malicious entities like Sybil attackers. Data collector can be either new service provider with a large user base such as Google, yahoo, Facebook, twitter, etc. many of these service providers have already been collecting reviews from their user and offered open APIs for exporting selected data from their systems. The above API provide the information which will fire query result will be much more trustworthy, which would be turn in help them attract more and more peoples. A main challenge for realizing and appealing system above is how to deal with untrusted and possibly malicious LBSP. In malicious LBSPs may still modify the data sets from data collectors and provide top-k query results in favor of POIs willing to pay. Even worse, they may falsely claim generating query results based on review data from trusted data collectors, which they actually did not purchase. Moreover, nonmalicious LBSPs may be compromised to return fake top-k query results.

III. Problem Analysis

Data privacy requires the data owner outsource the encrypted data to the service provider and efficient techniques are needed to support querying encrypted data. In bucketization method proposed to enable efficient range queries over encrypted data, which was recently improved. it presented novel methods for multi-

dimensional range queries over encrypted data. Recently proposed secure ranked keyword search or fine-grained access control over encrypted data. Ensuring query integrity is studied, i.e., that a query result is indeed generated from the outsourced data and contains all the data satisfying the query. In these schemes, the data owner outsources both its data and also its signatures over the data to the service provider which returns both the query result and a verification object (VO) computed from the signatures for the querying user to verify query integrity. Many techniques were proposed for signature and VO generations, based on signature chaining and based on the Merkle hash tree. These schemes assume that some master nodes are storing data from regular sensor nodes and answering the queries from the remote network owner.

To propose three novel schemes to tackle the spatial top k query processing challenge for fostering the practical deployment and wide use of the envisioned system. The key idea is that the data collector pre-computes and authenticates some auxiliary information about its data set, which will be sold along with its data set to LBSPs. To answer a top-k query, a LBSP return the correct top-k POI data records as well as proper authenticity and correctness proofs constructed from authenticated hints. The authenticity proof allows the query user to confirm query result only consists of authentic data records from the trusted data collector's data set, and the correctness proof enables the user to verify the returned top-k query POIs are the true ones satisfying. In first two schemes both the schemes gives top-k queries but differ in how authenticated hints are recomputed and how authenticity and correctness proofs are constructed and verified as well as the related communication and computation overhead. The third scheme, built upon the first scheme that is efficient and verifiable moving top-k queries. A data owner outsources its encrypted data either to a third-party service provider who is responsible for answering the data queries from the data owner or to the other users.

IV. Implementation

A. Data Contributor:

In Data contributors, contribute all information like POIs, reviews and location detail related to our spatial location which user want. All this information from data contributor submit for data collectors. Data contributor can submit the POI information with complete details of the object found nearby.

B. Data Collector:

Data collectors are considered trusted and as the central hubs for collecting POI reviews. Instead of submitting POI reviews to individual LBSPs, people can now submit them to a few data collectors to earn rewards. The data sets maintained by data collectors can thus be considered the union of the small data sets currently at individual LBSPs. Such centralized data collection also makes it much easier and feasible for data collectors to employ sophisticated defences, to filter out fake reviews from malicious entities like Sybil attackers. Data collectors is the new service providers for the user.

C. Location Based Service provider

The data collector sells aggregated POI reviews in the form of a location-based data set to individual LBSPs. Every LBSP operates a website for users to perform top-k queries over the purchased data set and may add some appealing functionalities to the query result.

D. User Query

User fire a query to location based service provider. This model enables the user to verify the authenticity and correctness of the query result returned by the LBSP. The query result is considered authentic if all its k POI records exist in the data collector's data set and have not been tampered with, and it is called correct if it contains the true top-k POI records in the query region.

E. Top-K Query Processing

Top- k query processing process query for user who want perfect POI and reviews for wanting place and provide top-k results will be given to the user. 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 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.

V. Result Analysis

Results of this paper is as shown in following figure.1 to figure.5

Figure.1

Figure.2

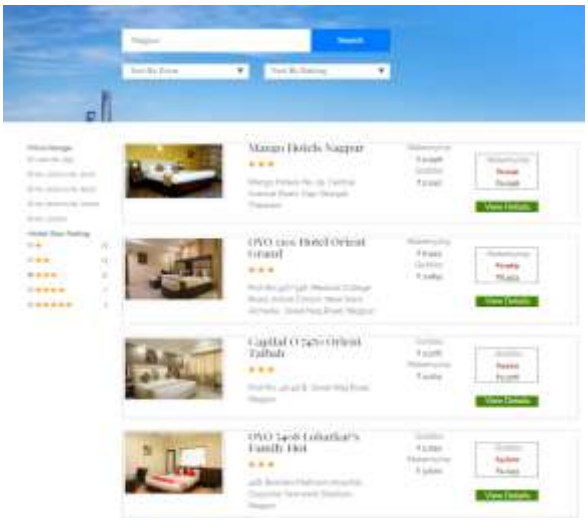

Figure.3

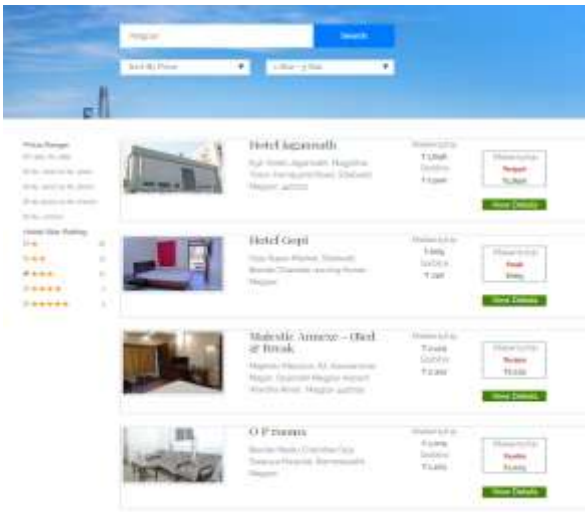

Figure.4

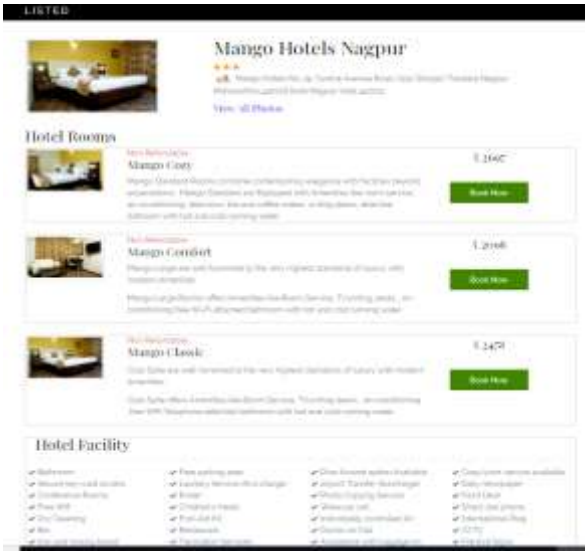

Figure.5

VI. Conclusion

Considered a novel distributed system for collaborative location-based information generation and sharing. Three novel schemes to enable secure top-k query processing via untrusted LBSPs for fostering the practical deployment and wide use of the envisioned system. Proposed schemes support both snapshot and moving top-k queries, which enable users to verify the authenticity and correctness of any top-k query result. The efficacy and efficiency of schemes are thoroughly analysed and evaluated through detailed simulation studies.

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, and B.
[5]. Iyer, "Providing Database as a Service," Proc. IEEE 18th Int'l Conf. Data Eng. (ICDE), Feb. 2002.
[6]. W.-S. Ku, L. Hu, C. Shahabi, and H.
[7]. Wang, "Query Integrity Assurance of Location-Based Services Accessing Outsourced Spatial Databases," Proc. Int'l Symp. Advances Fig.5. in Spatial and Temporal Databases, July 2009.
[8]. 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.
[9]. 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.