iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** X **Month of publication:** October 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue X, October 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on Untrusted Location-Based Service Providers Using Secure Spatial Top-K Query Processing

Shyamala.P[1], Deepa.D[2]
[1,2]Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam

Abstract— A novel distributed framework for cooperative location-based data information and sharing which turn out to be progressively well known because of the hazardous development of Web skilled and location-based mobile phones. The framework comprises of an information authority, information donors, location-based administration suppliers (LBSPs), and framework clients. The information authority accumulates audits about purposes of-interest (POIs) from information benefactors, while LBSPs buy POI information sets from the information gatherer and permit clients to perform spatial top-k inquiries which request the POIs in a sure locale and with the most noteworthy k appraisals for an intrigued POI trait. Practically, LBSPs are untrusted and may return fake question results for different awful thought processes, e.g., for POIs willing to pay. This paper presents three novel plans for clients to recognize fake spatial depiction and moving top-k question results as a push to cultivate the useful arrangement and utilization of the proposed framework. The effectuality and productivity of schemes are analysed and evaluated.

Keywords— Spatial top-k query, location-based service, security, POI

I. INTRODUCTION

The explosive growth of Internet-capable location-aware cell phones and the surge in interpersonal organization use are encouraging synergistic data era and sharing on an exceptional scale. All mobile phones have Wi-Fi Web get to and can simply get their exact locations through pre-introduced situating programming. Likewise attributable to the developing notoriety of informal communities, it is more advantageous and inspiring for versatile clients to impart to others their involvement with a wide range of purposes of intrigues. In the meantime, it gets to be regular spot for individuals to perform different spatial POI inquiries at online location-based administration suppliers (LBSPs). This paper concentrates on spatial top-k questions, and the expression "spatial" will be overlooked from now on for curtness.

II. PROBLEM FORMULATION

This work is most identified with information outsourcing, for which we 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.

A. Survey On Secure Query Processing

Project Title	Algorithm/ Techniques	Remarks/ Problem Identification
Secure Top-k Query Processing via Untrusted Location-based Service Providers	Using of 2 scheme novel based approach	1. It may falsely claim generating query results based on the review data from trusted data collectors. 2. The non-malicious LBSPs may be compromised to return fake top-k query results.

©IJRASET 2015: All Rights are Reserved

Sybil Guard: Defending Against Sybil Attacks via Social Networks	Sybil Guard, a novel protocol	1. The Sybil Attack is a powerful threat faced by any decentralized distributed system that has no central, trusted authority to vouch for a one-to-one correspondence between users and identities. 2. The important issues include how to bootstrap the social network and what applications can best benefit from Sybil Guard's fully decentralized approach.
Sybil Limit: A Near Optimal Social Network Defense against Sybil Attacks	Sybil Limit's and Sybil Guard's approach	1. Sybil Limit's guarantees on much smaller social networks with only 100 nodes. It cannot extract 100 node sub graphs from our social network data sets. 2. It does not intend to implement Sybil Limit within the context of some real-world applications and demonstrate its utility.
Query Integrity Assurance of Location based Services Accessing Outsourced Spatial Databases	Partially Materialized Digest scheme	1. It does not extend algorithms to support more spatial query types such as spatial join, spatial path queries, etc.

B. Existing System Model

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. Proceed with the eatery case. The information sets at individual LBSPs may not cover all the Italian restaurants within a search. Also, the same restaurants may get assorted evaluations at distinctive LBSPs, so clients may get confounded by altogether different inquiry results from diverse LBSPs for the same question. 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 assault whereby the same assailant can submit numerous fake surveys for the same POI.

III. RELATED WORK

The solution for the two issues is to present some trusted data collectors as the focal center points for gathering POI surveys. Specifically, data collectors can offer different motivators, for selling so as to invigorate survey entries and afterward benefit the audit data to individual LBSPs. Rather than submitting POI audits to individual LBSPs, individuals can now submit them to a couple data collectors to procure rewards. The data sets kept up by data collectors can in this manner be viewed as the union of the little data sets right now at individual LBSPs. Such brought together data gathering likewise makes it much less demanding and attainable for data collectors to utilize modern protections, for example, to sift through fake surveys from vindictive elements like Sybil assailants. Data collectors can be either new administration suppliers or all the more ideally existing ones with an expansive client base, for example, Google, Facebook, Twitter, and MSN. A number of these administration suppliers (e.g., Google) have as of now been gathering surveys from their clients and offered open APIs for sending out chose data from their frameworks.

IV. PROPOSED SYSTEM

In proposed 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

©IJRASET 2015: All Rights are Reserved

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.

A. *Proposed Implementation Scheme*

The proposed system implemented with

1) *Data Collector:* Gathers the reviews about point of interest (POIs) from the data contributors.
2) *Data Contributors:* These are the people who submit POIs. Combined the data sets which gathered at individual LBSPs and provide centralized data sets.
3) *Location Based Service Providers (LBSP) :* It purchase POIs data sets from the data collector and allow users to perform spatial top-k queries which ask for the POI in a certain region.

B. *Secure Snapshot Top-K Query Processing*

1) Scheme 1: Using of *Merkle hash tree* is for creating chaining ordered POIs in every zone. It allow 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.

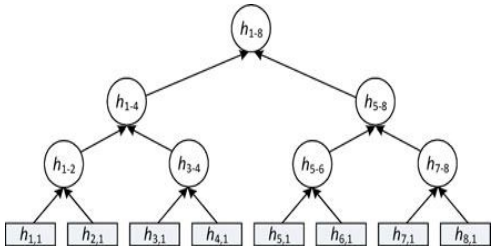


Fig. 1. An example of constructing the Merkle hash tree

In Scheme 1, authenticated hints are created by chaining ordered POIs in every zone via cryptographic hash functions and then tieing the POIs in different zones via a Merkle hash tree.

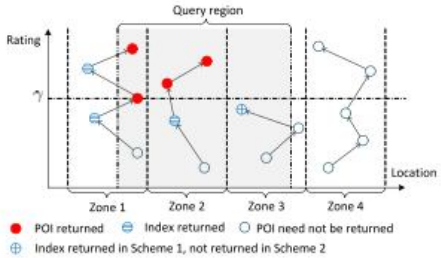


Fig:2 An example for scheme 1, the dots in zone i correspond to POI records from top to bottom

To perform correctness verification, the user first checks if zones **I** encloses the query region **R**. If so, he proceeds with the following verifications in accordance with the mentioned correctness condition used in query processing: There are exactly k data records in the query result with POI locations all in **R**, which correspond to the top-k POIs (i.e., kPOI) in **R**. If so, the user locates the lowest attribute-k rating g.

2) Scheme 2: It points to the work by embedding or combining some information among nearby zones to reduce the amount of information return to the user. In scheme 2, LBSP return the information to the user, where no POIs are present. To implement the basic idea, the data collector binds to every POI data index some additional information about the POIs in adjacent zones. In particular, the data collector partitions the original M zones into non-overlapping macro zones, each consisting of m nearby zones, where m is a public system parameter. The LBSP purchases the original data set D, the signatures on Merkle root hashes, and all the intermediate results for constructing the Merkle hash tree of every

©IJRASET 2015: All Rights are Reserved

interested POI category from the data collector.

3) Scheme 3

Using Of Top-K Query

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

An update in the top- k POIs may occur when a current top-k POI is no longer in the moving query region or when a new POI appears in the moving query region, which has an attribute-q rating higher than the lowest among the current top-k POIs. The user can directly tell when the first situation occurs based on the current top-k POIs he knows, in which case he can issue a new snapshot top-k query for the current query region.

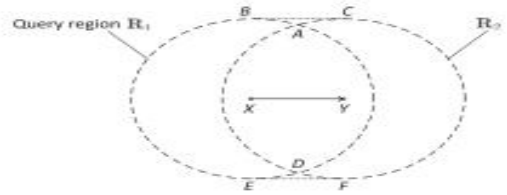


Fig:3 an example of two consecutive snapshot top-k query

The user, however, cannot tell when the second situation will occur. Without a sound defense in place, the LBSP can choose not to inform the user about updated top-k POIs in the second situation.Scheme3 is done by using neither scheme1 nor scheme2.The data sets has been pre-processed by the data collector when it is selected. Using of scheme 1 is due to space constraints and for without loss of generality scheme 2 is used.

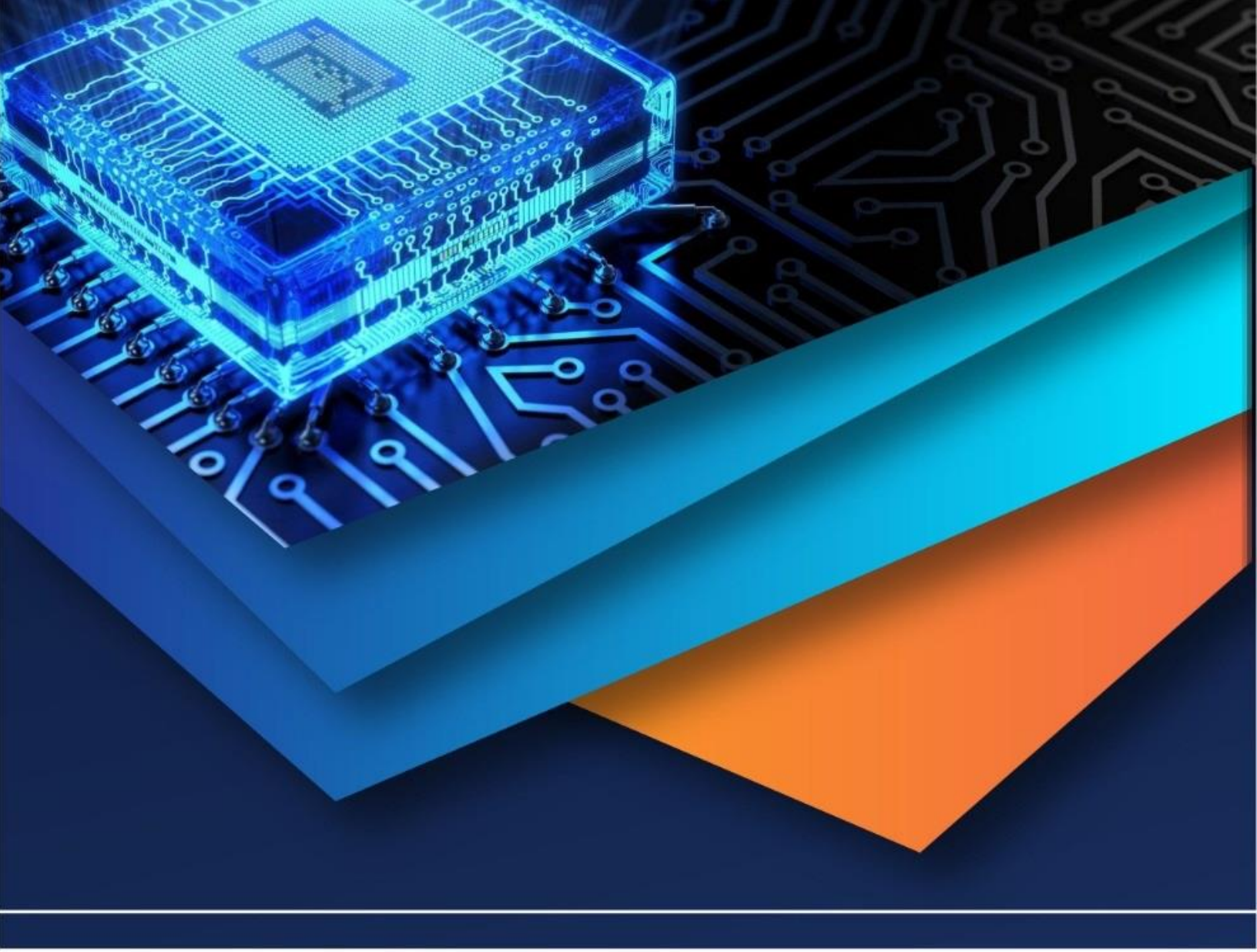
V. CONCLUSIONS

This novel distributed system for collaborative location-based information generation and Sharing. This proposed 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. The location based information generation and sharing for distributed system enables a secure processing, which enables the users to verify authenticity and correctness of the query result for untrusted location using novel schemes.

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, "Sybil Guard: Defending against Sybil Attacks via Social Networks," IEEE/ ACM Trans. Networking, vol. 16, no. 3, pp. 576-589, June 2008.
[3] W.-S.Ku, L. Hu, C.Shahabi and H.Wang, "Query Integrity Assurance of Location-Based Services Accessing Outsourced Spa- tial Databases," Proc. Int'l Symp. Advances in Spatial and Temporal Databases, July 2009.
[4] H.Hacigümüş, 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.
[5] 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.
[6] 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.
[7] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Sensor Networks," Proc. IEEE INFOCOM'08, pp. 46-50, Apr. 2008.
[8] J.Shi, R.Zhang, and Y.Zhang, "Secure Range Queries in TieredSensor Networks," Proc. IEEE INFOCOM'09, Apr. 2009.
[9] R.Zhang, J.Shi, and Y.Zhang, "Secure Multidimensional Range Queries in Sensor Networks," Proc. ACM MobiHoc'09, pp. 197-206, May 2009.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)