Novel Schemes for Spatial Top-K Query Processing for Vulnerable Location Based Service Providers

[1]K.Srikanth, [2]M.Rajakumar, [3]A.Lakshman Rao
[1,2,3]Dept.of CSE, Pragati Engineering College, Surampalem, Andhra Pradesh, India

Abstract
This paper presents a novel distributed framework for collaborative location based information generation and sharing that becomes popular due to internet ability and position aware mobile devices. This framework contains Location Based Service Providers (LBSPs), Information Collector, Information Contributors and framework users. The information collector gets the information about point of interest (POI) from information contributors, while Information collector sells the data sets to the LBSPs. The LBSPs allow the users thus providing top-k queries which are requested to ask for the POIs in particular region information with highest top k rating for POI's trait. Assuming LBSP's may still change the data sets from data collector and provide basic top k query results in favor of POIs willing to pay. In this paper, there are three novel schemes are used for clients which are easily identified fake spatial queries and moving top k query results thereby utilizing proposed framework.

Keywords
Spatial top-k query, Security, LBSP, POI.

I. Introduction

There is much growth of internet-capable and location-aware cell phone devices and the surge in social network usages are highly used in these days. So that almost all smart phones having cellular/ Wi-Fi internet connection and they can easily identified their exact location through different types of location based software's or apps. Now days the social networks are more popular and the smart phone users to share their experience with other mobile users with all kinds of Point of Interests (POIs) about Educational Institutions, Police Stations, Hospitals, Restaurants, Grocery Stores, Coffee Cafes and Hotels. These are all common places for peoples to received different types of spatial POI queries at online Location Based Service Providers (LBSPs) such has Google and Others. The LBSPs are requested to ask for the POIs in particular region with the highest k rating for a given POI attributes. For example one may search for the best five coffee cafes with the highest rates and within five/ten kilometers of his current position.

A. Existing System Model

In the present framework two drawbacks are available, first one is location based service providers have maintain little amount of information sets counting POI reviews. The information sets at individual LBSPs may not cover all the Educational Institutions inside pursuit span and moreover client may get mistook for different rating from various LBSPs for the same question. Second one is LBSPs may change their information sets by erasing some original rating records and adding fake rating records in favor of particular Educational Institutions that will pay.

B. Proposed System Model

There are three novel schemes are proposed in this paper. First scheme, verified indications are made by fastening requested POIs in each zone and afterward tying the POIs in various zones. The LBSP to give back some data for each hopeful zone regardless of the fact that it has no top k POI fulfilling the query. Second scheme, which works by implanting some data among close-by zones to significantly diminish the measure of information, came back to the user. Third scheme, the LBSP procedure back to back snapshot top k questions required in a moving top k query in general and give back a question comes about if there are any redesigns in the top-k POIs fulfilling the query.

II. Related Work

The work is most related to information outsourcing [1], for which it can simply audit individual plans in light of space limitations. The arrangement of information outsourcing was at first exhibited [1] [4], in which a information proprietor outsources its data to a pariah organization supplier who is mindful of nothing the data proprietor or distinctive customers. Generally speaking, there are two security worries in information outsourcing: data security and data integrity [2] [7] .

The data security requires the data proprietor to outsource encoded information to the administration supplier and proficient systems are expected to bolster questioning scrambled information. A bucketization strategy was proposed into empower proficient extent questions over scrambled information [5-6]. This profession is orthogonal to our work as we concentrate on openly available location based information without requirement for privacy protection. Another line of exploration has been given to guaranteeing information integrity. In this scheme, the information owner outsources both its information furthermore its marks over the information to the service suppliers which returns both query results and Verification Object (VO) processed to the marks for the questioning client to verify query integrity [8].

III. System Architecture

The below figure shows the architecture for location-based services. The query is implementing in the following way the authentication module in the cell phone transportation queries the services communications for the plan of trusted model. It does so by relocate the query to the authentication query method module in the service interactions. All cell phone users who want to access a site based service sends a service question to the cell phone connections, to the forwarder module checks strength for the query from the database (should the user sign up to the location based service) These service checks whether contacts is nearby or not, The locator module proceeds location information only in encrypted form with the symmetric key. Next the question process module hand's over the location in order the operator's public key and classification information.

The trust module decrypts the place information, as necessary as in the case of a query for good-looking, the module ask for the scrupulous place in the database. Such as road maps or conditions. To detect misbehaviours by the service providers these generated cataloguing information. Finally the forwarder module forwards the plaintext response to the cell phone.

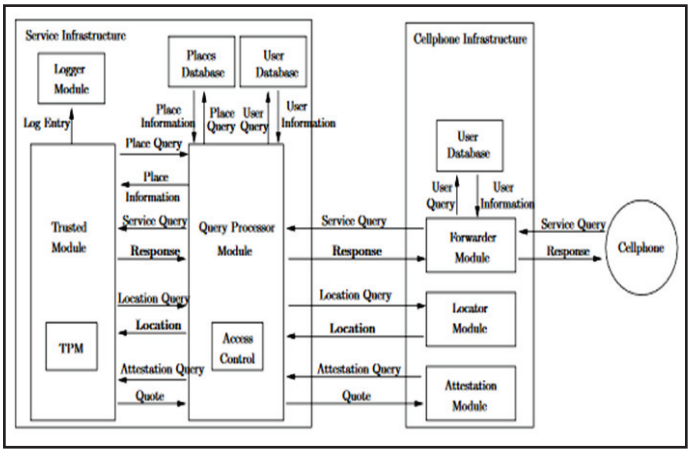

Fig. 1: Architecture for LBSP

IV. System Model

The novel distributed framework contain information collector, information contributor, Location Based Service Providers and top k query users. Common people constitute an information contributor, who will submit POI reviews to the information collector's website. The information collector normally stimulates the review submission and has counter measures on malicious information contributors who provide fake reviews. The information collector sells aggravated POI reviews in the form of a location based data sets to individual sets. For clients LBSP works to on a site to perform top-k inquiries over the acquired information set and may add some available functionalities to the inquiry result, for example, road maps and photographs.

The information set is arranged by classifications, such has Educational Institutions, Police Stations, Hospitals, Restaurants, Grocery Stores, Coffee Cafes and Hotels and it contain exceptional record for each POI in each classification. The information collector covers area, which is partitioned into M≥1, equally sized non-over lapping zones. For every zone i, let ni denotes the number of POIs, POIij and Dij denotes the jth POI and corresponding data record respectively. Assumed that nij data contributors provide a review about POIi,j to the data collector. A rating on every attribute and text comments are included in every review. The data record Di,j for POIi,j includes its name, location li,j, review nij, and possibly other information.

V. Secure Spatial Top K Query Processing

Secure spatial top k query processing includes three phases. Initial one is information processing phase; the information gatherer utilizes cryptographic techniques to make validation indications over the information sets. Next one is query processing phase; the LBSP answers a top k query by giving back the question comes about and in addition the validness and precision proofs to the query users. Last one is query result verification phase, the user verify authenticity and correctness proofs.

A. Scheme1

Authentication indications are made by affixing requested POIs in each zone by means of cryptographic hash capacities and afterward tying the POIs in fluctuates zones through Markle hash tree. In below figure shows an example of constructing Markle hash tree.

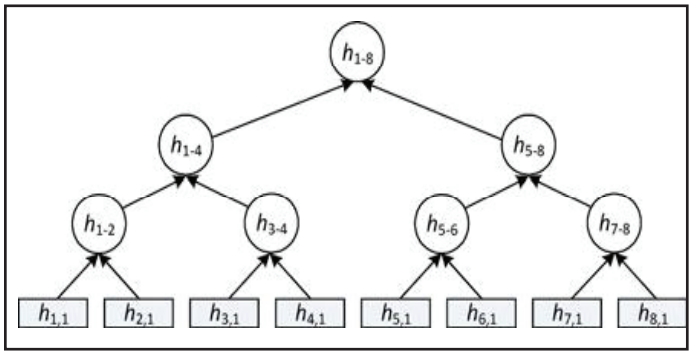

Fig. 2: Constructing Markle hash tree for Scheme1

In Query processing, the information sets of intrigued POI classifications are bought by LBSP from the data gatherer. For every POI class picked by the LBSP, the information collector gives back the primary information set D, the imprints on Markle root hashes and all the intermediate results comes about for building the Markle hash tree. The handling of depiction top k query incorporates the coveted POI classification, the intrigued quality q, for positioning POIs the question area R, and k are required. K POIs in R with the highest k attribute-q is denoted by k, and the lowest attribute q rating is denoted by g. Likewise, every zone either totally or partially covered by the query region is called as an applicant zone. A privilege and veritable query result needs to fulfill two conditions. The rightness condition needs the query result to contain the following information: (A) the accomplished data records for k POI;(B) the information records for whole the POIs in every applicant zone however not in R whose characteristic q rating is more conspicuous than g and (C) inexact data is expected to demonstrate that the query arrangement incorporates either the information record or list of each POI in each applicant zone with property q rating not littler than g. Also, the variability condition requires that the query result incorporate the auxiliary set for each hopeful zone for the calculation and confirmation of the qth Markle root hash.

In Query result verification, the user verified that each bit of data in the query result will prompt the same Markle root hash which coordinates the information collector's signature. This is made for authentication purpose. If the query result is authentic, the user can reason the same root hash for every i to I, by which further confirmation is done to check whether the information authority's mark in the question result is a substantial mark on the determined root hash. If so, it is considered that the query result is authentic. The output of query result verification figure is shown below.

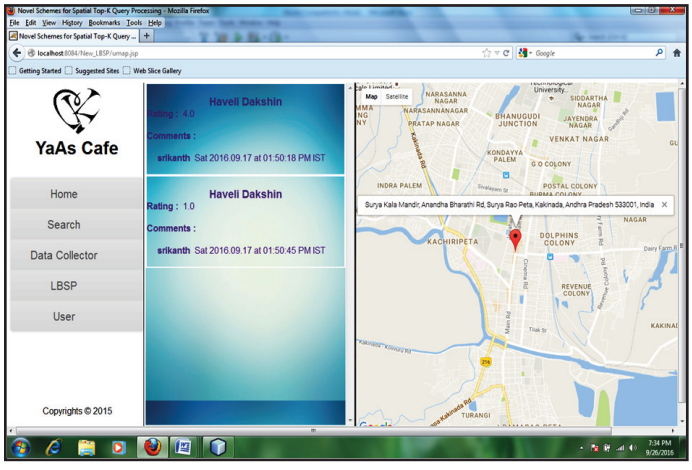

Fig. 3:

B. Scheme2

Scheme1 requires the LBSP to give back some data for each hopeful zone regardless of the fact that it has no top k POI fulfilling the query. This may incur significant communication overhead for a large query region. Given this perception the scheme2 is proposed, which works by implanting some data among close-by zones to significantly decrease the measure of data came back to the customer. The essential thought of scheme2 can better outline utilizing a basic case. Expect i and j are two candidate zones. But nether contain a POI. Under scheme1, the LBSP need return both {i, ¢i,1, hi,2,Ti} and both {j, ¢j,1, hj,2,Tj} to demonstrate that no POI zones i or j fulfills the query. In the event that i and j are viewed as virtual zones, the LBSP just need return {x, ¢x,1, hx,2,Tx} where x=i if the biggest attribute q rating in j zone is littler than in i zone and x=j generally. The amount of data came back to the user can along these lines be decreased.

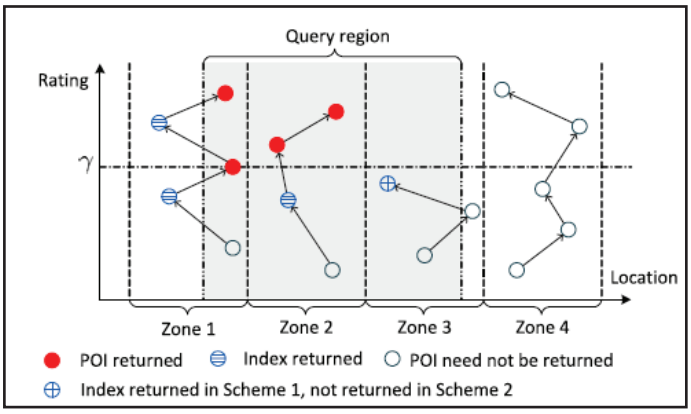

Fig. 4: Markle hash tree for Scheme2

C. Scheme3

Here secure moving top k was presented, the LBSP procedure successive depiction top k query required in a moving top k query all in all and just give back a query results if there is any upgrade in the top k POIs fulfilling the question. An upgrade in the top k POIs may happen when a present top k POI is no more in the moving query area or when another POI shows up in the moving query area, which has a quality q rating higher than the least among the present top k POIs.

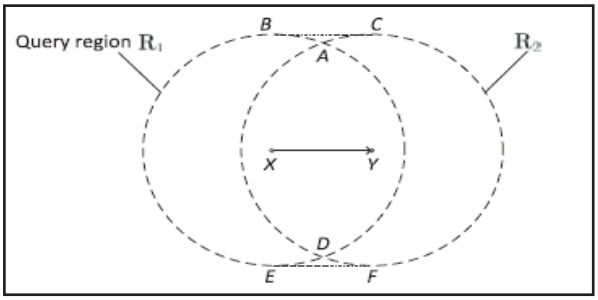

Fig. 5: The two consecutive snapshot top k query

The goal of scheme3 is because of space constraints and expects that the information set has been preprocessed by the information gathered in like manner and the same configuration standards apply when scheme2 is picked. Without loss of consensus and accept that a client issues a moving top k query for attribute q during time period (0,T), where T may be unknown in advance. Since a moving top k query indicates the ath snapshot top k query by Qa and the relating inquiry area Ra. Let kPOIa a chance to be the top k POIs in Ra and Ya the most reduced property q rating among kPOIa.

VI. 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. As shown below figure the location proof updating architecture and message flow.

Fig. 6: Location proof updating architecture and message flow

VII. Searching Location Based on User Rating

These geographical locations are protected with the breach of trust. This paper targets to supply a trusted communication among Mobile Users, Mobile Servers and Mobile Service Providers. We framed an authentication algorithm E2SQ- LBS (Exploring and securing the spatial queries of location based services). Firstly, the mobile server gets the user-specified queries and verifies whether the user specified location. If it's authorized, a secure communication channel is enabled between the mobile users and Mobile Service Providers. These credentials are transmitted via public channel which leads to violation of privacy, known as Intrusion. To defend from colluding attacks, spatial queries oriented clustering is formed that helps to eliminate the redundant data. Ranking schemes is employed to sum up the topmost –searched queries. This application will perfectly work with Global Positioning System or Bluetooth with lessened storage space and power cost. Performance validation will prove that information are preserved at both user and server location. The output of our proposed system looks like this by the following output.

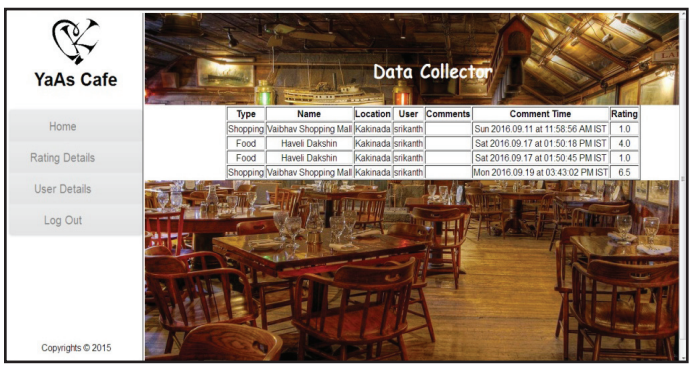

Fig. 7:

VIII. Conclusion

Here a novel appropriated framework for helpful location based data generation and sharing. It anticipated three novel plans to change secure top k query process for vulnerable location based administration suppliers for cultivating the sensible planning and wide utilization of the envisioned framework. This scheme supports every photo and moving top k inquiries, the change clients to check the validity and accuracy of any top k question comes about. The location based generation and sharing for appropriated framework enables a secure processing, which enable the clients to check legitimacy and accuracy of the inquiry results for vulnerable location using novel schemes. The key value which is used to construct the tree is also encrypted so that is not possible to add a fake query results in the list. The efficacious and potency of our schemes area unit completely analyzed and evaluated through care full simulation studies. The projected platform itself wherever pushes and pull LBSP services are often integrated on a singular visual portal.

References

[1] R. Zhang, Y. Zhang, C. Zhang,"Secure Top-k Query Processing via Untrusted Location-Based Service Providers," Proc. IEEE INFOCOM'12, Mar. 2012.

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

[3] S.Choi, H. Lim, E. Bertino,"Authenticated top-k aggregation in distributed and outsourced databases", SOCIALCOM-PASSAT12, pp. 779–788, 2012.

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

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

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

[7] F. Chen A. Liu,"SafeQ: Secure and Efficient Query Processing in Sensor Networks," Proc. IEEE INFOCOM'10, pp. 1-9, Mar. 2010.

[8] R. Zhang, J. Shi, Y. Liu, Y. Zhang,"Verifiable Fine-Grained Top-K Queries in Tiered Sensor Networks," Proc. IEEE INFOCOM'10, Mar. 2010.

[9] H. Yu, P. Gibbons, M. Kaminsky, 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.

[10] H. Hu, J. Xu, Q. Chen, Z. Yang,"Authenticating location-based services without compromising location privacy", In Proc. SIGMOD, pp. 301–312, 2012.

[11] X. Lin, J. Xu, H. Hu.,"Authentication of location-based skyline queries", In Proc. CIKM, 2011.

[12] M. L. Yiu, E. Lo, D. Yung,"Authentication of moving knn queries", In Proc. ICDE, 2011.

Mr. K.Srikanth is a student of Pragati Engineering College, Surampalem, East Godavari Dist, Andhra Pradesh, India. Presently, he is pursing Masters of Technology [Computer Science & Engineering] from this college and he has received his Bachelor of Technology from Narasaraopet Engineering College, Narasaraopeta Affiliated to Jawaharlal Nehru Technical University, Kakinada in the year 2010. His area of interest includes Secure Computing, Cloud Computing and Networking.

Mr. M.Rajakumar is currently working as an Associate Professor in Department of CSE, Pragati Engineering College. He acquired Bachelor of Technology and Master of Technology [Ph.D] from Jawaharlal Nehru Technical University, Kakinada. He published nearly 8 papers in International Journals. His area of interest includes Network Security and Cryptography.

Mr. A.Lakshman Rao is currently working as an Associate Professor in Department of CSE, Pragati Engineering College. He acquired Master of Technology from GIET, Rajamundry. He published nearly 10 papers in International Journals. His area of interest includes Data Warehousing and Network Security.