Review on Keyword Processing According to Rank in LBSP (Location-Based Service Providers)

Miss Apeksha B. Nachone (ME,CSIT)
HVPM'S Amravati
Maharashtra, India.

Prof. Karuna G. Bagde
HVPM'S Amravati
Maharashtra, India.

ABSTRACT

The geographic information is present on the internet which is in the scattered format. When user search for any place then various locations based service providers find out the results. The commonly used location based service providers are Google, Bing, Yahoo etc. we considers a novel distributed system for collaborative location-based information generation and sharing which become increasingly popular due to the explosive growth of Internet-capable and location-aware mobile devices. The results that are given by location based service providers not fully processed. The system consists of a data collector, data contributors, location-based service providers (LBSPs), and system users. The data collector gathers reviews about points-of-interest (POIs) from data contributors, while LBSPs purchase POI data sets from the data collector and allow users to perform spatial top-k queries which ask for the POIs in a certain region and with the highest k ratings for an interested POI attribute. The data contributor is the peoples or users who provide the information about the place. The user can gives comment and reviews to the product or the place. It's not necessary the LBSP provides proper information. In practice, LBSPs are untrusted and may return fake query results for various bad

motives, e.g., in favour of POIs willing to pay. In our approach when the data contributor searches for any query, it will process by the LBSP. But before result showing to the user, it will process by the data collector. There are various results for the same query. So each query processed and special top result according to the location will provide to the users. This paper presents three novel schemes for users to detect fake spatial snapshot and moving top-k query results as an effort to foster the practical deployment and use of the proposed system. The efficacy and efficiency of our schemes are thoroughly analysed and evaluated.

Keywords:Bing,Datacollector,Data contributor, LBSP ,POI , top k query .

I) 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 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) BACKGROUND

The work is most related to outsourced databases, and can review the existing schemes related to work. R. Zhang, Y. Zhang, and C. Zhang [1]. They considers a novel distributed system for collaborative location-based information generation and sharing which become increasingly popular due to the explosive growth of Internet-capable and location aware mobile devices. The system consists of a data collector, data contributors, location-based service providers (LBSPs), and system users. The data collector gathers reviews about points-of-interest (POIs) from data contributors i.e. common people, while LBSPs purchase POI data sets from the data collector and allow users to perform spatial top-k queries which ask for the POIs in a certain region and with the highest k ratings for an interested POI attribute. In practice, LBSPs are untrusted and may return fake query results for various bad motives, e.g., in favor of POIs willing to pay. This paper presents three novel schemes for users to detect fake spatial snapshot and moving top-k query results as an effort to foster the practical deployment and use of the proposed system. This paper focuses on spatial top-k queries. They notice two essential drawbacks with current top-k query services. First, individual LBSPs often have very small data sets comprising POI reviews. The data sets at individual LBSPs may not cover all the Italian restaurants within a search radius. Second, LBSPs may modify their data sets by deleting some reviews or adding fake reviews and return tailored query results in favor of the restaurants that are willing to pay or against those that refuse to pay.

Rui Zhang and Yancho Zhang, Chi Zhang [2] proposed the tremendous growth of Internet-capable and location aware mobile devices and the surge in social network usage are fostering collaborative information generation and sharing on an unprecedented scale. In this paper they considers a novel distributed system for collaborative location-based information generation and sharing which become increasingly popular due to the explosive growth of Internet-capable and location-aware mobile devices. The system consists of a data collector, data contributors, location-based service providers (LBSPs), and system users.

Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons [3]. In this paper, peer-to-peer and other decentralized, distributed systems are known to be particularly vulnerable to *sybil attacks*. In a sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. By controlling a large fraction of the nodes in the system, the malicious user is able to “out vote” the honest users in collaborative tasks such as Byzantine failure defenses. This paper presents *SybilGuard*, a novel protocol for limiting the corruptive influences of sybil attacks. Our protocol is based on the “social network”

among user identities, where an edge between two identities indicates a human-established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately small "cut" in the graph between the sybil nodes and the honest nodes. SybilGuard exploits this property to bound the number of identities a malicious user can create. The advantage of this paper is that the main drawback of a slower mixing social network is that more honest nodes will be (mistakenly) rejected and drawback is that defending against sybil attacks without a trusted central authority is much harder.

Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou [4].In this paper, they define and solve the problem of multi-keyword ranked search over encrypted cloud data, and establish a variety of privacy requirements. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to effectively capture the relevance of outsourced documents to the query keywords, and use "inner product similarity" to quantitatively evaluate such similarity measure. For meeting the challenge of supporting multi-keyword semantic without privacy breaches, we propose a basic idea of MRSE using secure inner product computation. The disadvantage of this paper is that they not explore supporting other multi keyword semantics (e.g., weighted query) over encrypted data, integrity check of rank order in search result.

Man Lung Yiu, Yimin Lin, Kyriakos Mouratidis [5]. It proposes a scheme on shortest path verification in outsourced network databases. Also propose the concept of authenticated hints, which is used to reduce the size of the proofs. We develop several authentication techniques and quantify their trade-offs with respect to offline construction cost and proof size. Shortest path search in transportation networks is unarguably one of the most important online search services nowadays (e.g., Google Maps, MapQuest, etc), with applications spanning logistics, spatial optimization, or everyday driving decisions. Often times, the owner of the road network data (e.g., a transport authority) provides its database to third-party query services, which are responsible for answering shortest path queries posed by their clients. It uses distance quantization and distance compression techniques forreducing the overall proof size is advantage of this paper.

III) EXISTING SYSTEMS

Data privacy techniques

Ensuring data privacy requires the data owner to outsource encrypted data to the service provider, and efficient techniques are needed to support querying encrypted data. A bucketization approach was proposed to enable efficient range queries over encrypted data, which was recently improved.

Shi et al. presented novel methods for multi-dimensional range queries over encrypted data. Some most recent proposals aim at secure ranked keyword search or fine-grained access control over encrypted data.

Ensuring query integrity

Secure remote query processing in tiered sensor networks is also studied. These schemes assume that some master nodes are in charge of storing data from regular sensor nodes and answering the queries from the remote network owner.

Disadvantages

1)None of these schemes consider spatial top-k queries .

2)As spatial top-k queries exhibit unique feature in that whether a POI is among the top-k is jointly determined by all the other POIs in the query region and that the query region cannot be predicted in practice.

IV) ANALYSIS AND DISCUSSION

There are two essential drawbacks with current top-k query services. First, individual LBSPs often have very small data sets comprising POI reviews. This would largely affect the usefulness and eventually hinder the more prevalent use of spatial top-k query services. The data sets at individual LBSPs may not cover all the Italian restaurants within a search radius. Additionally, the same restaurant may receive diverse ratings at different LBSPs, so users may get confused by very different query results from different LBSPs for the same query. A leading reason for limited data sets at individual LBSPs is that people tend to leave reviews for the same POI at one or at most only a few LBSPs's websites which they often visit. Second, LBSPs may modify their data sets by deleting some reviews or adding fake reviews and return tailored query results in favor of the restaurants that are willing to pay or against those that refuse to pay. Even if LBSPs are not malicious, they may return unfaithful query results under the influence of various attacks such as the Sybil attack whereby the same attacker can submit many fake reviews for the same POI. In either case, top-k query users may be misled by the query results to make unwise decisions.

V) 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 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.

Modules:

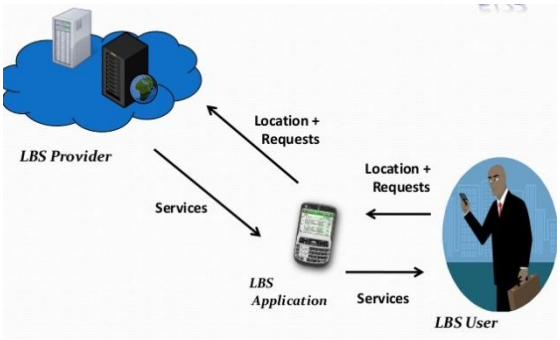
1)Data collector : It gathers the reviews about point of interest (POIs) from the data contributors.
2)Data Contributors : These are the people who submit POIs. It combines the data sets which gathered at individual LBSPs and provide centralized data sets.

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.

4)Geolocation : The 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.

SYSTEM ARCHIETECTURE :



VI) CONCLUSION:

LBSP is location-based service providers which collect POI from data collectors . Numerous techniques are developed in the last years like data privacy technique,ensuring query integrity,Secure query processing technique etc.The wide scope of LBSP is presented in this paper. The accuracy level is achieved without huge time consuming as in previous works. Although,Best position algorithm provide high accuracies

VII) FUTURE SCOPE

We need to work more on faithfully answer a top-k query, a LBSP need return the correct top-k POI data records as well as proper authenticity and correctness proofs constructed from authenticated hints.

References

[1] R. Zhang, Y. Zhang, and C. Zhang, "Secure Spatial Top-k Query Processing via Untrusted Location-Based Service Providers," IEEE Transaction On Dependable And Secure Computing, Vol. 12, NO. 1, Jan/Feb 2015.

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

[3] 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.

[4] 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.

[5] Man Lung Yiu, Yimin Lin, Kyriakos Mouratidis, "Efficient Verification of Shortest Path Search via Authenticated Hints," IEEE ICDE Conference 2010.