International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

Authentication of k Nearest Neighbor Query on Road networks using Voronoi diagram

P.Santhiyapriya[1], B.Chithra[2]

[1]Research Scholar, Computer Science Department, SNMV College of Arts and Science, Tamil Nadu ,India
[2]Head of the Department, Computer Technology Department, SNMV College of Arts and Science, Tamil Nadu ,India

---

Abstract - ***Outsourcing spatial information bases to the cloud provides a cost-effective and versatile means for information house owners to deliver spatial data to users of location-based services. However, within the information outsourcing paradigm, the third-party service supplier isn't invariably trustworthy, therefore, guaranteeing spatial question integrity is crucial.***

During this paper we tend to propose Associate in Nursing economical road network k-nearest-neighbor question verification technique that utilizes the network Voronoi diagram and neighbors to prove the integrity of query results. In contrast to previous work that verifies k -nearest-neighbor ends up in the metric space; our approach has to verify each the distances and therefore the shortest ways from the question purpose to its kNN results on the road network. We tend to evaluate our approach on real-world road networks along with each real and artificial point of interest datasets.

Our experiments run on Google golem mobile devices that communicate with the service supplier through wireless connections. The experiment results show that our approach results in compact verification objects (VO) and therefore the verification formula on mobile devices is economical, particularly for queries with low property.

Index Terms: *Spatial information outsourcing, location-based services, question authentication, road networks*

1. INTRODUCTION

1.1 Providing Database as a Service: In this paper, we have a tendency to explore the" database as service" paradigm and also the challenges introduced by that. Though it's attainable to purchase the required hardware, deploy information product, establish network property, and rent the skilled letter people World Health Organization run the system, as a standard answer, this solution has been obtaining progressively dearly-won and impractical because the information systems and issues become larger and more difficult.

The new paradigm challenges the ancient model of knowledge management followed by current organizations. Database service supplier provides seamless mechanisms for organizations to form, store, and access their databases. Moreover, the entire responsibility of information management, i.e., information backup, administration, restoration, information reorganization to reclaim house or to restore preferred arrangement of knowledge, migration from one database version to consecutive while not impacting availability will befall such a corporation. Users wish to access data can currently access it mistreatment the hardware and software package at the service supplier rather than their own organization's computing infrastructure. The appliance wouldn't be impacted by outages because of software package, hardware and networking changes or failures at the info service provider's site. This might alleviate the matter of buying, installing, maintaining and change the software package and administrating the system.

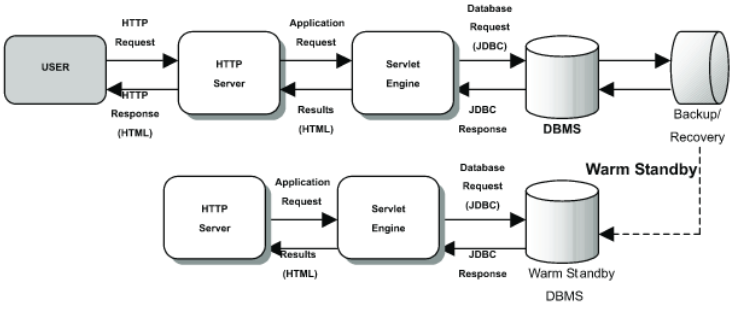

Fig1. System Architecture of NETDB2

The technological aspects of developing information as a service lead to new analysis challenges. Initial and foremost is that the issue of data privacy. Within the information service provider model, user knowledge has to reside on the premises of the information service supplier. Most firms read their knowledge as a terribly

valuable plus. The service supplier would need to supply enough security measures to protect the data privacy.

Second key challenge is that of performance. Since the interaction between the users and also the information service provider takes place in a completely different medium, the network, than it wills in ancient databases, there are potential overheads introduced by this design. Thus the sources of performance degradation and its significance ought to be determined.

Another challenge facing the information service supplier model is that of AN acceptable user interface. Clearly, the interface should be straightforward to use; nonetheless it has to be powerful enough to permit ease in building applications.

We have developed a information service on the web, known as NetDB2, AN experimental network based application service supplier (ASP) system. It has been operational over a year and utilized by range of universities to assist teaching information courses at completely different locations.NetDB2 provides information services as well as tools for application development, making and loading tables, and play acting queries and transactions to the users over the web.

In the system, knowledge and all of the necessary information products are placed on the server website. A user makes a connection to the system through the web and performs the knowledgebase queries and different relevant tasks over the information through an online browser or AN application programming interface like JDBC [6]. The planning principle of the system is to soak up quality and work on the server website as abundant as attainable.

The goal is to keep the shopper aspect lightweight, probably requiring solely an online browser to access the system. This makes the system transportable and readily out there from any location with none installation and configuration at the shopper aspect

By employing a internet browser based affiliation and internet interface, the user encompasses a likelihood to access and use the entire set of information product, which are professionally managed, without fear regarding the system administration, maintenance, upgrading the system etc.

1.2 Query Access Assurance in Outsourced Databases

Data are progressively collected during a distributed fashion. In such systems, information are generated by multiple purchasers and forwarded to a central server for management and query process. In brief, the distributed databases, as shown in Figure 2(a).

The remote access of the information inevitably raises the problem of trust, especially once the server is provided as a service by a third party that purchasers might not absolutely trust thus brings the requirements of auditing the question process efforts performed by the server.

There are 2 kinds of dishonest servers.

- ✓ Incorrect responses is send by a lazy servrerfor saving his computation resources. The inducement is to produce services to more purchasers or lower his operation value.
- ✓ A malicious server is willing to pay significant amounts of efforts (much over honestly death penalty the question if necessary) to govern the purchasers in order that they'll settle for wrong question results.

Not astonishingly, to protect against a malicious server is much tougher and a lot of pricey than defeating a lazy server. In several sensible applications, purchasers solely would like to worry a couple of lazy server rather than a malicious one. The selection of choosing a selected server's service has indicated an inexpensive degree of trust between information owners and also the server, so the prospect that the chosen server has any malicious intent ought to be low. However, the server still has lots of incentive to be lazy to lower his operation value or save his computation resources Formally, denote the number of work (computation and IO costs) that a server needs to do in honestly death penalty a batch of queries Q as W Q and the correct question answers for Q as A Q, and let the particular amount of labor the server has purchased Q be W′Q and the corresponding question results as A′Q. question execution assurance is to make sure the followings. If a consumer accepts A′Q, then W′Q/W Q ≥ θ holds with a high chance, where θ is some threshold price that's near 1.

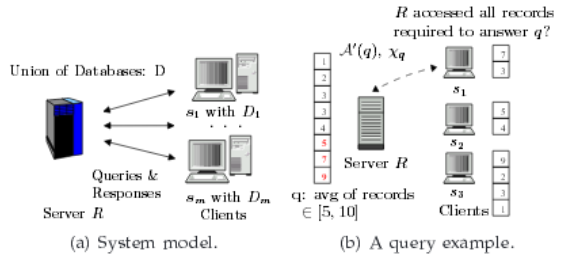

Fig 2. Query access assurance in distributed databases

Sion has designed a chic theme (based on the ringer's idea) that achieves the question execution assurance in a very single information owner model. It additionally wants the assumption that queries square measure submitted in batches. The core plan is to let the consumer execute a set of queries (from the batch to be submitted) regionally and procure their answers first. Challenge-tokens, victimization some unidirectional, collision resistant hash operate square measure then made based on these answers.

1.3 Authenticated indexing for outsourced spatial databases

A common framework for information outsourcing adopted from the relative literature is illustrated in fig 3.. The data owner (DO) obtains, through a key distribution center, a private and a public key. Additionally to the initial knowledge, the owner transmits to the LBS a collection of signatures needed for authentication. Whenever updates occur, the relevant knowledge and signatures also are forwarded to the LBS. The LBS receives and processes abstraction queries, (e.g., ranges, k-nearest-neighbors) from purchasers. The 3 parties have completely different machine power: a typical DO possesses a couple of workstations; the LBS run a server farm; a consumer is typically a mobile device (e.g., PDA) on battery power. Therefore, the LBS ought to perform most of the computation so as to attenuate the employment of the DO and, especially, the purchasers.

Fig 3. Query access assurance in distributed databases

Each incoming question initiates the computation of a verification object (VO) victimization the ADS. The VO (which includes the query result) is come to the consumer which will verify soundness and completeness victimization the general public key of the DO

In the majority of outsourcing systems, the initial construction further because the updates of the ADSs aren't outsourced, but performed regionally by the owner and transmitted to the service provider. Consequently, the DO should acquire the software package for maintaining the structures, and dedicate the hardware to perform the computations.

In this paper, we study one of those considerations, especially, the question integrity concern. That is, the way to make sure that the question results came back by SP area unit still trustworthy. As SP is not the real owner of the data, it would come back incorrect results to mobile purchasers out of its own interests, as an example, associate SP that hosts a collection of restaurants may favor some restaurants that pay a lot of advertising fees. Moreover, associate SP may come back suboptimal results to question purchasers by applying imperfect or inferior algorithms so as to avoid wasting computation resources.

On the opposite hand, with the growing quality of the Cloud, a lot of and a lot of security breaches and attacks on such systems have been brought to people's attention.

Fig 4.Database outsourcing architecture.

We tend to conjointly would like associate degree approach that will verify the path between 2 points. In this work, we tend to specifically focus on the k-nearest-neighbor (kNN) question verification on road networks and style verification schemes that support each distance verification and path verification . That is
The k resulting objects have the shortest distances to the question purpose among all the objects within the information,

The trail from the question purpose to every k -nearest-neighbor result is the valid shortest path on the network.
In order to verify the kNN question result on a road network, a naïve answer would be to come back the full road network and the purpose of interest (POI) dataset to the client to show correctness and completeness of

the result. However, this approach can incur a preventive communication overhead between SP and the consumer.

This paper subsumes and extends our earlier work [15] by providing a sound proof for our kNN question verification theme, which utilizes the network Voronoi diagram to come up with a compact VO, as well as making certain the completeness and correctness of the kNN question result with reference to each distances and paths.

Moreover, this thesis proposes a pre-computation based verification theme to accelerate the verification on mobile purchasers by utilizing the distance pre-computation. In addition, this thesis includes a discussion on updates of the outsourced information. Afterward, we tend to propose 2 update modes:
The one-by-one update mode
The batch update mode.

Finally, we tend to conduct intensive experiments using real-world and artificial datasets to evaluate the verification performance and therefore the information update price.

1.4 Problem Formulation

Formally, assume that m data owners forward their databases to the server R. we have a tendency to specialize in the case wherever the purchasers within the system are knowledge homeowners themselves.
The databases from all purchasers adjust to identical relative schema. For a client i, his information Di is a assortment of records. While not loss of generality, we assume that purchasers have distinct records, i.e., for ∀ i, j ∈ [1, m], i6=j, Di ∩ D j=∅. This can be simply possible by imposing a primary key field id r.
The server R maintains the union of all databases, denoted as D, and answers queries from clients, as shown in Figure 2(a). The quantity of records in D is | D|=N (hence P mi = 1 ni=N). Within the sequel, unless otherwise fixed, |X| for a set X denotes the number of components in X. A query q's selection predicate defines a group of records in every D i (and D) that satisfy its question condition.
Consider the subsequent example in SQL: "select sum (A3) from D where 10 ≤ A1 ≤ 100 group by A2". The choice predicate of this question is A1 ∈ [10,100] and it defines the set of records that has to be concerned so as to provide the final question result.
For a information Di and a question q, we have a tendency to denote this set of records as qi, t. we will apply the same definition to the information D and outline the set q t as well.
Obviously, q t=∪ mi=1 qi, t. we have a tendency to additionally outline ρ q = | q t|/|D| as the query property of q. The consumer expects a question answer A′ q for q and an evidence χ q that R has honestly accessed all records in q t. Let the particular set of records from q t that R has accessed to produce A′ q be q a, i.e., q a ⊆ q t. formally,

2. LITERATURE REVIEW

2.1 Spatial Outsourcing for Location-based Services

Query authentication was initial studied in the sepultureography literature. The Merkle Hash Tree (MH-tree) [M89] is a main-memory binary tree that hierarchically organizes hash1 values. Figure 5.1 illustrates a MH-tree covering eight data records d1-d8, every appointed to a leaf. A node N contains a hash value hN computed as follows: if N could be a leaf node, hN =H(dN), and dN is the appointed record of N,e.g.,h1 =H(d1);otherwise (N is an enclosed node), hN =H(hN.lc |hN.rc), where N.lc (N.rc) is that the left (right) kid of N severally, and "|" concatenates 2 binary strings, e.g.,h1-4 = H(h1-2 |h3-4).

In this paper we have a tendency to review previous work connected to k-nearest-neighbor question and question authentication strategies for outsourced abstraction databases.

2.2 Nearest Neighbor question

Papadiaset al. [16] projected techniques for NN queries in abstraction network databases by progressively increasing road segments around the question point. In addition, associate degree approach primarily based on the network Voronoi diagram was introduced in [17] for evaluating NN queries on abstraction networks. The key plan is to partition a giant network into a range of little Voronoi regions and then pre-compute distances each at intervals and across the regions. Hu et al.[18] bestowed associate degree index structure for distance computation and question process over long distances.

2.3 Question Authentication for Outsourced abstraction Databases

Hacigümüs et al. were the initial to propose the plan of outsourcing databases to third-party service suppliers in their pioneering work [2]. Afterward, varied question authentication solutions are projected for outsourced relational databases [21]–[27]. Mykletun et al. [23] provided techniques supported digital signature aggregation to confirm data integrity and legitimacy for outsourced information bases. However, the techniques cannot assure completeness of the result set

Pang et al.[24] used AN mass signature in order to sign every record with the data from neighboring records by forward that each one the records are sorted in an exceedingly sure order. Their mechanism helps users verify that question results are each complete and authentic. In addition, the challenge token theme, introduced by Sion [25], is for a server running outsourced databases to give a proof of the actual question execution, which is then checked at the consumer facet for integrity verification. Compared to [24], the theme conjointly supports a lot of question types while not forward that all the records are sorted. Nonetheless, none of the techniques are specifically designed for abstraction databases

2.4 Voronoi Diagrams

Given a set of distinct objects P={P1,P2…, Pt}in R2, the Voronoi diagram of P, denoted as VD (P), partitions the space of R2 into t disjoint regions, such that every object pi in P belongs to solely one region and each purpose in that region is nearer to pi than to any different object of P in the Euclidian area. The region around pi is referred to as the Voronoi two-dimensional figure or Voronoi cell of pi, denoted as VC (pi), and pi is the generator of the Voronoi cell. Therefore, the Voronoi diagram of P is the union of all Voronoi cells

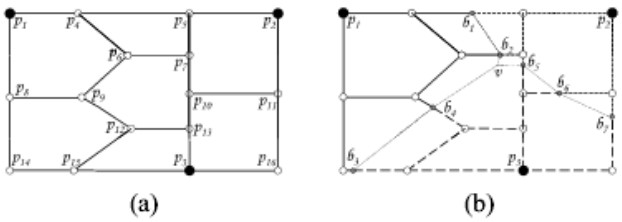

Fig. 5. Example of road network and network Voronoi diagram:(a) Road network. (b) Network Voronoi diagram.

2.5 Road Network Voronoi Diagrams

A road network system are often modeled as a weighted graph G(V,E,W) consisting of a set of vertices V=and a set of edges E =connecting vertices to create a graph. W represents the price of every edge up E, as an example, the space, the traveling time or the toll fees. Let P ⊂ V be a set of points of interest (POI). We tend to assume all POIs area unit restricted on road network segments (edges).

2.6 Authentication Data Structure

To support the question verification, we tend to want a well-defined authentication knowledge structure (ADS) engineered on the outsourced data, that ought to be cryptographically signed by DO to ensure knowledge integrity. think about the outsourced information with a set of POIs P over associate degree underlying road network G. In this work, we tend to propose associate degree elaborate authentication knowledge structure so as to support k-nearest-neighbor question verification on road networks wherever the distances from the query purpose to things square measure measured by the shortest path on the graph with relation to the sting weight W.

2.8 Verifying NN On Road Networks

Nearest neighbor (NN) queries on road networks are common abstraction question varieties for location-based services. Specifically, kNN queries modify mobile shoppers to retrieve the nearest k POIs from the information with regard to the network distance to the location of the question purpose. A verifiable kNN question requests a verification object (VO) from SP that contains not solely the kNN question result, but also a proof to justify that the kNN result is correct and complete.

2.9 Pre-computation primarily based Verification theme

During the verification in algorithmic rule one, the shopper wants to reason the shortest distance and path from the query purpose q to candidate neighbor generators in lines 14 and twenty by victimization Dijkstra [36] or A*[37] algorithmic rule. Unfortunately, these distance computations are sometimes expensive; particularly as the sub graph network g grows large. From Fig.5, we have a tendency to will observe that every path from q to any dish, except the 1st nearest neighbor, always passes through one or additional border points.

2.10 Database update

We have a tendency to discuss however DO updates its outsourced database for either dish updates or road network updates. For different styles of updates, DO follow the same update procedure as follows. Initial of all, DO wants to update the network Voronoi diagram.

Secondly, it ought to update those affected authentication knowledge structures and renew their signatures.

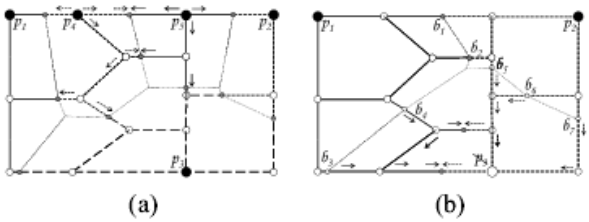

Fig 7.Database update - POI update examples: (a) POI insertion. (b) POI deletion.

3. PROPOSED METHOD

3.1 Future Work Trust-Preserving Set Operations

Trust-Preserving Set Operation drawback is projected by Ruggero et.al.in paper [24]. In this drawback, the party performing arts the computation doesn't got to be trustworthy, but the result is a group that is trustworthy to a similar extent because the original input. The techniques have a spread of potential applications like addressing the matter of firmly reusing content-based search ends up in peer-to-peer (P2P) networks. Given Associate in Nursing example model with 2 trustworthy supply nodes, s1, s2, every store Associate in Nursing index in the variety of S1, S2; Associate in Nursing un trusted directory d; and a consumer c, commonplace set operation (such as union, difference, and intersection) are performed with drawback raised on however to construct a theme that enables c to verify that d didn't falsify the results of the question. Current answer of this drawback is accomplished by requiring trustworthy nodes to sign appropriates, outlined digest of generated sets, and every such digest consists of Associate in Nursing RSA accumulator and a Bloom filter. 2 styles of attacks can be performed:

- ✓ Insertion attack
- ✓ Deletion attack.

3.2 Authenticating Aggregation Queries in Outsourced information Systems

Current cooking pan on question authentication has centered on learning the final choice and projection queries. Another necessary facet of question authentication in outsourced database system that has not been thought of nonetheless is handling aggregation queries. When process Associate in nursing aggregation question, though intermediate information can be concerned during the computation, solely result answers got to be came back. However, during a Third party Publisher System, it'd be impossible for the user to certify the came back answer from publisher while not the data of the elaborate information. During this case, we address the state of affairs wherever a user has the rights to grasp (at least some of) the elaborate data underlying the aggregation it's given.

The most easy answer is, alongside the aggregation result came back, the publisher sends all the answer-related elaborate information to user. The user may initial verify the came back information with authentication techniques like Merkle Hash Tree or Signature Chain [29] strategies, then work out the result and verify believability its own. However, with this methodology, a "sum" question would possibly need the publisher returns all the values to the user, during this case this trivial answer is extremely inefficient.

There are several drawbacks:

- ✓ Communication Cost: the communication between the publisher and therefore the user might be expensive.
- ✓ Network Traffic: network traffic can be caused throughout information transmission especially once such great amount of knowledge transferred.
- ✓ Access Control: typically, the user won't be inspired to grasp the elaborate data of Associate in nursing aggregation question.
- ✓ Computation Workload: The user's work can be too serious once complicate calculations needed.

3.3 Reducing Verification area by Euclidian Restriction

By applying the Euclidian restriction rule, we tend to solely want to reason the network distance from q to p3 and p4, and discard p6 and p7 as they're more faraway from q than p2.The network k-nearest-neighbor question verification process is shown in formula one. The inputs to the formula are the question purpose q, the verification object VO, and the parameter k. The VO contains the genuine network Voronoi object of each dish in the k

NN result, including the generator dish, the Voronoi cell of the generator and its neighbors

The algorithmic rule starts with the initial NN p1 by checking whether the question purpose q belongs to the road segments inside the Voronoi cell V (p1) of p1(lines 3-5). If not, p1 is not the first NN and therefore the verification method fails. Otherwise, p1 is verified because the initial NN and is other to the Visited set on line 6. Next, the road segments within the V (p1) are merged with g which could be a sub graph of the road networks within the Voronoi cells of already retrieved NNs, and all the neighbors of p1 are inserted into H and Visited set. The next for loop (lines 8-40) iterates through every object within the k NN result set obtained from VO (line 9). If the present NN p is not in H (the current NN came isn't one in every of the Voronoi neighbors of antecedently verified NNs), then p is not the i th NN of q(according to Property 6), and therefore the verification fails on line 11. Otherwise, p is one in every of the neighbors of already verified NNs, and that we ought to verify that the network distance of p is the smallest among all the Voronoi neighbors and identical to the distance in the question result came by SP (lines 13-39).

Algorithm 1 VerifyNetwork$k$NN(q,$\mathcal{VO}$,k)

1. $H \leftarrow \emptyset$; *Visited* $\leftarrow \emptyset$; $g \leftarrow \emptyset$;
2. $\langle p, V(p), Nbrs\rangle \leftarrow \mathcal{VO}.getNN(1)$;
3. **if** $(q \notin V(p))$ **then**
4. **return false**;{the 1^{st} NN fails by Property 5}
5. **end if**
6. *Visited.add*(p);
7. $g \leftarrow V(p)$; $H \leftarrow Nbrs$; *Visited* $\leftarrow Nbrs$;
8. **for** $i = 2$ to k **do**
9. $\langle p, V(p), Nbrs\rangle \leftarrow \mathcal{VO}.getNN(i)$;
10. **if** $p \notin H$ **then**
11. **return false**;{Property 6}
12. **end if**
13. $g \leftarrow g \cup V(p)$;
14. $lb \leftarrow computeSP(g, q, p)$; {Lemma 2}
15. $minDist \leftarrow MaxValue$; $minPt \leftarrow null$;
16. **for all** $(h \in H)$ **do**
17. **if** $(h.ed > lb)$ **then**
18. *break*; {apply Euclidean restriction}
19. **else**
20. $h.nd = computeSP(g, q, h.poi)$;
21. **if** $(h.nd < minDist)$ **then**
22. $minDist \leftarrow h.nd$;
23. $minPt \leftarrow h$;
24. **end if**
25. **if** $(minDist < lb)$ **then**
26. **return false**; {$minPt$ is closer to q than p}
27. **end if**
28. **end if**
29. **end for**
30. **if** $(p == minPt.poi$ && $p.nd == minDist)$ **then**
31. $H.remove(minPt)$;{the i^{th}NN is verified}
32. **for all** $(nbr \in Nbrs)$ **do**
33. **if** $(nbr \notin Visited)$ **then**
34. $H \leftarrow H \cup nbr$; $Visited \leftarrow Visited \cup nbr$;
35. **end if**
36. **end for**
37. **else**
38. **return false**;{the i^{th}NN is not verified}
39. **end if**
40. **end for**
41. **return true**;

4. EXPERIMENTAL STUDY

In this paper we have a tendency to evaluate the performance of the network Voronoi diagram-based k - nearest-neighbor question verification approach through experiments. Our information outsourcing framework contains 2 phases:

- ✓ The offline information transformation part on DO
- ✓ The on-line part on SP and shoppers.

In the offline part, DO computes the network Voronoi diagram on the dish set and the under- lying road network, and it then generates a signature for each dish by incorporating the authentication data into every dish object. In the on-line part, SP evaluates queries and sends results to question shoppers on behalf of the DO, and then the shopper verifies the question result. Our implementation for the on-line question analysis and verification is in Java. The server-side program (SP) runs on a Linux Server with AN Intel Core2 couple a pair of.13GHz CPU and 4GB memory. Meanwhile, the client-side question verification program runs on a HTC EVO 3D mobile device with the Google mechanical man OS that communicates with the SP server via web connections through WiFi. The cryptographic operations are enforced victimization the SHA-256 digest rule (with 32-byte hash digest) and RSA-1024 signature rule (with 128-byte keys) from [39]. Our experiments were performed on 2 real-world road networks obtained from [40], [41]: (i)CA which consists of the major freeways and highways within the state of California with a complete of twenty one, 048 nodes and twenty two, 830 edges, and (ii) BAY which contains highways as well as surface streets with 174, 956 nodes and 223, 001 edges within the San Francisco Bay Area, California. though the second network (BAY) covers a smaller geospatial region, the size of the network is larger than the California road network thanks to the inclusion of surface streets. In addition, we have a tendency to use each real and artificial dish datasets on these 2 road networks. For the CA road network, we use a real dish dataset originating from U.S. Census [41], [42] representing airports, hospitals, schools, etc. From the state of California. In addition, to study the impact of the different density of POI datasets in our system, we experimented with a few synthetic POI datasets generated on the BAY road network.

4.1 VO Size over k

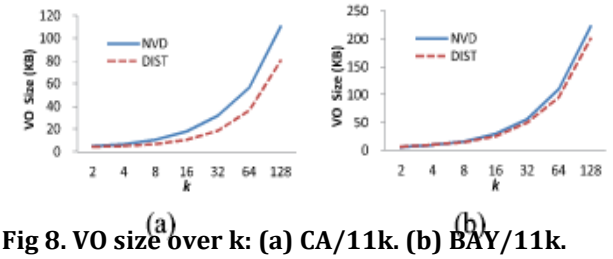

Fig 8. VO size over k: (a) CA/11k. (b) BAY/11k.

Fig.8 (a) shows the computation cost for generating authenticated network Voronoi cells (NVD) as described in, and the additional cost for pre-computing the distance and hashed path table within each cell (DIST). Fig.8 (b) describes the size of the original datasets (ORIG), the extra storage overhead for storing the network Voronoi cells, neighbors, signatures (NVD) and the additional cost for storing the distance and hashed path table (DIST). As we can see in Fig. 8(a), the computation cost increases significantly with the size of the road network and the number of POIs, especially the time spent for pre-computation for the BAY network. This is because when there are more POIs on the network, more network Voronoi cells are generated, resulting in a higher time cost for computing the distances and paths. Similarly, extra storage overhead is required to store Voronoi cells, neighbors, and signatures in the NVD scheme. Additionally, ore space is needed for storing the distance and hashed path tables in the DIST scheme as shown in Fig. 8 (b).

4.2 Communication time over k on mobile clients

In the second set of experiments, we investigate the size of the VO over the query parameter k. Fig. 13(a) presents the VO size over k on the CA road network with 11k POIs,

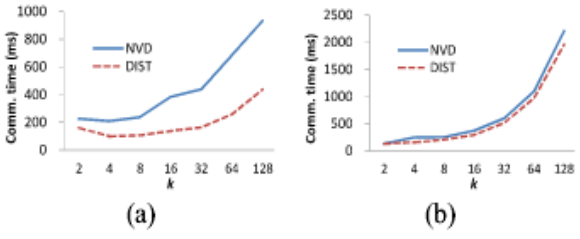

Fig 9. Communication time over k on mobile clients: (a) CA/11k. (b) BAY/11k.

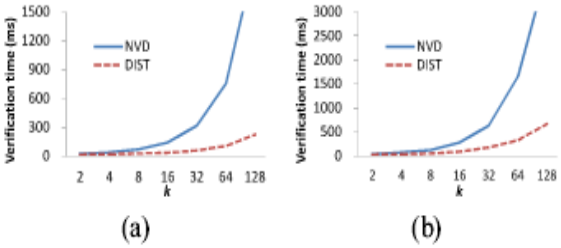

Fig 10. Verification time over k on mobile clients: (a) CA/11k. (b) BAY/11k.

And Fig. 9 (b) shows the VO size on the BAY road network also with eleven k POIs. The results show that on each road networks, the VO sizes within the DIST theme are smaller than in the NVD theme. This is as a result of in the DIST theme, the distance table is came back instead of the original road network within the Voronoi cells of the k NN results (except for the first NN), ensuing in a smaller VO size particularly for queries with k larger than eight. Our next set of experiments studies the communication time for evaluating network k-nearest-neighbor queries on mobile devices. The communication time is measured by the trip time price per question for a consumer.

Fig. 10 shows the communication cost over k on each the CA road network and therefore the BAY road network, every with eleven k POIs. The next set of experiments investigates the computation time price for corroboratory k-nearest-neighbor results on mobile devices. once receiving the VO, the mobile consumer starts the verification algorithmic program (Algorithm 1) to verify the correctness and completeness of the k NN results.

4.3 Verification cost over density of POI

The verification time price over k on the CA and BAY networks is shown in fig 11. Note that the verification time additionally includes the signature verification time, that includes computing a hash digest based mostly on the raw knowledge and corroboratory the sig-nature. Taking the BAY/11K dataset as AN example, the average size of a network Voronoi cell is regarding one.75KB, and hashing and corroboratory one.75KB knowledge takes regarding one.3ms on a mobile device. The experiments demonstrate that on each networks, the DIST scheme is considerably additional economical in corroboratory the network k NN result than the NVD theme, particularly once the worth of k is larger than sixteen. This is due to the truth that when k increases, the

sub graph within the union of the Voronoi cells of the k NN results grows. Our next set of experiments studies the VO size and verification time price on the BAY road network by variable the Value of ρ (POI density) from one hundred and twenty fifth (2.2 k POIs) to 100% (22 k POIs).

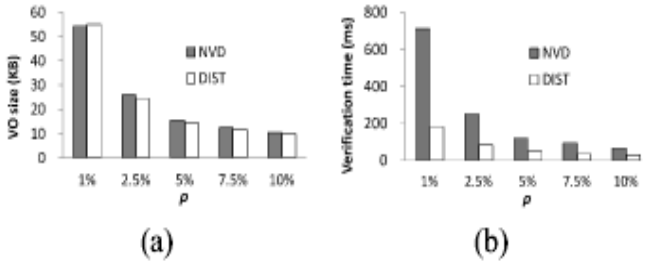

Fig 11. Verification cost over density of POI: (a) VO size. (b) Verification time.

4.4 Database update cost

Fig. 12 (a) shows the dimensions of VO over ρ and Fig. 12 (b) presents the verification price over ρ. All the experiments are performed by setting the question parameter k to 8. The results show that as the worth of ρ increases, the size of VO declines.

This is often as a result of once there are a unit fewer POIs on the network; the network Voronoi cell of every dish covers a larger region with additional road segments. Therefore, the size of every network Voronoi cell is larger, ensuing in larger VO size. For the same reason, the verification price on a sparse dish dataset is higher than on a dense dish dataset, as shown in Fig. 12 (b).

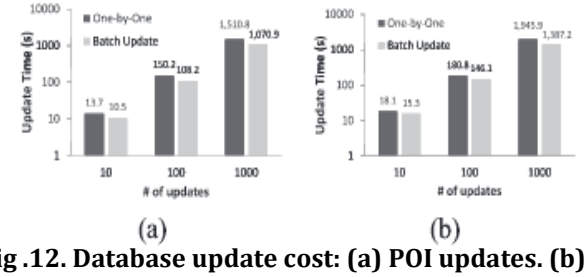

Fig .12. Database update cost: (a) POI updates. (b) Edge updates.

Fig. 12 shows the update price on DO to method a number of dish updates and edge updates on the BAY/11K Dataset, severally. The coordinate axis corresponds to the amount of updates, and coordinate axis shows the update time.

The update time includes prices on change the network Voronoi diagram, change all affected echt network Voronoi cells, the connected pre-computation, and refreshing signatures.

The results show that the update time will increase linearly with the range of updates. On average, each update may be processed in one.5-2 seconds (30-40 updates per minute) in the one-by-one mode.

Moreover, since our data structure supports parallel updates, the update price in batch mode achieves 15%-30% performance improvement over the one-by-one update mode.

Our last set of experiments studies however info size affects the size of VO . 2 larger real-world road networks from [43] are used:(i) COL , the road network of Colorado with a complete of 435, 666 nodes and 528, 533 edges, and (ii) FLA , the road network of American state, with 1, 070, 376 nodes and one, 356, 399 edges

4.5 Effects of database size on VO size

A artificial dish dataset with 5% density (ρ= 5%) is generated on every network. Fig. 13 shows that the VO size remains roughly the same on the two road networks of various sizes. this is often as a result of the dimensions of VO is directly connected to the average size of Network Voronoi Cells (NVC) made based mostly on the road network, not the total size of the road network.

The average NVC size is around one.75 K on each network. Hence the VO sizes are similar over k.

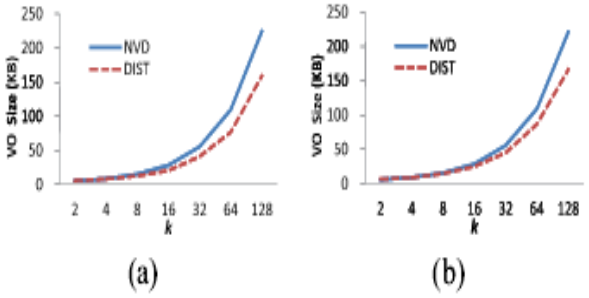

Fig.13. Effects of database size on VO size: (a) COL. (b) FLA.

We may set our goal of this drawback is to cut back the communication price between the user and publisher furthermore as come through high accuracy of aggregation result.

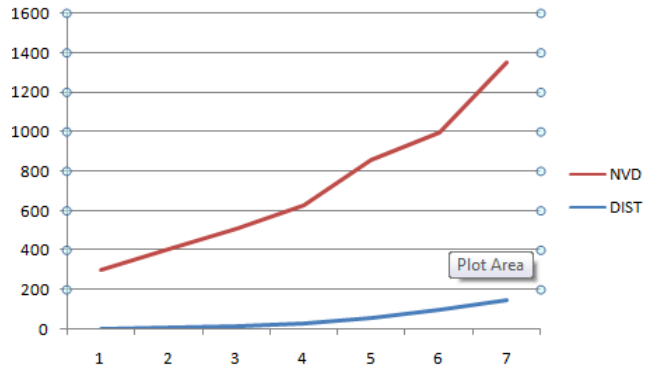

Fig 14. Comparison for NVD&DIST method for data collecting

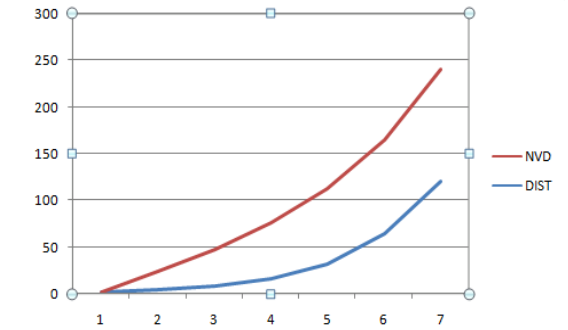

Fig 15. Number of neighbor node based selected query

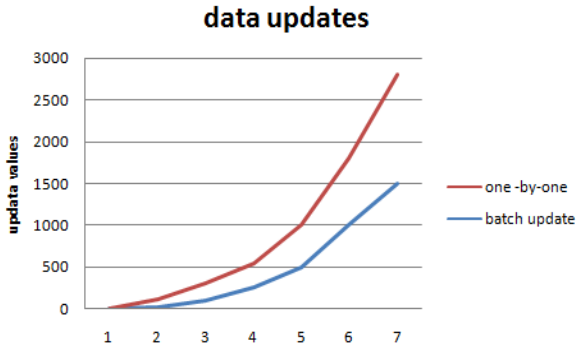

Fig 16 Comparison of signal file and batch files

5.CONCLUSION

Outsourcing of abstraction databases for supporting location-based services has become a trend in recent years because of the economy of scale. Existing solutions area unit designed for information privacy protection or question integrity auditing, severally, instead of considering each information privacy and question integrity as a full. We have introduced question integrity assured algorithms for each vary question and k-nearest-neighbor question with area coding techniques to secure information privacy. We have incontestable through simulation results that our mechanisms have remarkable performance. For future work, we tend to commit to extend our algorithms to support a lot of abstraction question varieties like abstraction be a part of, abstraction path queries, etc.

Recent advances in location-based services and device networks, as well as the quality of web-based access to spatial knowledge (e.g., MapQuest, Google Earth, etc.), necessitate question authentication for outsourced and replicated multi-dimensional knowledge. During this thesis we tend to propose the MR-tree, an authenticated index supported the Merkle Hash tree and also the R*-tree. Our methodology outperforms the simplest current resolution by many orders of magnitude in several necessary metrics such as construction value, index size and verification overhead. Moreover, we tend to develop the MR*-tree, an alternate to the MR-tree, that considerably reduces the communication overhead between the LBS and also the shopper. additionally, both the MR-tree and also the MR*-tree are absolutely outsourced, in the sense that their maintenance is performed entirely by the LBS, and will be verified with negligible effort by the data owner.

We tend to conclude our contributions with an intensive experimental study that validates the effectiveness and efficiency of the planned structures. As future work, we tend to commit to extend our solutions to the problem of authenticating different question sorts that can't be reduced to ranges, like abstraction joins (e.g., "find all cities that are crossed by a river"), aggregates ("find the amount of objects in an exceedingly given vary rather than their IDs"), etc.

Another direction issues additional versatile models that permit the shopper decide whether or not a proof of question results is needed from the LBS.

A brute-force resolution, for instance, is to stay associate ordinary index for question process and a separate ADS for authentication. Finally, it'd be attention-grabbing to analyze the integration of privacy-preserving techniques and question authentication models to achieve an answer with each security guarantees.

In this paper we tend to studied the question verification drawback for k-nearest-neighbor queries on road networks. . In addition to the basic verification algorithmic program (NVD), Associate in nursing improved version (DIST) with pre-computed distances among every network Voronoi cell is bestowed for k NN question verification to more scale back the verification price on mobile shoppers.

Secondly, during this paper, we only thought-about one information owner party. However, in practice, there may well be multiple information house owners. For instance, the POIs and the road networks will return from 2 completely different data house owners.

Hence, however to handle the question verification problem in the presence of multiple information house owners is additionally an interesting direction to explore. Last however not least, how to handle extremely frequent network updates, such as traffic changes throughout rush hours, is additionally a terribly difficult problem.

REFERENCES

[1] F. Gens. (2011, Oct. 20). IDC's new IT cloud services forecast: 2009-2013 [Online]. Available: http://blogs .idc.com/i.e./?p = 543

[2] H. Hacigümüs, S. Mehrotra, and B. R. Iyer, "Providing info as a service," in Proc. 18th ICDE, San Jose, CA, USA, 2002, pp. 29–38.

[3] Google Maps [Online]. Available: http://maps. google.com/

[4] C. Cachin and M. Schunter, "A cloud you will trust, "IEEE Spectrum , vol. 48, no. 12, pp. 28–51, Dec. 2011.

[5] A. Fiat, "Batch RSA," J. Cryptology, vol. 10, no. 2, pp. 75–88, 1997.

[6] W. Cheng and K.-L. Tan, "Query assurance verification for out-sourced multi-dimensional databases," J. Comput. Secur. , vol. 17, no. 1, pp. 101–126, 2009.

[7] Y. Yang, S. Papadopoulos, D. Papadias and G. Kollios, "Spatial outsourcing for location-based services," in Proc. IEEE twenty fourth ICDE, Cancun, Mexico, 2008, pp. 1082–1091.

[8] Y.Yang, S. Papadopoulos, D. Papadias and G. Kollios, "Authenticated classification for outsourced spacial databases," VLDB J., vol. 18, no. 3, pp. 631–648, Jun. 2009.

[9] K. Mouratidis, D. Sacharidis, and H. Pang, "Partially materialized digest scheme: Associate in Nursing economical verification technique for outsourced databases," VLDB J., vol. 18, no. 1, pp. 363–381, 2009.

[10] W.-S. Ku, L. Hu, C. Shahabi and H. Wang, "Query integrity assurance of location-based services accessing outsourced spatial databases," in Proc. 11th Int. Symp. SSTD, Aalborg, Denmark, 2009, pp. 80–97.

[11] W.-S. Ku, L. Hu, C. Shahabi and H. Wang, "A question integrity assurance theme for accessing outsourced spatial databases," GeoInformatica, vol. 17, no. 1, pp. 97–124, 2013.

[12] L. Hu, W.-S. Ku, S. Bakiras and C. Shahabi, "Verifying spatial queries exploitation voronoi neighbors," in Proc. 18th GIS, SanJose, CA, USA, 2010, pp. 350–359.

[13] L. Hu, W.-S. Ku, S. Bakiras and C. Shahabi, "Spatial question integrity with voronoi neighbors," IEEE Trans. Knowl. Data Eng., vol. 25, no. 4, pp. 863–876, Apr. 2013.

[14] M. L. Yiu, E. Lo, and D. Yung, "Authentication of moving kNN Queries," in Proc. IEEE twenty seventh ICDE, Hannover, Germany, 2011, pp. 565–576.

[15] L. Hu, Y. Jing, W.-S. Ku and C. Shahabi, "Enforcing k nearest neighbor question integrity on road networks," in Proc. 20th SIGSPATIAL/GIS, Redondo Beach, CA, USA, 2012, pp. 422–425 (short paper).

[16] D. Papadias, J. Zhang, N. Mamoulis and Y. Tao, "Query processing in spatial network databases," in Proc. 29th VLDB, Berlin, Germany, 2003, pp. 802–813.

[17] M. R. Kolahdouzan and C. Shahabi, "Voronoi-based K nearest neighbor hunt for spatial network databases," in Proc. 13th Int. Conf. VLDB , Toronto, ON, Canada, 2004, pp. 840–851.

[18] H. Hu, D. L. Lee and V. C. S. Lee, "Distance compartmentalization on road networks," in Proc. 32nd Int. Conf. VLDB, 2006, pp. 894–905.

[19] H. Samet, J. Sankaranarayanan and H. Alborzi, "Scalable network distance browsing in spatial databases," in Proc. SIGMOD, New York, NY, USA, 2008, pp. 43–54.

[20] K. C. K. Lee, W.-C. Lee, B. Zheng and Y. Tian, "ROAD: A new spatial object search framework for road networks," IEEE Trans. Knowl. Data Eng., vol. 24, no. 3, pp. 547–560, Mar. 2012.

[21] H. Hacigümüs, B. R. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted information within the database-service-provider model," in Proc. SIGMOD, Madison, WI, USA, 2002, pp. 216–227.

[22] H. Pang and K.-L. Tan, "Authenticating question results in edge computing," in Proc. ICDE, Washington, DC, USA, 2004, pp. 560–571.

[23] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced informationbases," TOS, vol. 2, no. 2, pp. 107–138, May 2006.

[24] H. Pang, A. Jain, K. Ramamritham, and K.-L. Tan, "Verifying completeness of relative question leads to information business," in Proc. SIGMOD Conf., Baltimore, MD, USA, 2005, pp. 407–418.

[25] R. Sion, "Query execution assurance for outsourced databases," in Proc. 31st Int. Conf. VLDB, Trondheim, Norway, 2005, pp. 601–612.

[26] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in Proc. SIGMOD,, Chicago, IL, USA, 2006, pp. 121–132.

[27] M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity auditing of outsourced data," in Proc. 33rd Int. Conf. VLDB, Vienna, Austria, 2007, pp. 782–793.

[28] S. Papadopoulos, L. Wang, Y. Yang, D. Papadias and P. Karras, "Authenticated Multistep nearest Neighbor

Search," IEEE Trans. Knowl. Data Eng., vol. 23, no. 5, pp. 641–654, May 2011.
[29] M. T. Goodrich, R. Tamassia, N. Triandopoulos and R. Cohen, "Authenticated information structures for graph and geometric searching," in Proc. CT-RSA, point of entry, CA, USA, 2003, pp. 295–313.
[30] M. L. Yiu, Y. Lin and K. Mouratidis, "Efficient verification of shortest path search via documented hints," in Proc. ICDE ,Long Beach, CA, USA, 2010, pp. 237–248.
[31] H. Hu, J. Xu, Q. Chen and Z. Yang, "Authenticating location-based services while not compromising location privacy," in Proc. SIGMOD, Scottsdale, AZ, USA, 2012, pp. 301–312.
[32] A. Okabe, B. Boots, K. Sugihara, and S. N. Chiu, Spatial Tessellations: ideas and Applications of Voronoi Diagrams. New York, NY, USA: Wiley, 2000.
[33] M. Erwig, "The graph voronoi diagram with applications, Netw" vol. 36, no. 3, pp. 156–163, Oct. 2000.
[34] M. Sharifzadeh and C.Shahabi, "VoR-Tree: R-trees with voronoi diagrams for economical process of spatial nearest neighbor queries," PVLDB, vol. 3, no. 1, pp. 1231–1242, Sept. 2010.
[35] U. Demiryurek and C. Shahabi, "Indexing network voronoi diagrams," in Proc. 17th Int. Conf. DASFAA, Busan, Republic of Korea, 2012, pp. 526–543.
[36] E. W. Dijkstra, "A note on 2 issues in connation with graphs," Num. Math. , vol. 1, no. 1, pp. 269–271, Dec. 1959.
[37] P. E. Hart, N. J. Nilsson, and B. Raphael, "A formal basis for the heuristic determination of minimum value methods," IEEE Trans. Syst. Sci. Cybern. , vol. 4, no. 2, pp. 100–107, Jul. 1968.
[38] T. H.Cormen, C. E. Leiserson, R. L. Rivest, and C.Stein, Introduction toAlgorithms. Cambridge, MA, USA: Massachusetts Institute of Technology Press, 2009. Oracle firm.Java SE Security. Retrieved on June twelve,2012[Online].Available: http://www.oracle.com/technetwork/ java/javase/tech/index-jsp-136007.html
[39] F. Li, D. Cheng, M. Hadjieleftheriou, G. Kollios, and S.-H. Teng, "On trip designing queries in spatial databases," in Proc. SSTD, Angra dos Reis, Brazil, 2005, pp. 273–290.
[40] F. Li. (2012 Apr. 2). Real Datasets for spatial Databases [Online]. Available: http://www.cs.utah.edu/~lifeifei/SpatialDataset.htm
[41] U.S. geologic Survey [Online]. Available: http://www.usgs.gov/
[42] DIMACS. (2013 Jun. 13). 9th DIMACS Implementation Challenge -Shortest methods
[43] [Online]. Available:http://www.dis.uniroma1.it/challenge9/download.shtml

BIOGRAPHIES

1. Mrs.Santhiya Priya completed her MSc Computer Science in udumalpet Govt College and she is persuing her Mphil (Computer Science) in SNMV College of Arts and Science, Coimbatore. Her area of interest is Datamining.

2. Mrs.B.Chithra is persuing Ph.D in computer science. She is the Head of Computer Technology Department in SNMV College of Arts and Science. She is Having 10 Years of teaching experience.Her area of interest is Data mining.