EXPERIMENTAL ESTIMATED K NEAREST NEIGHBOR QUERIES WITH POSITION AND QUERY PRIVACY

Bade. Anil Kumar[1], S. L. V. V. D. Sarma[2]
[1]PG Scholar, [2]Asst Prof
St. Mary's Group of Institution, Chebrolu, Guntur, AP, India

***ABSTRACT:* Mobile devices equipped with positioning capabilities (e.g.,GPS) will ask location-dependent queries to Location primarily based Services (LBS). To protect privacy, the user location should not be disclosed. Existing solutions utilize a sure anonymize between the users and therefore the LBS (in recent years, the situation of a query could reveal security information regarding the mobile user). During this paper, we are proposed Paillier public-key cryptosystem and may offer each location and query privacy. To preserve question privacy, our basic resolution permits the mobile user to retrieve one variety of POIs.**

I. INTRODUCTION

Location-Based service providers (LBS) supply remote mobile clients with querying services on points-of-interest (e.g., restaurants, cafes, gas stations). Mobile consumer Q problems a moving k nearest neighbor (kNN) question so as to seek out k points-of-interest highest to q endlessly whereas traveling. Such queries have various mobile applications. For instance, a traveler could issue a moving kNN query to get k nearest restaurants endlessly once walking during a town. A driver issues a moving kNN question to seek out k nearest gas stations continuously whereas driving.LBS that supply kNN querying services typically come mobile purchasers a secure region in addition to the query results. Given a moving consumer q, its safe region contains all potential query locations that have similar results as q. In different words, the consumer only problems a replacement query to the LBS (for the newest results) once she leaves the safe region. This optimization considerably reduces the communication frequency between the service supplier and also the clients. Sadly, the query results and safe regions returned by LBS might not forever be correct. For example, a hacker could have infiltrated the LBS's servers in order that results of kNN queries all include a specific location (e.g., the White House). moreover, it's potential that the LBS is self compromised, and therefore ranks sponsored facilities higher in its query results.

The LBS an excessively large safe region to the purchasers for the sake of saving computing resources and communication information measure; On the opposite hand, the LBS could value more highly to come to fault tiny safe regions in order that the clients need to request new safe regions additional oftentimes, if the LBS charges fee for every request, or if the LBS would like to spice upits request rate. Recently, techniques for authenticating query results have received lots of attentions. Most authentication techniques are supported Merkle tree, which is an attested arrangement (ADS) for guaranteeing the correctness of query results on an information set. Recently, Yang et al. developed an ADS known as Merkle R-tree (MR-tree) for authenticating queries on a spacial information set, and additionally an improved tree known as MR*-tree. Upon receiving a query issued by a mobile consumer, the LBS not only retrieve the question results but additionally cipher a verification object from the tree. Specifically, the verification object consists of bound tree entries that may be later used by the consumer to verify the correctness of results.

The issue of authenticating moving kNN queries, however, has not been self-addressed nonetheless. Existing authentication techniques for static spatial queries have their authentication target as the query results, being a set of the information set. In distinction, the authentication target of moving queries includes the safe region that may be a geometric form computed by the LBS at run time however not a part of the information set. Since a secure region is defined supported each query results furthermore as points not within the query results, the missing of a non-result purpose within the verification object could also fail the authentication of the safe region. Thus, the above techniques cannot facilitate in authenticating moving kNN queries.

This paper is dedicated to addressing this difficult issue of authenticating moving kNN queries. During this paper, we improve the best authentication methodology and prove that it achieves verification object optimality. This optimality notion guarantees that the verification object contains the minimum information points and tree entries (with respect to the given tree). We tend to additionally present new optimization techniques for reducing the computation value and also the communication value of our authentication methodology. It's particularly necessary to minimize the mobile client's total communication value because it translates to the client's money (paid to the mobile network provider).

II. RELATED WORK

Authentication techniques are developed for a range of queries, together with relative queries, window queries, spatial queries, text similarity queries, shortest path queries, moving kNN queries, moving vary queries, and sub graph search. However, all existing authenticated information Structures(ADS) are either irrelevant or inefficient, since the authentication of kNN queries involves corroboratory each spatial proximity and text relevancy. Moreover, authenticating a kNN query includes confirming each the top-k result and also the accompanying safe zone. The safe zone is calculated supported both the objects within the top-k result and also the objects not within the top-k result, so missing a non-result object could cause asafe zone to fail within the authentication. Though authentication techniques for moving kNN queries and moving vary queries involve safe zone verification, the safe zone of a kNN query is very totally different. Authentication consists of 2 phases, i.e., format and query process &amp; authentication. Within the format section, the DO initial gets a personal key from a key distribution center.

Next, it signs the ADS created on the information set exploitation the private key and transfers the ADS and signatures to the SP. A client downloads a public key from the key distribution center and the signatures from the SP. within the query process and authentication part, the consumer initial problems and kNN query. Upon receiving the query, the SP computes the top-k result, the safe zone, and a verification object that encodes the question result and its safe zone. The consumer gets the verification object from the SP. The top-k result RS and its safe zone k (RS) are obtained from the verification object.

The correctness of the top-k result and also the safe zone can be verified by the consumer exploitation the verification object, the signatures, and the public key. The consumer must send a new request to the SP only when it leaves the safe zone. Once the query moves across the boundary of a secure zone, it requests an updated top kresult and corresponding safe zone. Therefore, authenticating a kNN query is like confirming the correctness of each the top-k result RS and also the corresponding safe zone. Moreover The SP is that the potential soul. The SP is outside the administrative scope of the DO and so can't be sure. With the exception of the DO’s personal key, adversaries are assumed to understand all data, together with the general public key for the secure-hash operate, the ADS, the signatures, and the authentication algorithms. They will alter the information set or the ADS, and that they could tamper with the search result.

III. FRAME WORK

Our model considers a location-based service situation in mobile environments, as shown in Fig. 1, wherever there exist in the mobile user, the location-based service supplier, the base station and satellites, every taking part in a distinct role. The mobile user sends location-based queries to the LBS provider (or referred to as the LBS server) and receives location-based service from the provider. The LBS provider provides location-based services to the mobile user. The bottom station bridges the mobile communications between the mobile user and therefore the LBS provider. Satellites give the situation data to the mobile user. We assume that the mobile user will acquire his location from satellites anonymously, and therefore the base station and therefore the LBS provider don't conspire to comprise the user location privacy or there exists an anonymous channel like Tor2for the mobile user to send queries to and receive services from the LBS provider. Our model focuses on user location and query privacy protection against the LBS provider and a kNN query protocol.

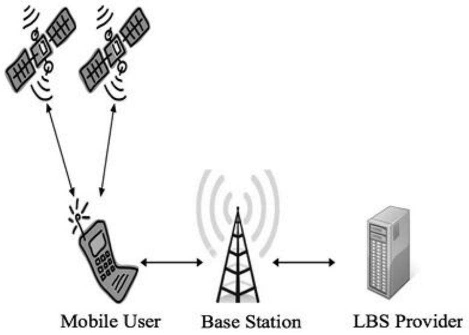


Fig: 1 Location-based service

A private kNN query protocol is illustrated in Fig. 2and is correct if kNN=RR(R, s) outputs k nearest POIs of the type t corresponding the cell at (i, j)where (Q, s) = QG (CR, n, m,(i, j), t, k) and R = RG(Q, D).The security of a personal kNN query protocol involves location privacy. Intuitively, the mobile user U doesn't would like to reveal to the LBS provider his location (i, j) to the LBS server that is considered as someone.

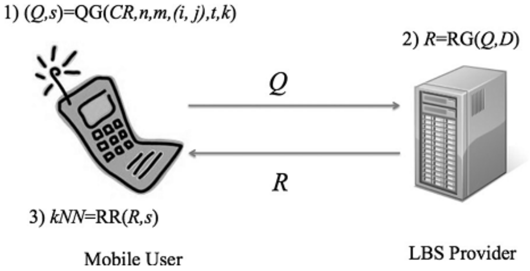


Fig: 2 Private KNN query

First of all, the LBS server divides the location-based database D (a geographic map) into cells with a similar size, for instance, one kilometer dimension and one kilometer length, denoted as grid equal to one kilometer. Supported the middle of every cell, given a type of POIs, the LBS server collects K nearest POIs of the type, P1; P2; . . . ; PK, as shown in Fig. 3, wherever K = eight and each purpose is delineated by a tuple (x; y), wherever x and y are the latitude and great circle of the purpose, severally. We assume that dish sorts are coded into 1; 2; . . . ; m which is revealed to the general public. samples of poi varieties includes: Churches, Schools, Post offices / postboxes, telephone boxes, Restaurants, Pubs, Car parks, Speed cameras, Tourist attractions and etc.

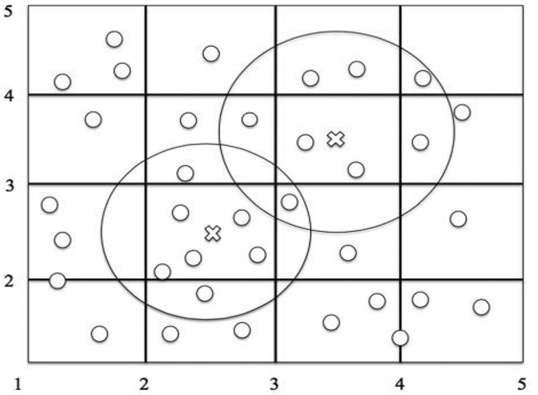
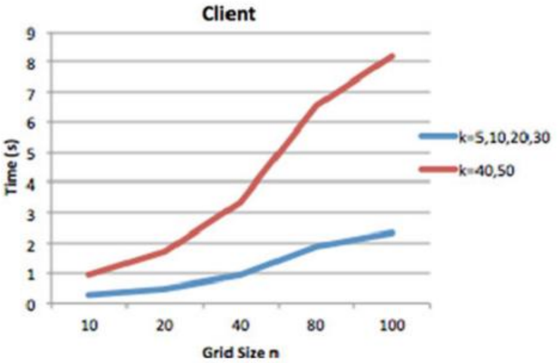


Fig: 3 K nearest POIs for cells

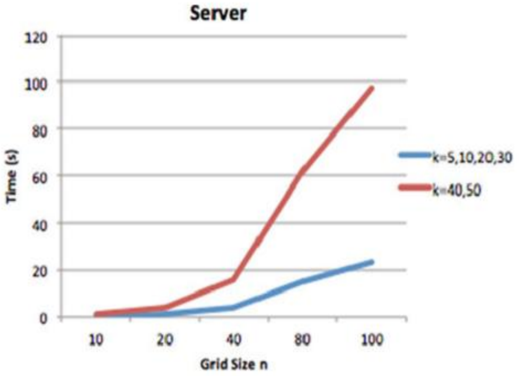
Because the LBS provider collects K nearest POIs consistent with the middle of every cell (i.e., the cross points shown in Fig. 3), it responses a similar k (where k<=K) nearest POIs to the 2 mobile users at intervals a similar cell regardless of where the 2 mobile users are within the cell. For the mobile user locating near the border of 2 cells, he could query 2cells around his location and so establish k nearest POIs among the question responses. The aim of our technique is to avoid in private examination distances that is tough to try to without revealing the situation of the user.

IV. EXPERIMENTAL RESULTS

We enforced our basic protocol and check its performance. The implementation was executed on a machine with an Intel Core i7-2600 processor at a clock speed of3.40 GHz, and with 16 GB of RAM. The experiment used Linux because the OS and is written exploitation the C programming language. We used the GMP library for computations exploitation large integers. According the poi dataset3 that contains 62,556California place names, we tend to construct our kNN info(grid = 1 km) with ten kinds of POIs (school, lake, bridge, creek, hotel, farm, mine, course, hospital, and campground) where k = 5, 10, 20, 30, 40, 50, severally, as represented in the initialization. The running times of our basic protocol in several settings for consumer and server are shown in Figures.



We neglected public key initialization and RSA encryptions of all information within the info D as a result of these variable scan be pre-computed. In the above figure, the dimensions of the RSA modulus is 1,024 bits when k = 5, 10, 20, 30 and 2048 bits when k = 40, 50. Usually, k =20 is adequate massive. Additionally, when n =100, the cloaking region covers an adequate massive area 10,000 km^2.



V. CONCLUSION

In this paper, we've given 3 private kNN query protocol and one personal cloaking region protocol. We have proved that our protocols are all correct. Security analysis has shown that each one of our protocols has location privacy. Our protocol with information privacy and our protocol supported poi type have information privacy for the LBS provider. Performance has shown that our protocol with information privacy is additional efficient than previous PIR-based LBS query protocols.

REFRENCES

[1] M. Bellare and P. Rogaway, “Optimal asymmetric encryption how to encrypt with RSA,” in Proc. Eurocrypt, 1994, pp. 92–111.

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang, “Supporting anonymous location queries in mobile environments with privacygrid,” in Proc. 17th Int. Conf. World Wide Web, 2008, pp. 237–246.

[3] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,” IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, 2003.

[4] C. Y. Chow, M. F. Mokbel, and X. Liu, “A peer-to-peer spatial cloaking algorithm for anonymous location-based services,” in Proc. 14th Annu. ACM Int. Symp. Adv. Geograph. Inform. Syst., 2006, pp. 171–178.

[5] T. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. Inform. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[6] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, “Secure k-nearest neighbor query over encrypted data in outsourced environments,” in Proc. IEEE 30th Int. Conf. Data Eng., 2014, pp. 664–675.

[7] C. Gentry and Z. Ramzan, “Single-database private information retrieval with constant communication rate,” in Proc. 32nd Int. Conf. Automata, Lang. Program., 2005, pp. 803–815.

[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Private queries in location-based services: Anonymizers are not necessary,” in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2008, pp. 121–132.

[9] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, “Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection,” GeoInformatica, vol. 15, no. 14, pp. 699–726, 2010.

[10] G. Ghinita and R. Rughinis, “An efficient privacy-reserving system for monitoring mobile users: Making searchable encryption practical,” in Proc. 4th ACM Conf. Data Appl. Security Privacy, 2014, pp. 321–332.