International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Reasonable Estimated K Nearest Neighbor Queries with Locality and Query Privacy

Bade Ankamma Rao[*1], Desu Sudhisha[2]
*[1]Assistant Professor , Department of MCA , St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India
[2]PG Student , Department of MCA , St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

In mobile communication, spatial queries pose a serious threat to user location privacy because the location of a query may reveal sensitive information about the mobile user. In this paper, we study approximate k nearest neighbor (KNN) queries where the mobile user queries the location-based service (LBS) provider about approximate k nearest points of interest (POIs) based on his current location. We propose a basic solution and a generic solution for the mobile user to preserve his location and query privacy in approximate KNN queries. The proposed solutions are mainly built on the Parlier public-key cryptosystem and can provide both location and query privacy. To preserve query privacy, our basic solution allows the mobile user to retrieve one type of POIs, for example, approximate k nearest car parks, without revealing to the LBS provider what type of points is retrieved. Our generic solution can be applied to multiple discrete type attributes of private location-based queries. Compared with existing solutions for KNN queries with location privacy, our solution is more efficient. Experiments have shown that our solution is practical for KNN queries.

Keywords: Location based query, location and query privacy, private information retrieval, Parlier cryptosystem, RSA.

I. INTRODUCTION

In portable correspondence, spatial questions represent a genuine risk to client area protection because the area of an inquiry may uncover touchy data about the versatile client. In this paper, we consider inexact k closest neighbour (kNN) questions where the portable client inquiries the area based administration (LBS) supplier about rough k closest purposes of intrigue (POIs) on the premise of his present area. We propose a fundamental arrangement and a bland answer for the portable client to protect his area and question security in estimated kNN inquiries. The proposed arrangements are for the most part based on the Paillier open key cryptosystem and can give both area and inquiry protection. To safeguard inquiry security, our fundamental arrangement enables the versatile client to recover one kind of POIs, for instance, inexact k closest auto parks, without uncovering to the LBS supplier what sort of focuses is recovered. Our bland arrangement can be connected to different discrete sort characteristics of private area based inquiries. Contrasted and existing answers for kNN inquiries with area protection, our answer are more proficient. Tests have demonstrated that our answer is functional for kNN questions.

The implanting of situating capacities (e.g., GPS) in cell phones encourages the development of area based administrations (LBS), which is considered as the following "executioner application" in the remote information advertise. LBS enable customers to question a specialist organization, (for example, Google or Bing Maps) in a pervasive way, with a specific end goal to recover definite data about purposes of intrigue (POIs) in their region (e.g., eateries, healing facilities, and so on.).

The LBS supplier forms spatial questions on the premise of the area of the versatile client. Area data gathered from portable clients, purposely and unknowingly, can uncover significantly something beyond a client's scope and longitude. Knowing where a versatile client is can mean realizing what he/she is

doing: going to a religious administration or a help meeting, going by a specialist's office, looking for a wedding band, completing non-business related exercises in office, or spending a night at the corner bar. It may uncover that he is meeting for another occupation or "out" him as a member at a firearm rally or a peace dissent. It can mean knowing with whom he/she invests energy, and how regularly. At the point when area information is collected, it can uncover his/her general propensities and schedules - and when he goes amiss from them.

A 2010 overview led for Microsoft in the United Kingdom, Germany, Japan, the United States, and Canada found that 94 percent of customers who had utilized area-based administrations thought of them as significant however, a similar overview found that 52 percent were concerned about potential loss of privacy1. In this paper, we consider estimated k closest neighbour (kNN) inquiries where the versatile client questions the area based administration (LBS) supplier about inexact k closest purposes of intrigue (POIs) on the premise of his present area. When all is said in done, the versatile client needs to present his area to the LBS supplier, which at that point discovers and comes back to the client the k closest POIs by contrasting the separations between the portable client's area and POIs adjacent. This uncovers the portable client's area to the LBS supplier.

There have been various methods that can star vide a specific level of area protection. These techniques for the most part incorporate Data get to control [16], [35]; Mix zone [3]; k-obscurity [15], [2], [4] "Sham" areas [13], [34], [27]; Geographic information change [12], [31], [11], [32]; Private Information Retrieval (PIR) [8], [22], [21].

Two LBS servers [6], [26].

LBS inquiries in view of get to control, blend zone and k-obscurity require the specialist organization or the middleware that keeps up all client areas. They are vulnerable to bad conduct of the outsider. They offer little security when an entrusted party claims the specialist organization/middleware. There has been private information unintentionally uncovered over the Internet previously.
K-secrecy is at first utilized for character protection expert taction. It is largely lacking for area security insurances, where the idea of separation between locations is essential (dissimilar to separations between personalities). The impact of LBS inquiries in view of k-secrecy depends.

Intensely on the dispersion and thickness of the portable clients, which, in any case, are outside the ability to control of the area security method?

LBS inquiries in view of sham areas require the portable client arbitrarily to pick an arrangement of fake areas, to send the fake areas to the LBS and to get the false reports from the LBS over the versatile system. This acquires both calculation and correspondence overhead in cell phones. With the end goal of productivity, the portable client may pick less fake areas, yet the LBS supplier can confine the client in a little sub space of the aggregate area, prompting feeble security.

An LBS question based geographic information change is inclined to get to design assaults [30] in light of the fact that a similar inquiry dependably restores the same encoded comes about. For instance, the LBS may watch the frequencies of the re-turned cipher texts. Knowing about the setting of the database, it can coordinate the most well known plaintext POI with the most oftentimes returned cipher text and, therefore, unwind data about the question.

LBS questions in light of PIR give solid crypto-realistic assurances however are frequently computationally and communication ally costly. To enhance productivity, trusted equipment was utilized to perform PIR for LBS questions [21]. This procedure is based on equipment helped PIR [29], which expect that a trusted outsider (TTP) instates the framework by setting the mystery key and the change of the database. Like LBS inquiries in view of get to control, blend zone and k-namelessness, this strategy is powerless against mischief of the outsider.

It is a test to give reasonable answers for kNN inquiries with area security on the premise of PIR.

In this paper, we expand our work [33] displayed in ICDE 2014. We develop answers for kNN inquiries on the premise of PIR with the Paillier open key cryptosys-tem. We have four primary commitments as takes after:

Current PIR-based LBS questions [8], [9], [22], and [23] for the most part require two phases. In the principal arrange, the versatile client recover the list of his area from the LBS supplier. In the second stage, the versatile client recovers the POIs as indicated by the file from the LBS supplier. The versatile client and the LBS supplier need to run two PIR conventions succeed-kingly. To rearrange the procedure, we give an answer for kNN inquiries, which needs one PIR just, i.e., the portable client sends his area (scrambled) to the LBS supplier and gets the k closest POIs (encoded) from the LBS supplier.

Current PIR-based LBS inquiries just permit the mo-bile client to discover k closest POIs paying little mind to the sort of POIs. Surprisingly, we consider the kind of POIs in kNN questions. We give an answer for the portable client to save inquiry security, i.e., discovering k closest PIOs of a similar sort without uncovering to LBS supplier what kind of POIs he is occupied with. For instance, our answer enables the versatile client to discover k closest auto parks from the LBS supplier without uncovering to LBS supplier that the sort of POIs is auto stop.

Current PIR-based LBS inquiries [8], [9], [22], [23], [33] enable the versatile client to recover just a single POI after a convention execution. Surprisingly, we consider successive questions. We give an answer for the portable client to inquiry a succession of POIs without need of numerous executions of the entire convention. This significantly enhances the productivity of consecutive inquiries.

Current PIR-based LBS arrangements [33] permit LBS questions as per area and single POI sort quality as it was. They do not bolster LBS questions with numerous POI sort properties, e.g., auto stop and every day stopping charge (which can be classified into discrete information esteems, for example, "Low" (<$10), "Centre" ($10-$30) and "High" (>$30)). Surprisingly, we give a non-specific arrangement, which can be connected to different discrete sort qualities of private inquiries.

To examine the security of our answers, we characterize a security display for private kNN questions. The security investigation has demonstrated that our answers guarantees both area protection as in the client does not uncover any data about his area to the LBS supplier and inquiry protection as in the client does not uncover what kind of POIs he is occupied with to the LBS supplier. Furthermore, our answers have information protection as in the LBS supplier discharges to the client just k closest POIs per question.

We have executed our answers on a case of area based database and examinations have demonstrated that our answers are pragmatic.

The fundamental contrasts between our past work [33] and our present paper are: (1) The past work settled the quantity of closest neighbors k. The present work permits any number of closest neighbors k up to K, where K is a steady; (2) The past work characterized area protection which inferred question security. The mongrel lease work characterizes area and inquiry security independently;

(3) The past work utilized the Rabin cryptosystem [24] to keep the versatile client to recover more than one information for every inquiry and did not permit successive questions without numerous executions of the entire convention. The present work utilizes RSA [25] to accomplish the information protection and bolster consecutive inquiries; (4) The present work includes a non specific answer for numerous discrete sort qualities of private area based questions; moreover, (5) we have included a few analyses for variable k.

Whatever is left of the paper is organized as takes after. Re-lated works are studied in Section 2. Foundations are presented in Section 3. We characterize our model in Section 4 and depict our answers in Sections 5 and 6.

II. RELATED WORKS

Data get entry to manipulate [16], [35]: person places are despatched to the lbs company as traditional. this approach relies on the lbs issuer to restrict get entry to to stored loca-tion records thru rule-primarily based polices. it helps three varieties of location-based queries:

1) person region queries (querying the region of a selected person or customers, identi-fied by their particular identifiers);

2) enumeration queries (querying lists of customers at precise places, expressed either in phrases of geographic or symbolic attributes);

3) asynchronous queries (querying "occasion" information, inclusive of while customers enter or go away unique areas). this approach requires the lbs provider to maintain all person locations. it's miles at risk of misbehavior of the lbs company.

Blend zone [3]: a relied on middleware relays between the cell customers and the lbs issuer. earlier than forwarding the region-based totally queries of the users to the lbs, the middleware anonymizes their places with the aid of pseudonyms. the primary concept is: when a person enters a mixture area, the middleware assigns him a pseudonym, by which the user queries lbs. the verbal exchange between the user and the lbs is thru the middleware and the pseudonym adjustments every time the person enters the mix quarter. currently, the combination-zone has been applied to street networks [20]. this method calls for the middleware to anonymize consumer places. it is at risk of misbehavior of the middleware.

K-anonymity [28]: this method ensures that a report could not be distinguished from okay-1 different records. in-stead of sending a unmarried user's actual place to the lbs, k-anonymity primarily based schemes gather ok user locations and ship a corresponding (minimum) bounding place to the lbs as the question parameter. the gathering of various cell user locations is completed either through a relied on 0.33-party [15], [2] between the customers and the lbs, or thru a peer-to-peer collaboration [4] amongst customers. because ok-anonymity is performed, an adversary can simplest discover a area's consumer with probability no better than 1=k. this approach is predicated on the 0.33 birthday party or a peer consumer to collect special cellular user locations. it is at risk of misbehavior of the third celebration or the peer person.

"dummy" places [13], [27]: the primary concept is when the cellular user queries the lbs, he sends many ran-dom different places along together with his location to the lbs issuer to confuse his location such that the server can't distinguish the actual region from the fake places. specific from ok-anonymity based totally schemes, this approach encompass faux or fixed places, in place of the ones of different cellular users, as parameters of queries sent to the lbs issuer. Faux dummy places are generated at random, and stuck places are chosen from unique ones together with street intersections. Both manner, the precise person locations are hidden from the carrier issuer. Even though this approach does now not rely upon any 1/3 birthday party, the lbs provider can restrict the consumer in a small sub area of the overall domain, main to vulnerable privateers.

Private data retrieval (per) [18]: this technique allows a person to retrieve a document from a database server without revealing which record he is retrieving. pirated totally protocols [8], [9], [22], [23] are proposed for poi queries and composed of levels. within the first stage, the person privately determines the index of his place through the carrier issuer without disclosing his coordinates to it. in the second stage, the consumer runs a per protocol with the carrier provider to retrieve the pois corresponding to the index. The difference between ghinita et al. [8], [9] and paulet et al. [22], [23] pirated protocols is in the first level, in which ghinita et al. technique is based totally on homomorphism encryption

[19] Whilst the method of paulet et al. is primarily based on oblivious switch [17]. further, relied on hardware changed into employed to carry out pir for lbs queries [21]. their approach is built on hardware-aided pir [29], which is based on a depended on third celebration (ttp) to set the secret key and the permutation of the database. like lbs queries based totally on get entry to manage, blend region and ok-anonymity, this approach is susceptible to misbehavior of the third birthday celebration.

Geographic statistics transformation [31], [11], [32]: this approach entails three events: 1) a statistics owner who has a database d of points, and would really like to outsource d to a server (i.e., cloud provider provider) that cannot be absolutely trusted. 2) a consumer who desires to get right of entry to and pose queries to the database d. three) a server this is honest however potentially curious within the tuples in d and/or the queries from the users. a server may be curious both because he is simply curious or he has been compromised to come to be curious on the behalf of a 3rd birthday celebration with out his express knowledge. on this placing the information owner isn't the same as the lbs. the owner transforms the database

(the usage of a few encoding methodology) previous to transmitting it to the lbs. an authorized consumer that possesses the name of the game transformation keys issues an encoded query to the lbs. both the database and the queries are unreadable by way of the lbs and, hence, region privateness is included. the purpose is to offer the lbs with looking skills over the encoded information. wong et al. [31] advocate a relaxed factor transformation, which preserves the relative distances of all of the database pois to any question factor. in every other answer [32], given simplest the encryption of location factor e(q) and the encryption of database e(d), the server can return a applicable (encrypted) partition e(g) from e(d), such that that e(g) is assured to include the solution for the nn query. these techniques permit approximate nn search immediately at the converted factors. they're liable to access sample assaults [30] due to the fact the equal query usually returns the identical encoded effects.

lbs servers: to conquer the access sample assaults, elmehdwi et al. [6] gave an answer for knn question based at the semantically comfy paillier encryp-tion [19], assuming two lbs servers exist, one having the encrypted records and some other having the decryption key. further, schlegel et al. [26] proposed a solution for continuous region-based totally offerings, assuming a query server and a service provider exist, in which a query server holds the encrypted vicinity at the same time as the carrier provider has the decryption key. those solutions must anticipate that lbs servers never collude.

Recently, ghinita and rughinis [10] proposed an inter-esting vicinity-based alert device, in which a cell person keeps sending the encryption of his area to a lbs server and handiest when he enters a disaster vicinity, the server is capable of know his location and send an alert to him.

III. BACKGROUNDS

3.1 Paillier Public-Key Cryptosystem

Paillier public-key cryptosystem [19] consists of three algorithms as follows.

Key Era: a person randomly chooses two massive wonderful primes p; q and an detail g of zn2 whose order is a nonzero multiple of n = pq, publishes the general public key pk = (n; g), and maintains the personal key sk = (p; q) mystery.

Encryption: given the public key pk of the user, you may encrypt a message m where m is a high-quality integer less than n via randomly deciding on r from zn2 and computing

c = e(m; pk) = gmrn (mod n2)(1)

where c is the ciphertext of m. when you consider that r is randomly chosen, the ciphertext c of a message m is random. consequently, paillier cryptosystem is a probabilistic encryption.

Decryption: the person can decrypt the ciphertext c with the non-public key sk via computing

m = d(c; sk) = (c (mod n2) 1)=n (mod n) (2)
(g (mod n2) 1)=n

Where in = LCM (p 1; q 1).
homomorphism homes: Paillier cryptosystem has homomorphic encryption homes as follows:

e(m1)e(m2) = e(m1 + m2) (three)
e(m1)a = e(am1) (four)

for any m1; m2; m; a 2 zn .

Suppose that e(mi) = gmi rin (mod n2) for i=1; 2, it is straightforward to affirm (3) and (four) due to the fact e(m1)e(m2) = gm1+m2 (r1r2)n (mod n2) = e(m1 + m2); e(m1)a = gam1 (r1a)n (mod n2) = e(am1):
three. 2 rsa rsa [25] is a public-key cryptosystem, composed of 3 algorithms as follows.
Key generation: a user randomly chooses two huge distinct primes p; q and computes n = pq and '(n) = (p 1)(q 1). subsequent, he chooses an integer e such that 1 < e < '(n) and gcd(e; '(n)) = 1, i.e., e and '(n) are coprime, and determines d such that e d = 1 (mod '(n)) the use of the prolonged euclidean algorithm. then, he publishes the general public

key pk = (e; n) and maintains the personal key sk = d secret. in addition, p; q, and '(n) ought to additionally be stored secret due to the fact they can be used to calculate d.

Encryption: given the general public key (e; n) of the user, you may encrypt a message m where m is a high-quality integer much less than n by using computing

c = e(m; pk) = me (mod n) (five)
in which c is the ciphertext of m.

Decryption: the person can decrypt the ciphertext c with the personal key d with the aid of computing
m = d(c; sk) = cd (mod n) (6)
rsa isn't always a probabilistic encryption scheme. to trans-shape rsa to a probabilistic encryption scheme, we need to add some random bits into the message m before encrypting m with rsa. most effective uneven encryp-tion padding (oaep) [1] is a padding scheme frequently used collectively with rsa encryption.

IV. OUR MODEL

Our model considers an area based administration situation in versatile conditions, as appeared in Fig. 1, where there exist the portable client, the area based administration (LBS) supplier, the base station and satellites, each assuming an alternate part.

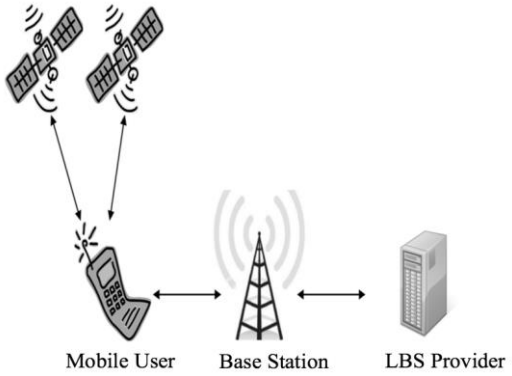

Figure 1. Location-Based Service

The portable client sends area based inquiries to the LBS supplier (or called the LBS server) and gets area based administration from the supplier.

The LBS supplier gives area based administrations to the portable client.

The base station connects the versatile correspondences between the portable client and the LBS supplier.

Satellites give the area data to the versatile client.

We expect that the portable client can get his lo-cation from satellites namelessly, and the base station and the LBS supplier don't intrigue to contain the client area security or there exists an unknown station, for example, Tor2 for the versatile client to send inquiries to and get administrations from the LBS supplier. Our model

concentrates on client area and question security assurance against the LBS supplier and a kNN inquiry convention (where k K and K is a consistent) is made out of three
calculations as takes after.
(1) Query Generation (QG): Takes as information a shrouding area CR with n n cells and m particular sorts of POIs, the area (i; j) of the portable client,
the sort t of POIs, and the quantity of closest
neighbors k, (the portable client) yields an inquiry Q
(containing CR) and a mystery s, signified as
(Q; s) =QG(CR; n; m; (i; j); t; k).

(2) Response Generation (RG): Takes as information the inquiry Q and the area based database D of POIs, (the LBS supplier) yields a reaction R, indicated as R = RG(Q;D).

(3) Response Retrieval (RR): Takes as information the reaction R and the mystery s of the versatile client, (the versatile client) yields k closest POIs of the sort t,
meant as kNN = RR(R; s).
A private kNN question convention can be shown in

Fig. 2 and is right if kNN = RR(R; s) yields k closest

POIs of the sort t relating the cell at (i; j), where

(Q; s) = QG(CR; n; m; (i; j); t; k) and R = RG(Q;D).

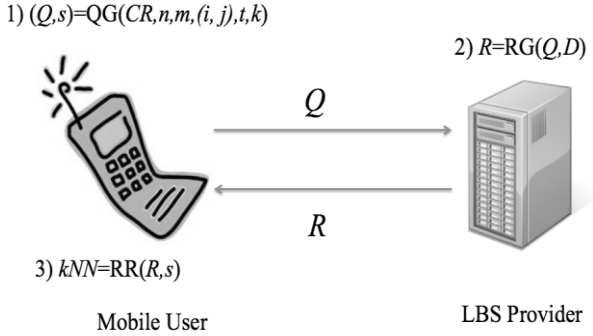

Figure 2. Private kNN Query

V. FUNDAMENTAL NON-PUBLIC K NEAREST NEIGHBOR QUERIES

Based on our model, we give a fundamental construction of non-public knn query protocol on this

phase. our basic answer is built on the paillier scheme [19] and rsa [25].

VI. INITIALIZATION

Earlier than execution of any personal knn protocol, an initialization happens in the lbs server.to begin with, the lbs server divides the place-based database d (a geographic map) into cells with the identical size, as an instance, 1 km width and 1 km period, denoted as grid = 1 km. primarily based on the center of every cell, given a form of pois, the lbs server collects k nearest pois of the sort, p1; p2; ; pk, as proven in fig. three, wherein ok = eight and every point is represented by a tuple (x; y),where x and y are the latitude and longitude of the point,respectively.

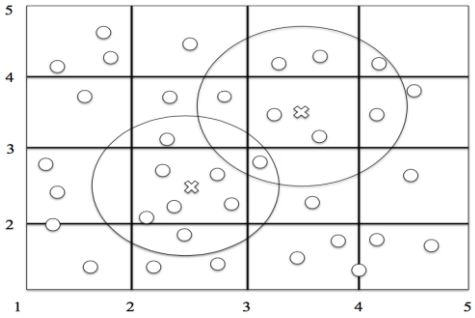

Figure 1. k Nearest POIs for Cells

We assume that poi types are coded into 1; 2; mwhich is published to the general public. examples of poi kindsconsists of: churches, schools, publish workplaces / postboxes,phone containers, restaurants, pubs, car parks, velocitycameras, traveller points of interest and and many others.for each cellular (i; j) and each poi kind t, the lbs servermaintains ok (e.g, okay = 20) nearest pois of kind t, representedby a circulate of bits, denoted as an integer dk

i;j;t, wherethe points are ordered in keeping with the distance to thecenter of the cell such that the first k (where k ok)points, denoted as dki;j;t, are the ok nearest pois. everymobile incorporates m integers for one of a kind forms of pois. wecount on m(k) = max(dki;j;t), i.e., the longest file.observation. the lbs server can construct special poidatabases for distinct grids. this doesn't affect privacyfor the mobile person and the lbs server. The smaller thegrid is, the extra correct the result of knn query is, but the much less green the reaction technology for givencloaking area is. a cellular consumer can select a grid consequently while he queries the lbs. due to the fact the lbs provider collects okay nearest poising keeping with the centre of every cellular (i.e., the pass factors proven in fig.), it responses the equal okay (wherein k k) nearest pois to the two mobile users in the same cellular no matter in which the 2 mobile customers are within the cell. Forth mobile person locating near the border of cells, he may also query cells round his area after which discover k nearest pois many of the question responses. The cause of our approach is to keep away instances, which is tough to do without revealing the from privately comparing area of the consumer. Next, the lbs server generates the rash public and personal key pair (pike; ski), where

pk = fe;ng and
sk =fdg. relying on okay exact by means of the consumer, lbs server

will encrypt dk
i;j;t to dk i;j;t
0 for all i; j; t in step with

rsa encryption algorithm (described in section three.2) and most efficient asymmetric encryption padding (oaep) [1] as

dk i;j;t0= e(dki;j;t; pk) = (dki;j;t)e(mod n) (7)

remark. the general public key pk = fe;ng of the lbs server ispublished and acknowledged to all mobile customers. it's miles required that log2 n > 2 log2m(k) for knn question. for distinct k, the lbs server can publish one-of-a-kind public key. Assume the area of a poi can be represented by way of 32 bits, dk

i;j;t

Is much less than 1024 bits while ok = five; 10; 20; 30, and much lessthan 2048 bits while k = forty; 50 unusually. The area of poi may be represented via much less bits if we introduce latitude and longitude relative to a reference point. For simplicity, we also use dki; j;t to denote the okay nearest pois after ape.

5.1 basic private knn query protocol

We count on that poi kinds are coded into 1; 2; . ;m that's published to the public and the mobile consumeru desires to discover okay nearest pois of kind t around hisplace. the consumer u chooses a cloaking region cr

within n cells, where u is located inside the cell (i; j), andruns the knn question protocol with the lbs provider s,composed of algorithms 1- 3 observation.

Algorithm 1 Query Generation (User)

Input: $CR, n, m, (i, j), t, k, pk = \{e, N\}$
Output: Q, s

1: Randomly choose two large primes p_1, q_1 such that $N_1 = p_1 q_1 > N$.
2: Randomly choose two large primes p_2, q_2 such that $N_2 = p_2 q_2 > N$, where $N_2^2 < N_1$.
3: Let $sk_1 = \{p_1, q_1\}, pk_1 = \{g_1, N_1\}$.
4: Let $sk_2 = \{p_2, q_2\}, pk_2 = \{g_2, N_2\}$.
5: For each $\ell \in \{1, 2, \cdots, n\}$, pick a random integer $r_\ell \in \mathbb{Z}^*_{N_1^2}$, compute

$$c_\ell = \begin{cases} \mathsf{E}_1(1, pk_1) = {g_1}^1 r_\ell^{N_1} (mod\ {N_1}^2) & \text{if } \ell = i \\ \mathsf{E}_1(0, pk_1) = {g_1}^0 r_\ell^{N_1} (mod\ {N_1}^2) & \text{otherwise} \end{cases}$$

where E_1 denotes the Paillier encryption algorithm with public key $pk_1 = \{g_1, N_1\}$ as described in Section 3.1.
6: For each $\ell \in \{1, 2, \cdots, m\}$, pick a random integer $r'_\ell \in \mathbb{Z}^*_{N_2^2}$, compute

$$c'_\ell = \begin{cases} \mathsf{E}_2(1, pk_2) = {g_2}^1 {r'_\ell}^{N_2} (mod\ {N_2}^2) & \text{if } \ell = t \\ \mathsf{E}_2(0, pk_2) = {g_2}^0 {r'_\ell}^{N_2} (mod\ {N_2}^2) & \text{otherwise} \end{cases}$$

where E_2 denotes the Paillier encryption algorithm with public key $pk_2 = \{g_2, N_2\}$.
7: Let $Q = \{CR, n, m, k, c_1, c_2, \cdots, c_n, c'_1, c'_2, \cdots, c'_m, pk_1, pk_2\}$, $s = \{sk_1, sk_2\}$.
8: **return** Q, s

The cr can be specified with the aid of the coordinates (x; y) of a starting place point and the order n of a square grid. The mobile which includes the foundation point is labelled as(1,1). the cr covers the rectangular grid from the mobile (1,1) to the cellular (n; n).

Algorithm 2 Response Generation RG (Server)

Input: $D, Q = \{CR, n, m, k, c_1, c_2, \cdots, c_n, c'_1, c'_2, \cdots, c'_m, pk_1, pk_2)$
Output: $R = \{C_1, C_2, \cdots, C_n\}$

1: Based on CR, n, k, for any t in the cell (i, j), take the first k points of $d^K_{i,j,t}$, denoted as $d^k_{i,j,t}$, and encrypt it according to RSA encryption algorithm described in Section 3.2. The result is denoted as ${d^k_{i,j,t}}'$.
2: Based on CR, n, m, for each cell (α, β) in CR, compute

$$C_{\alpha,\beta} = \prod_{\ell=1}^{m} {c'_\ell}^{{d^k_{\alpha,\beta,\ell}}'} (mod\ {N_2}^2)$$

3: Based on CR and n, compute $R = \{C_1, C_2, \cdots, C_n\}$, where for $\beta \in \{1, 2, \cdots, n\}$,

$$C_\beta = \prod_{\alpha=1}^{n} {c_\alpha}^{C_{\alpha,\beta}} (mod\ {N_1}^2).$$

4: **return** R

observation. with the aid of slightly modifications of algorithms 1-3, our protocol can defend place or question privacy most effective.

Algorithm 3 Response Retrieval RR (User)

Input: $R = \{C_1, C_2, \cdots, C_n\}, s = \{sk_1, sk_2\}, sk = \{d\}$
Output: z

1: The user randomly chooses an integer $r < N$ and computes and sends to the server

$$w = r^e \mathsf{D}_2(\mathsf{D}_1(C_j, sk_1), sk_2)(mod\ N)$$

where $\mathsf{D}_1, \mathsf{D}_2$ are the Paillier decryption algorithm as described in Section 3.1.
2: The server computes and replies to the user

$$v = \mathsf{D}(w, sk) = w^d (mod\ N)$$

where D denotes the RSA decryption algorithm as described in Section 3.2.
3: The user computes

$$z = r^{-1} v (mod\ N)$$

4: **return** z

In case that a person desires to keep place privateness most effective(i.e., keep (i; j) non-public inside the question), given the kind t ofpois, he runs steps 1, three, 5 in algorithm 1 and submitsq = fcr; n; m; k; c1; c2; ; cn; t; pk1g to the lbs server.because t is given, the lbs server runs steps 1 and threein set of rules2,inwhich = dk = 1; 2; ; n

and returns r = fc1;c2; ;cng to the person. In reactionretrieval, the person computes w = red1 (cj; sk1) (mod n) where r is a random integer and runs steps two and three toretrieve knn of the kind t.

In case that a person needs to preserve question privateers only (i.e., maintain the kind t personal in the query), given the place (I; j) of the user, he runs steps 2, four, 6 in algorithm1 and submits q = far; n; m; ok; (I; j); c0 1; c0 2; ; c0 m; pk2g

To the lbs server. because (i; j) is given, the lbs server runs steps 1 and a couple of in algorithm 2, in which and returns r = fci;jg to the person. in reaction retrieval, the person computes w = red2(conj ; sk2)(mod n) wherein rips a random integer and runs steps 2 and three to retrieving of the kind t.statement. in algorithm three, whilst the cellular consumer getsthe reaction, he can forget about c` (` 6= j) and obtain cjmost effective due to the fact simplest cj includes the records about thek nearest pois in the cell (i; j). in truth, the cell user

iscapable of retrieval the okay nearest pois of kind t in any mobile

(i;) (= 1; 2; ; n) by running set of rules three with outwant of query generation and reaction technology. thisfunction makes non-public queries very green while thecell user moves from the cellular (i; j) to every other cell suchbecause the cell (I; j + 1) (where j + 1 n) or (i; j 1) (wherein j 1 1). Further, the lbs server can without difficulty manage the facts release via decryption due to the fact one response retrieval invocation releases one statistics simplest.

Theorem 1 (correctness) our primary knn query protocol(algorithms 1-three) is correct. in different words, for anycloaking location cr with n n and m sorts of pois,and the index i; j of any mobile (1 i; j n), any kind t ofpois, and any quantity of nearest neighbor ok k, we have dki;j;t = rr(r; s) holds, where dk i;j;t stands for k nearest pois of the kindt regarding the center of the cell (i; j), and (q;; sk) = qg(cr; n; m; (i; j); t; okay), r = rg(q;d).evidence.

DATA PRIVACY OF OUR PROTOCOLS

Next, we analyze data privacy of the LBS server according to Definition 3 in Section 4. Data privacy of our protocols is built on the security of RSA with OAEP.

Theorem . If RSA with OAEP is semantically secure, our basic and generic kNN query protocols described in Sections 5 and 6 have data privacy for the LBS server.

Proof. With reference to Game 3 in Section 4, the adversary

A (the mobile user) chooses any two distinct cloaking regions CR0 and CR1 with n _ n cells such that k nearest POIs of the type t or the type attributes (t1; t2; _ _ _ ; tT) in the cell (i; j) are same. The adversary generates a query Q to retrieve the k nearest POIs of the type t or the type attributes (t1; t2; _ _ _ ; tT) in the cell (i; j) and sends Q;CR0;CR1 to the challenger C (the LBS server). The challenger C chooses a random bit b 2 f0; 1g, encrypts CRb with RSA and OAEP, and runs the Response Generation algorithm RG to obtain Rb = RG(Q; E(CRb)), and then sends Rb back to A, where E(CRb) denotes the encryptions of all data in CRb.Since RSA with OAEP has semantic security [1], theadversary cannot distinguish E(CR0) from E(CR1) andhe cannot distinguish R0 from R1. Therefore, the adversaryA, given Rb, cannot guess b chosen by the challengercorrectly with a non-negligible advantage. Based onDefinition 3, the theorem is proved. 4

VII. CONCLUSION

In this paper, we have presented a basic and a generic Approximate KNN query protocols. Security analysis has Fig. . Performance of our basic protocol for communication (where m = 10) shown that our protocols have location privacy, query Privacy and data privacy. Performance has shown that our basic protocol performs better than the existing PIRbased LBS query protocols in terms of both parallel computation and communication overhead. Experiment evaluation has shown that our basic protocol is practical. Our future work is to implement our protocol on mobile Devices.

VIII. REFERENCES

[1] M. Bellare and P. Roadway. Optimal asymmetric encryption - how to encrypt with RSA. In Proc. Eurocrypt 1994.

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang. Supporting anonymous location queries in mobile environments with PrivacyGrid. In Proc. WWW 2008.

[3] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing 2(1), 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. ACM GIS 2006.

[5] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31 (4): 469-472, 1985.

[6] Y. Elmehdwi, B. K. Samanthula, W. Jiang. Secure k-nearest neigh-bor query over encrypted data in outsourced environments. In Proc. ICDE 2014.

[7] C. Gentry and Z. Ramzan. Single-database private information retrieval with constant communication rate. In Proc. ICALP'05, pages 803-815, 2005.

[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 2008.

[9] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino. Approx-imate and exact hybrid algorithms for private nearest-neighbor queries with database protection. GeoInformatica 15(14): 699-726, 2010.

[10] G. Ghinita, R. Rughinis. An efficient privacy-reserving system for monitoring mobile users: making searchable encryption practical. in Proc. ACM CODASPY 2014.

[11] Haibo Hu, Jianliang Xu, Chushi Ren, and Byron Choi, Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism, In Proc. ICDE 2011.

[12] A. Khoshgozaran and C. Shahabi. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In Proc. SSTD 2007.

[13] H. Kido, Y. Yanagisawa, and T. Satoh. An anonymous commu-nication technique using dummies for location-based services. In Proc. ICPS 2005, pages 88 - 97.

[14] E. Kushilevitz and R. Ostrovsky. Replication is not needed: single database, computationally-private information retrieval. In Proc. 38th Annual Symposium on Foundations of Computer Science, pages 364-373, 1997.

[15] M. F. Mokbel, C.-Y. Chow, and W. G. Aref. The new casper: query processing for location services without compromising privacy. In Proc. VLDB 2006.

[16] G. Myles, A. Friday, and N. Davies. Preserving privacy in envi-ronments with location-based applications. IEEE Pervasive Com-puting 2(1):5664, 2003.

[17] M. Naor and B. Pinkas. Oblivious transfer with adaptive queries. In Proc. CRYPTO 1999, pages 791 - 791.

[18] R. Ostrovsky and W. Skeith. A survey of single-database private information retrieval: techniques and applications. In Proc. PKC 2007, pages 393 - 411.

[19] P. Paillier. Public key cryptosystems based on composite degree residue classes. In Proc. EUROCRYPT 1999, pages 223 - 238.

[20] B. Palanisamy and L. Liu. Mobimix: Protecting location privacy with mix-zones over road networks. In Proc. ICDE 2011, pages 494 505.

[21] S. Papadopoulos, S. Bakiras, D. Papadias. Nearest neighbor search with strong location privacy. In Proc. VLDB 2010.

[22] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino. Privacy-preserving and content-protecting location based queries. In Proc. ICDE 2012, pages 44 - 53.

[23] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino. Privacy-preserving and content-protecting location based queries. IEEE Transactions on Knowledge and Data Engineering, accepted in 2013.

[24] Rabin, Michael. Digitalized signatures and public-key functions as intractable as factorization. MIT Laboratory for Computer Science, January 1979.

[25] R. Rivest, A. Shamir and L. Adleman. A method for obtaining dig-ital signatures and public-key cryptosystems. Communications of the ACM 21 (2): 120-126, 1978.

[26] R. Schlegel, C. Chow, Q. Huang, D. Wong. User-defined privacy grid system for continuous location-based services. IEEE Trans-actions on Mobile Computing, Jan. 2015.

[27] P. Shankar, V. Ganapathy and L. Iftode. Privately querying location-based services with SybilQuery. In Proc. Ubicomp 2009, pages 31 - 40.

[28] L. Sweeney. k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10: 557 - 570, 2002.

[29] S. Wang, X. Ding, R. H. Deng, and F. Bao. Private information retrieval using trusted hardware. In Proc. ESORICS 2006.

[30] P. Williams and R. Sion. Usable PIR. In NDSS, 2008.

[31] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis. Secure kNN computation on encrypted databases. In Proc. SIGMOD 2009.