# Efficient Geosocial Application Query Processing With Privacy Preserving Policy

[1] Mayura Phadnis, [2]Prof.G.V.Kadam.
[1] Post Graduate Student, [2] Professer
[1]Computer Department,  RSSOER,Pune,India

***Abstract* - In recent years use of smart phones enables user to communicate surrounding environment through applications. User frequently searches information by asking other individuals even when they have admittance to huge reservoirs of information such as the internet and libraries. Friend recommendations are become very common source of information particularly for location-specific, community-specific and time-specific. This new era of geosocial application brings many threats to the security of the user. Many algorithms and privacy preserving frameworks have been proposed in the literature, but none of them achieve the desired privacy this paper proposes privacy mechanism along with the recommendation compression approach while transmitting data to the another user. The compression takes place while storing the recommendations on the data server which improves the efficiency while retrieving the recommendations from the server. Compression and encryption provides both privacy and performance for the system.**

***Index Terms* - Geosocial networks, Location Privacy, nearest neighbor queries, Circular range queries, Compression.**

## I. INTRODUCTION

A well-known method for searching information is asking from the surrounding. An individual may take advice from her/his friends, who thus will ask their friends, and so on, until the information is found. This kind of social networking is very prominent despite the accessibility of unbelievable reservoirs of information, for example, the internet and libraries. Exploring the information over social network, work better than the different strategies like internet, when individuals are looking for information which is location-specific, community-specific, or time-specific. This is because individuals are great wellsprings of these sorts of information, e.g., a great pizza shop in Toronto[3].

Geo-social networks (GeoSNs) provide context-aware administrations which is helpful in mapping of user with specific location and content. GeoSNs offer diverse sorts of applications such as photograph offering, friends tracking, check ins etc. which contributed in the rising popularity of GeoSNs among users.

However, this capacity to reveal user's locations causes new privacy risks, which thus call for new privacy-protection routines. There are multiple privacy techniques for securing privacy in these circumstances such as social networks location, colocation, and character privacy [1]. This massive increase in use of smartphone applications has increased the computing capacity of users but poses new security threats. Close friends use social applications to give suggestions, feedbacks for various activities like eating, shopping, gaming and collective network services etc. [5] . This use comes under Geosocial applications category. It also gave birth to risk of losing users privacy.

We all know about the "places" feature of facebook which was misused by some thieves [12]. Henceforth, there is a genuine requirement for stronger privacy properties for making it friendlier to the users. In literature, there have been used strategies to handle this issue like 1) adding vulnerability or errors into location data. 2) Relying on trusted servers or delegates to apply anonymization to users characters and private data, and 3) using complex cryptographic algorithms or private information retrieval (PIR) processes. The first needs users and application suppliers to give data that is not surely leading to sufficient privacy to the users. A smaller amount of precision makes it unacceptable to the users and the application suppliers are not ready to adapt the data legally. The second one relies upon trusted proxies or servers .Though, the trusted one seems very costly to be used on mobiles and noting queries to servers. Considering these issues in GeoSocial applications, we have to create mechanism that would give protection to the user's privacy as well as keep up the accuracy and performance of the system.

The two queries which improves the functionality of these applications are: point queries and nearest neighbor queries (KNN)[5]. Point queries inquiry for location data at a specific point and kNN for nearest data around a given location coordinates [7][8]. We are interested in these types of queries which are beneficial for geosocial applications.

In recent years, geosocial applications have emerged as an integral part of our lives. But our private information given by these applications may be misused and needs to be protected. LocX has a tendency to furnish with enhanced privacy and with highly certain result. The essential thing that is carried out to use secure location conversion. This conversion would be used just by companions of a specific user. It permits the server to work appropriately and effectively without getting to the private data of the user [9]. Many services are interested in gathering data between friends not between the arbitrary pairs of users. We can distinguish such useful data and send for conversion. The coordinate's conversions take care of distance metrics, and allows server to perform all query operations. The transformation is a safe one, since the unpredictability is the key to the data, which is known to the users group [10]. LocX has the ability to assure the privacy and models that is used in this method which does the task proficiently and effortlessly, making it close to ideal for cellular phones of the present day.

Observe that privacy is not secured by replacing the genuine user identity with a fake one (i.e., pseudonym), because, in request to process location-dependent queries, the LBS needs the precise location of the querying user. An attacker, which may be the LBS itself, can derive the information of the question source [11]. This can be effortlessly performed by and with the assistance of a public telephone directory, case in point queries, which contain subscriber's addresses.

Location-based social networking is more extensive than simply proximity detection. Develop the key cryptographic primitives on top of which such functionality can be inherent privacy preserving way. While proximity detection independent from anyone else covers a large scope of use-cases, these answers are useful for the methods that can be used to develop different sorts of privacy-preserving functionality [15].

Privacy could be ensured in such applications by rendering the data anonymous before imparting it to application administration suppliers [13]. An anonymous location dataset gives solid privacy protection while permitting imparting to arbitrary data buyers. Anonymization, on the other hand, requires systems beyond discarding clear identifiers, since the spatiotemporal qualities of the data permits tracking and re-identification of anonymous vehicles when user density is low. Existing calculations based on the k-anonymity idea [12, 13, 14], on the other hand, adjust the location follows considerably and can't meet the exactness prerequisites of the movement observing application. Different systems [6, 7, 3] accomplish better exactness however can't promise privacy in low user density scenarios.

There exist various systems that can give a certain level of location privacy, regardless of the fact that they were initially proposed in an alternate security area. These arrangements can be ordered by significant ideas: (i) location obfuscation, (ii) data transformation, and (iii) private information retrieval (PIR). We contend that presently no procedure can help arbitrary kNN queries giving solid location privacy. All the more specifically, in location obfuscation methods (e.g., [8, 6]) the LBS can confine the customer in a little sub space of the aggregate area, prompting weak privacy. Plans based on data transformation (e.g., [16, 5]) are defenseless against access example attacks [4], which might correspond the inquiry with anomalies, famous locations, and so forth.

Together with the privacy the performance of the system should be improved while retrieving the recommendations from the servers. If the recommendation size is very large e.g. images and videos, the access time increases with the size of recommendations. Transformation and encryption provides high security but to improve efficiency and performance the size of recommendation should be reduced by using the compression algorithm.The compression technique compresses the data and stored the recommendations on to the servers.

## II. Related work

G.Ananthanarayanan et.al. [4] of combine , considers a wireless virtual social network which mimics the way individuals search information by means of social networking. Peoplenet is a basic, versatile and minimal effort architecture design for proficient information lookups in a distributed way. It uses the infrastructure to propagate queries of an offered sort to users in specific geographic locations, called bazaars. Inside each bazaar, the question is further propagated between neighboring nodes by means of peer-to-peer integration until it discovers a matching query.

Methodology [11] concentrates on k nearest neighbor (kNN) queries and characterizes the thought of location privacy, which renders a question undefined from any location in the data space. Work presented in the literature neglects to support this property for arbitrary kNN lookups. Towards this end, author present systems that offer solid location privacy, by coordinating private information retrieval (PIR) functionality. Specifically, the author utilizes secure fittings supported PIR, which has been demonstrated extremely productive and is right now considered as a functional system for PIR. At first, author invents a benchmark arrangement expanding upon a current PIR-based system. Along these lines, then distinguishes its drawbacks and presented a new plan called AHG to tackle them. At long last, author exhibit the performance superiority of AHG over the competitor, and its suitability in applications demanding the most abnormal amount of privacy [11].

Sensing segment technique [12] uses the accelerometer, microphone, GSM radio, and/or GPS sensors in these phones to catch pot holes, braking and honking. Nericell addresses a few difficulties including virtually reorienting the accelerometer on a telephone that is at an arbitrary orientation, and performing honk detection and restriction in an energy proficient way. The author [12] additionally touches the thought of activated sensing, where different sensors are used in tandem to save energy. Author [12] assesses the adequacy of the sensing capacities in Nericell based on trials led on the streets of Bangalore, with guaranteeing results.

Author [14] introduces a middleware building design and algorithms that can be used by a unified location broker administration. The versatile algorithms change the determination of location information along spatial or temporal dimensions to meet pointed out anonymity requirements based on the elements who might be utilizing location services inside a given region. Utilizing a model based on automotive activity numbers and cartographic material, the author evaluates the sensibly anticipated spatial determination for diverse anonymity constraints [14].

A customized k-anonymity model described [15] for ensuring location privacy against different privacy risks through location information sharing. The model has two unique features. Initially, author gives an integrated privacy personalization framework to support location k-anonymity for an extensive variety of users with context-sensitive customized privacy necessities. This framework allows every portable node to define the base level of anonymity it wants and also the greatest temporal and spatial resolutions it is eager to tolerate when asking for k-anonymity preserving location-based services (LBSs). Second, author devised a productive message perturbation engine which runs by the location protection broker on a trusted server and performs location anonymization on versatile users LBS request messages, for example, personality evacuation and spatiotemporal cloaking of location information. The author create a suite of adaptable and yet productive spatiotemporal cloaking algorithms, called Clique cloak algorithms to give high quality customized location k-anonymity, going for escaping or avoiding known location privacy threats before forwarding solicitations to LBS provider(s)[15].

S. Papadopoulos et.al. [16] separates the issue of location privacy in wireless networks and presents a protocol for enhancing location privacy. The essential methodology is to obfuscate a few sorts of privacy-bargaining information uncovered by a versatile node, including sender character, time of transmission, and sign quality. Authors outline is determined by real system execution and field explores alongside investigation and recreations. The framework permits users to pick the level of privacy they want, along these lines expanding the performance of less private users (while not yielding private users privacy at the same time). The author evaluated the framework based on genuine versatility data and wireless LAN coverage. The results demonstrate that a user of framework can be undefined from a thousand users in the same coverage area[16].

A framework shows a mechanism [17], for avoiding location-based data derivation of users who issues spatial queries to Location-Based Services. The author establishes transformations based on the well-understood K-anonymity idea to figure precise responses for extent and nearest neighbor search, without uncovering the inquiry source. The techniques reorganize the whole methodology of anonymzing the solicitations and transforming the transformed spatial queries.

The author [18] states the framework to support private location dependent queries, based on the theoretical work on Private Information Retrieval (PIR). Our framework does not require a trusted outsider, since privacy is attained to through cryptographic methods. Contrasted with previous work, the methodology attains to stronger privacy for previews of user locations; moreover, it is the first to give provable privacy ensures against correlation attacks. Author uses the framework to execute inferred and definite algorithms for nearest- neighbor lookups. The author updates request execution by utilizing data mining procedures, which distinguish repetitive computations [18].

Methods discussed above do not provide adequate privacy for the users location information. Introduction of anonymizer or the anonymity in the query exposes various threats to the users location privacy. The recommendation size also affects the performance of the overall design of the system .A new innovative approach to address the privacy and performance issues of the geosocial applications is discussed in the section IV.

## III. Problem Modeling

Geosocial applications provide the facilities for the mobile users to share their reviews and recommendations. These applications require continuous sensing of the users location through GPS which creates new threats for the users sensitive location information .This threat creates the need to hide the users location from the outside world. Location Privacy can be achieved by separating the location information and the data. The query performance of the existing system depends on varying review sizes. As the size of the review increases the performance of the system degrades. Reviews having large size like videos take more time for uploading and downloading form the data sever. These types of reviews should be uploaded and downloaded in less amount of time independent on the type of query i.e. point query ,circular range query or nearest neighbor query.

## IV. IMPLEMENTATION DETAILS

### *A. Implementation Details*

Figure 1. Shows the proposed system architecture.

The proposed systems workflow can be divided into two parts. In the first part, mobile user1 transforms the location information which is routed through the proxy to the sever where all the location information is stored. The recommendations specific to the corresponding locations are first com-pressed using the compression mechanism so that the size of recommendations can be efficiently reduced. The compressed recommendation is encrypted with the secrete private key called as the SPK. The secure encryption and compression procedure ends here. While routing recommendations trough the proxy server IP address of mobile user1 is not transmitted it get secured by the system.

In the next part when mobile user2 wants recommendations of specific location fires the query to the index server which intern returns the encrypted index. The mobile user2 then decrypts the index and by using that index fires another query to the data server. Data server returns the encrypted compressed recommendation. The mobile user2 first decrypts the recommendation using same SPK and decompress it. This completes the one cycle of the proposed system.

### *B. Module Description*

***1. Transform Location Co-ordinates:***

This module done on android platform, here first fetch current location co-ordinates through GPS with content (media files). Now use the transformation information to carry out transformations and then forwards to proxy server. Proxy server sends trans-formed location co-ordinates to index server, index server store location co-ordinates Map with random generator index send to user [1].

***2. Compression and Decompression Review:***

Compression module is used for the decreasing the size of the review so that it can be uploaded or downloaded efficiently from/to the data server. The compression algorithm is used for compression of review.

***3. Encryption and Decryption:***

For providing the privacy the AES algorithm is used .In this module encryption/decryption is applied on the index as well as on the compressed review .The encrypted index is stored on the index server and encrypted compressed review is stored on the data server[1].

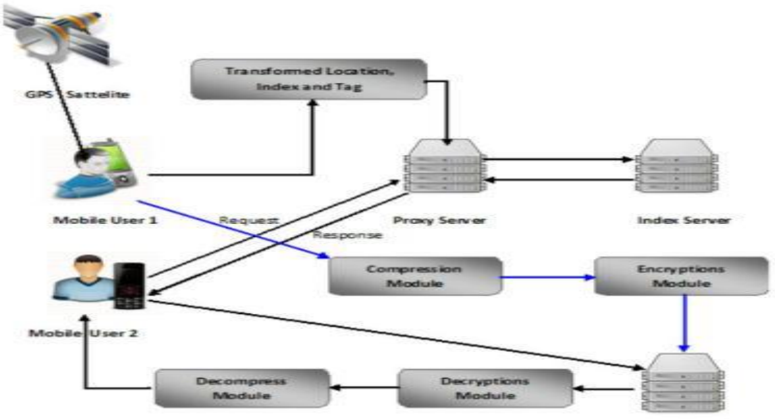

*Figure1:System Architecture*

***C.Algorithms***

**Algorithm 1: TranformLocation**

TranformLocation algorithm used to transform the co-ordinates of the location .It takes the location co-ordinates from the GPS system and transformed those co-ordinates for the further processing.

**Data:** Location co-ordinates in terms of longitude and latitude.

**Result:** Transformed co-ordinates**.**

**Begin:**

1. Retrieve longitude and latitude from the GPS system.
2. Retrieve the rotation angle and shift distance from the user.
3. Apply the rotation of co-ordinates (X,Y) by angle ‘ϴ’.
4. Apply the shift operation on rotated co-ordinates (X1, Y 1) by shift distance du.
5. Store the result of rotation and shift operation (X’,Y ‘) on to the index server.

**Algorithm 2: AddLocation**

This algorithm mainly deals with the addition of location for which user wants to write review. AddLocation (L’, PK i) →Y, location information is taken as a input and with the help of encryption key encrypted as Y.The review will be compressed and then encrypted with encryption key**.**

**Data:** The location information and reviews are received from the client.

**Result:** Encrypted location information and compressed reviews i.e image,video,text are stored in the database along with their tags and ratings.

Client →→Server→→Database

**Begin:**

1. Client sends the location information and the reviews along with their tags and ratings to the server.
2. Server first transforms the location information and apply the encryption on the transformed location information (L’, PK i) i.e Y.
3. Reviews compressed with the Quicklz4 algorithm.
4. Compressed reviews (Rcompress) and encrypted transformed location information Y are stored on the database.

**Algorithm 3: ViewLocation**

This algorithm used to view recommendations/reviews about the location. ViewLocation retrieves the ($R_{decompress}$) reviews from the database for the specific location as well as surrounded from the location depending on type of query.

**Data:** The location and the range are inputs for this algorithm.

**Result:** User get decompressed reviews i.e. image, video ,text as a response.

**Begin:**

1. The location is retrieved for the user and range is given for the review retrieval.
2. Server decompresses the reviews for the location.
3. Reviews then filtered according to the tags given to them.
4. The result set of reviews will be displayed on to the user screen as a response to the request.

***Mathematical Model***

The proposed system model can be explained by following parameters:

Consider the system S = {M, I, P, D , Loc, review, $\text{Compress}_{review}$; $\text{Encrypt}_{review}$, $S_{tgs}$}

Where, M = set of mobile users.

I = index server to which indexes are stored.

P = set of proxy servers through which requests to index severs are passed.

D = data sever which stores the encrypted compressed reviews.

Loc = Set of locations represented as longitude and latitude i.e (xi, yi).
review = Set of reviews stored on the data server.
Compress$_{review}$ = Compression algorithm to compress the review.
Encrypt$_{review}$ = Encryption function which encrypts the review.
Stgs = set of tags to differentiate reviews.
M = {m1, m2, m3,…..}
P = {p1, p2, p3 , ….}
Loc = {(x1, y1), (x2, y2), ……}
S$_{tgs}$ = {t1, t2, t3, …..}

## METHODOLOGY

In existing system while retrieving the review from the data server, if the review size more than the time required to retrieve that review is greater which decreases the performance of the application of the existing system. Therefore proposed system defines a new approach in which the application takes the location information from the user and encrypt that information and saved in the index sever as a index database .The recommendations from the user in the form of text, image, videos , compress them with the compression algorithm and save those compressed reviews/recommendations on the data server. This methodology also uses tags for the location so that they can be easily retrieved when user fires point query or circular range query.

When a user friend wants to find some reviews/recommendations, user has to enter the range of the distance and type of location he is interested in . According to the range and the type i.e. tag of the location the reviews/recommendations are retrieved from the database which is kept on the data server. The decryption of the location information is done on the server side and decompression of reviews/recommendations is done on the client side. This way the user can get recommendations about any place from his social friend circle. User can add some reviews for the same registered location by some of his friend .Proposed model also facilitates the user to add more friends by sending the friend requests.

### *A. Location Based Search*

The system discussed in this work ,proposed to overcome the shortcomings of the previously designed privacy mechanisms for the Location based search applications .Proposed system focuses on privacy of the user specific location information so that this information cannot be used for the malicious purposes as well as the compression of recommendations improves the retrieval efficiency. Application also provides the facility to retrieve the recommendations for the location from the circular range of given location and filter recommendations according to the tags given to them. This facility enables user to perform efficient search operation of the recommendations.

### *B. Compression Recommendations*

Compression recommendations use compression and decompression algorithm for compressing the size of large message or data. QuickLZ4 compression and decompression technique is used for this purpose. If the message to be encoded consists of only one character, QuickLZ4 outputs the code for this character; otherwise it inserts two-or multi-character, overlapping, distinct patterns of the message to be encoded in a Dictionary. It is useful to increase the performance of system.

## V. DATA TABLE AND DISCUSSION

### *Security Analysis*

The following Table 1 show the compression algorithm performance analysis on the basis of time required to compress the recommendations

Table 1 Comparison of Compression and Without Compression of File Uploading/Downloading

| S.NO | Algorithm | File Size (MB) | Upload Time (Min) | Download Time (Min) |
|---|---|---|---|---|
| 1 | Compression | 9 MB<br>(Before Compression file size 40MB) | 4.5 | 3 |
| | Without Compression | | 8 | 7.2 |
| 2 | Compression | 5 MB<br>( Before Compression file size 27 MB) | 3.2 | 2 |
| | Without Compression | | 6 | 3.5 |
| 3 | Compression | 12.5 MB<br>( Before Compression file size 53MB) | 7.2 | 6 |
| | Without Compression | | 12 | 9 |
| 4 | Compression | 15 MB<br>( Before Compression file size 60MB) | 8.2 | 7 |
| | Without Compression | | 13.5 | 10 |

Following bar chart shows the performance of the system with compression and without compression while uploading and downloading the recommendations. X-axis shows the size of recommendations in MB and Y-axis shows the time required to upload or download the recommendations.

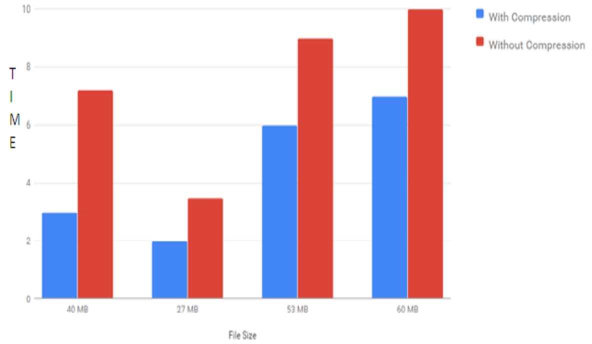

Figure2:Upload File Performance

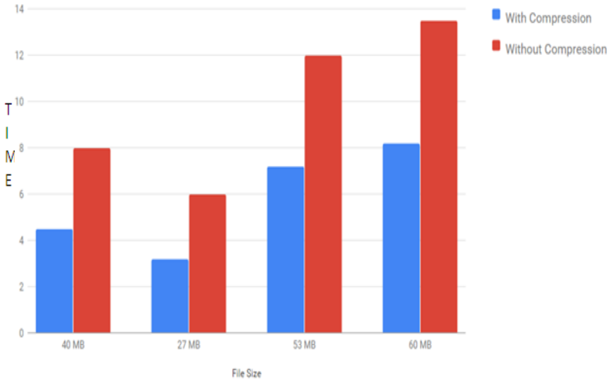

Figure3:Download File Performance

## VI. Conclusion

Here system discussed about providing the security, privacy and increasing the performance of the location-based social network system. The proposed system designed to provide a security and privacy aware protocol and recognized its completeness and soundness. Framework uses the compression technique and search by tag technique to increase a performance of Geosocial application. Existing system take time for transmitting the data or information to the server and also the for getting the correct data when the size of the message is large, which grades the performance of system. Proposed system overcomes the drawback of the existing system and improves the performance of the system by using the compression techniques.

## References

[1] Krishna P.N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal , Amr El Abbadi, Christopher Kruegel, and Ben Y. Zhao," Preserving Location Privacy in Geosocial Applications" , IEEE Transactions on Mobile Computing, vol. 13, no. 1, January 2014

[2]M. Motani, V. Srinivasan, and P.S. Nuggehalli, "PeopleNet:Engineering a Wireless Virtual Social Network," Proc. ACMMobiCom, 2005.

[3]M. Hendrickson, "The State of Location-Based Social Networking on the iPhone," http://techcrunch.com/2008/09/28/the-state-oflocation-rebased-social-networking-on-the-iphone, 2008.

[4]P. Mohan, V.N. Padmanabhan, and R. Ramjee, "Nericell: Rich Monitor-ing of Road and Traffic Conditions Using Mobile Smartphones," Proc. Sixth ACM Conf. Embedded Network Sensor Systems, 2008

[5]G. Ananthanarayanan, V.N. Padmanabhan, L. Ravindranath, and C.A. Thekkath, "Combine: Leveraging the Power of Wireless Peers through Collaborative Downloading," Proc. Fifth Intl Conf.Mobile Systems, Ap-plications Services, 2007.

[6]M. Siegler, "Foodspotting is a Location-Based Game that Will Make Your Mouth Water," http://techcrunch.com/2010/03/04/ foodspotting, 2013.SCVNGR, http://www.scvngr.com, 2013.

[7]B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protec-tion," Computer, vol. 36, no. 12, pp. 135-137, Dec. 2003.

[8]F. Grace, "Stalker Victims Should Check for GPS," http:// www.cbsnews. com, Feb. 2003.

[9]A. Gendar and A. Lisberg, "How Cell Phone Helped Cops Nail Key Murder Suspect. Secret Pings that Gave Bouncer Away,"New York Daily News, Mar. 2006.

[10]M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," Proc.First Intl Conf. Mobile Systems, Applications Services, 2003.

[11]M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: APrivacy-Aware Location-Based Database Server," Proc. IEEE 23rd Intl Conf. Data Eng., 2007

[12]B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Per-sonalized Anonymization Model,"Proc. IEEE 25th Int'l Conf.Distributed Computing Systems, 2005.

[13]Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[14]T. Jiang, H.J. Wang, and Y.-C. Hu, "Preserving Location Privacy in Wireless Lans," Proc. Fifth Intl Conf. Mobile Systems, Applications Services, 2007.

[15]P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge Data Eng., vol. 19, no. 12,pp. 1719-1733, Dec. 2007.

[16]G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD Intl Conf. Management Data, 2008.

[17]S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest Neighbor Search with Strong Location Privacy," Proc. VLDB Endowment,vol. 3, nos. 1/2, pp. 619-629, Sept. 2010.

[18]A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," Proc.Network Distributed System Security Conf., 2011.

[19]G. Zhong, I. Goldberg, and U. Hengartner, “Louis Lester and Pierre: Three Protocols for Location Privacy,” Proc. Seventh Intl Conf. Privacy Enhancing Technologies, 2007.