Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 6, June -2015

# THIRD PARTY IDENTITY DIFFUSER TECHNIQUE FOR THE PRIVATE LOCATION BASED QUERY USING THIRD PARTY IDENTITY DIFFUSER

**Megha Chavda[1], Dr. Vipul Vekariya[2]**

[1] *PG Research Scholar, Department of Computer Engineering, Noble Group of Institutions,*
[2] *Associate Professor, Department of Computer Engineering, Noble Group of Institutions,*

**Abstract:** *Privacy Concerns in LBS exist on two fronts: location privacy and query Privacy. In this paper we investigate issues related to query privacy. In particular, we aim to prevent the LBS server from correlating the service attribute. An important privacy issue in Location Based Services (LBS) is to hide a user's identity while still provide quality location based services. Recently, highly accurate positioning devices enable us to provide various types of location-based services. On the other hand, because position data obtained by such devices include deeply personal information, protection of location privacy is one of the most significant issues of location-based services. Therefore, we propose a technique to anonymize position data. In our proposed technique, the personal user of a location-based service generates several false position data (dummies) sent to the service provider with the true position data of the user. Because the service provider cannot distinguish the true position data, the user's location privacy is protected. But from this method traffic will be increase. As a solution, a diffuser can be placed between mobile unit location based services. Diffuser will send dummy locations to LBS and true data exchange will only be happen between mobile unit and diffuser. The traffic between mobile unit and diffuser will be decrease.*

***Key Words:*** *Location Privacy, Location-based Services, LBS, Privacy Preserving Approaches*

## I. INTRODUCTION

Availability of low cost Smartphone with good processing capacity and equipped with various positioning technology have powers location based services (LBS). Popularity of LBS is dramatically increasing among mobile users day by day. Consumers are understand and adopting LBS worldwide. Study shows that there are 486.0 millions mobile location based service users worldwide by year 2012 [1]. There is 47.7 % change in users from previous year. Today's smart phones, tablets and connected devices are virtually all GPS enabled thus allowing for a myriad of LBS like Geo-fence services: friend/family tracking, Enterprise Fleet Tracking, Travel and Point of Interest (POI), Geo-tagging, Check-in Based Contest and Games, Local search, Local/Hyperlocal Content, etc.

Almost all of the above LBS use location server that knows about location of users in order to provide customized services. Sometimes verify authenticity of location server is not possible. However, Users of LBS have to share their location information with these location servers to use their services. Some unauthorized and un-trusted location server may leak or misuse location information of their subscriber these leads term *location privacy*. Several issues of misusing their location information by service provider are reported worldwide. Many researchers have work toward this problem. There are many approaches and techniques to preserve privacy in LBS, but there are some strengths and weaknesses in every approach. In this paper we have analyzed each approach and highlighted their strengths and weaknesses. As illustrated in Figure 1, these approaches can be classified into groups based on the techniques they use. The groups are *cloaking, transformation, obfuscation, private information retrieval (PIR).*

To protect against various privacy threats while using LBS, several studies have proposed different approaches to protect the privacy of users while interacting with potentially untrusted location servers, hence coining the term *location privacy*. In this paper, we present a taxonomy of approaches proposed for the location privacy problem. As illustrated in Figure 1, these approaches are based on *anonymity/cloaking*, *transformation* and *private information retrieval* (PIR) techniques. We study each group in more details and briefly show how each approach supports sample spatial queries used in LBS.

 

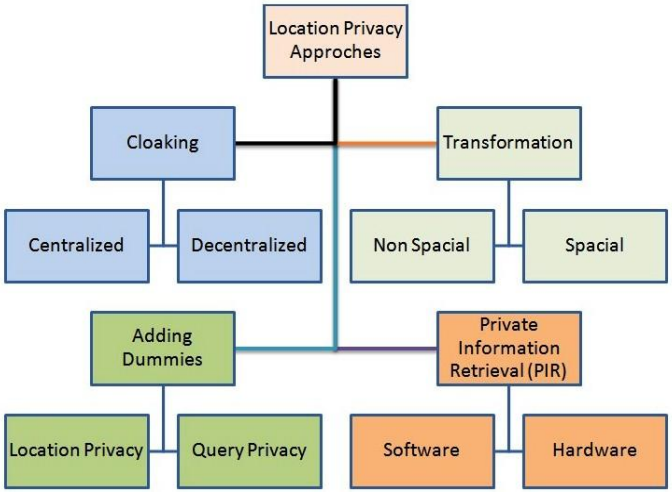


**Fig -1**: Location Privacy Approaches

## II. DUMMY BASED PRIVACY PRESERVING APPROACH

In cloaking techniques user sends position data with reduced precision to service provider for anonymous use of location based service. Service provider cannot determine exact location of user; it can learn only less precise location details of user. Such techniques have some problems. Some query processing requires precise location but this technique cannot provide exact location. Further, observer can easily comprehend users moving trajectory from observing cloaked region for several minutes.[3] To overcome this problems Hidetoshi Kido(2005)[2] proposed dummy based approach for privacy preservation of location based service. In this approach user sends true position data with several false position data (dummies) to a service provider, who creates a reply message for each received position data. The user simply extracts the necessary information from the reply message. In this manner, even if the service provider stores the set of position data, it cannot distinguish the true position data from the set of position data. Third Party Identity Diffusion is the broad area for the security of the user in Location Based Services.

### 2.1 System overview

The basic idea behind this technique is to send true position data including noise to service provider. So, service provider cannot determine exact position data of user. The noise consists of a set of false position data called dummies. Hidetoshi Kido(2005) proposed anonymous communication technique for LBSs based on dummies as shown in Figure 4.1. Theservices procedure from beginning to end follows:

1. An LBS user obtains his own position data r from a device such as GPS.
2. Dummies are generated at positions 1 and 2.
3. The user creates a service requiring message S that includes position data at r, 1 and 2 and sends S to the service provider.
4. The service provider creates a service answered message R that responds to receiving all position data and sends R to the user.
5. The user receives R and only picks up necessary data from R.

This technique also requires some real time dummy generation techniques because if randomly generated dummies are used than anyone can find difference between true position data and dummy data. Hidetoshi Kido(2005) also proposed two dummy generation algorithm.

- Moving in a Neighborhood (MN)

In this algorithm, the next position of the dummy is decided in a neighborhood of the current position of the dummy.

- Moving in a Limited Neighborhood (MLN)

In this algorithm, the next position of the dummy is also decided in a neighborhood of the current position of the dummy. However, the next position is limited by the density of the region. This algorithm is adaptable in cases where the communication device of the user can get other user's position data.

## III. THIRD PARTY IDENTITY DIFFUSER – PROPOSED APPROACH

Current work on dummy based techniques focus either on location privacy or query privacy, while our proposed approach will preserve privacy of both at same time using dummy. Location privacy means hiding true location of user and query privacy means hiding true POI (service attribute) or query of user. Dummy generation algorithm should generate dummies for both location and POI. Third Party Identity Diffuser will be added between the user and the service provider.

 

In this proposed techniques the traffic increasing problem of the dummy location adding was removed and the reliability, stability of this technique is better than the other techniques. Complexity of these techniques is lesser than the spatial and non-spatial techniques. Original data of the user (Users Private Information) will be hidden from the service provider by the third party diffuser. It will only be communicated between the user and the third party diffuser. The service provider will only get the data which is sent by the third party identity diffuser which is implemented between the User and the Service Provider.

### 3.1 System architecture

Our proposed system architecture is based on client-server model. In our system anonymity, Third party identity diffusers are generated at user side. The architecture of the overall system of our proposed plan is shown in Figure 2. In this architecture there are three main components. The user equipment, middle infrastructure and the service provider infrastructure. Figure 3 shows the block diagram of our proposed architecture.

Our proposed system architecture consists following main components:

1. Positioning infrastructure.
2. Third Party Identity Diffuser
3. LBS server

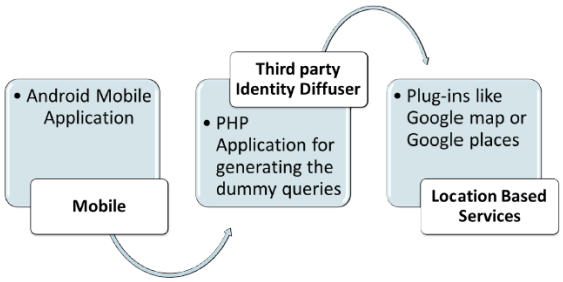


**Fig -2**: Architecture of Proposed System

#### 3.1.1 Positioning infrastructure

Position infrastructure provide location details for LBS. positioning infrastructure made with mobile device (smartphone, PDA, tablets) with positioning capabilities. Positioning infrastructure also has network capability for help mobile device to determine position. Positioning device uses various techniques to determine position like GPS, network triangulation, cell id, Wi-Fi access point, etc.

#### 3.1.2 Third Party Identity Diffuser

For anonymous use of LBS we use our third party identity diffuser which will be implemented between the user and the service provider. Diffuser will hide the original user's data from the service provider for the security and the original data will only be communicated between the third party identity diffuser and user or Positioning Infrastructure. Third Party Identity Diffuser system is responsible for generating dummy data which is look like true location and relevant to service attribute for the service provider.

#### 3.1.3 LBS server

LBS server provides services for location based services. LBS server stores various GIS information, location details, POIs information, etc. LBS server answers query issued by mobile devices based on location provided into query.

 

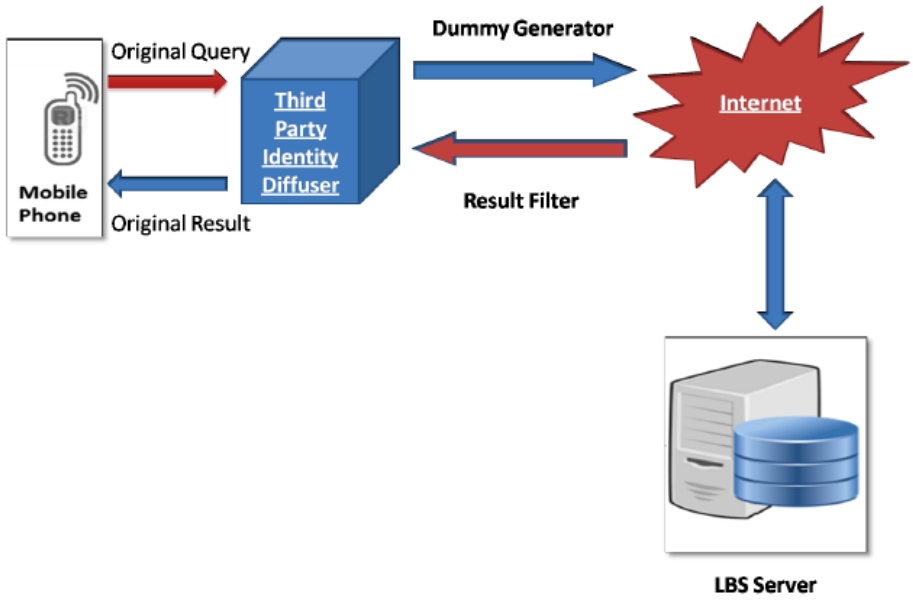


**Fig -3**: Block Diagram of our proposed system

## IV. IMPLEMENTATION AND FUTURE WORK

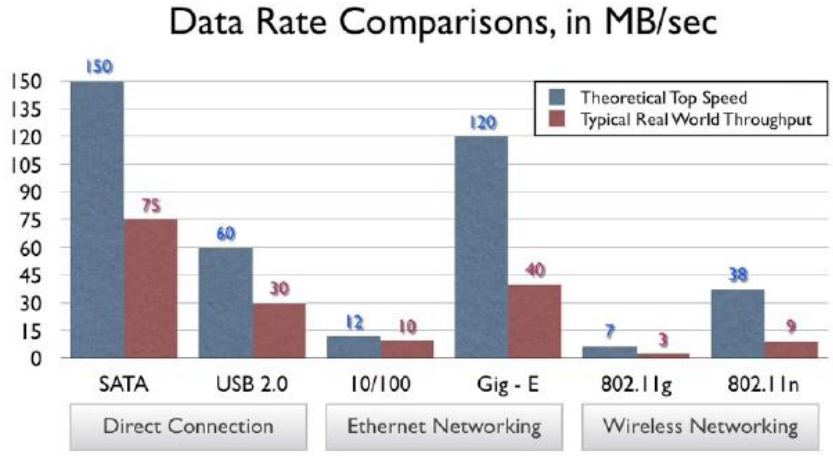


**Fig -4**: Comparison Graph of wireless and wired connections

### 4.1 Comparison with existing architecture

The existing techniques show that in any technique either location of the user or query of the user will be served [3]. We are proposing the third party identity diffuser which will generate the dummy location as well as dummy queries for the original user location and original user query. As we know the speed in wireless connection is less compared to the wired connection [18]. The figure shows the comparison graph of the wireless and wired connection.

The user data send to the LBS will take more time because of the wireless connections between user and service provider. So the third party implementation will increase the speed of the user connection. Till now the dummy generation was the part of the client or user side so if we are generating more dummies than it will take more time for each query or location of user. By implementation of the third party identity diffuser the time consumed will be almost half of the time in existing system. Generally the speed of wireless connection will be maximum 56 mbps when the speed may be 100 mbps in case of wired connection. It shows that the wireless connections are slower than the wired connection which is the main advantage of this technique.

### 4.2 Architecture of simple third party diffuser

In this work we have initiated one privacy protecting approach based on dummies which protects user's location privacy as well as query privacy. In our approach system generation fake location and fake service attributes and sends it with true position and service attribute to hide user's exact location and query. The main benefit of this new technique is the speed. Generally the connection between user and service provider is slow due to wireless connection the connection between service provider and LBS is fast due to wired connection.

 

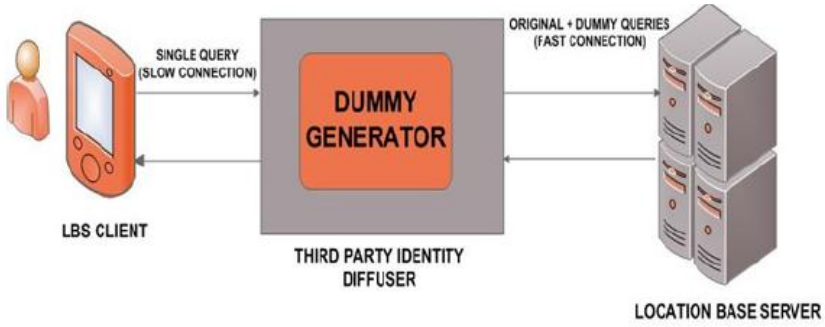


**Fig -5**: Architecture of simple third party diffuser

### 4.3 Detailed Architecture - Third Party Identity Diffuser

The Third party identity diffuser will generate the dummy queries for the location of the user and for query generated by the user. The query generated by the user will be reached to the third party identity diffuser and it will generate new queries according to the virtual grid shown in the figure.

For Example if the query is generated from the point 6 then the algorithm will send the random location in addition of 1 to 10. Same as the location, query(user data) can also be implemented with same strategy. The basic idea behind this technique is to send true position data including noise to service provider. So, service provider cannot determine exact position data of user. The storage element in the third party diffuser will store the previous data so that at the time of new query generation the same data cannot be fetched. We are implementing the strategy which will serve to secure the query and location privacy both in this technique. We will facilitate the user query as well as users location security at the same time and dummies will be generated for the users location as well as for the users query. We can also add the storage element for storing the searching attributes for the future reference for the same query generated by the user for same location. We have made a mathematical equation for the algorithm on this third party diffuser will work. The original query of the user will be reached to the third party diffuser and it will generate the dummy queries and send it to the Location Based Services. The original data whether it is location or query will be made secured or private by the third party identity diffuser. So the third party diffuser will store the original query and fires the dummy queries according to the algorithm explained with the mathematical equation.

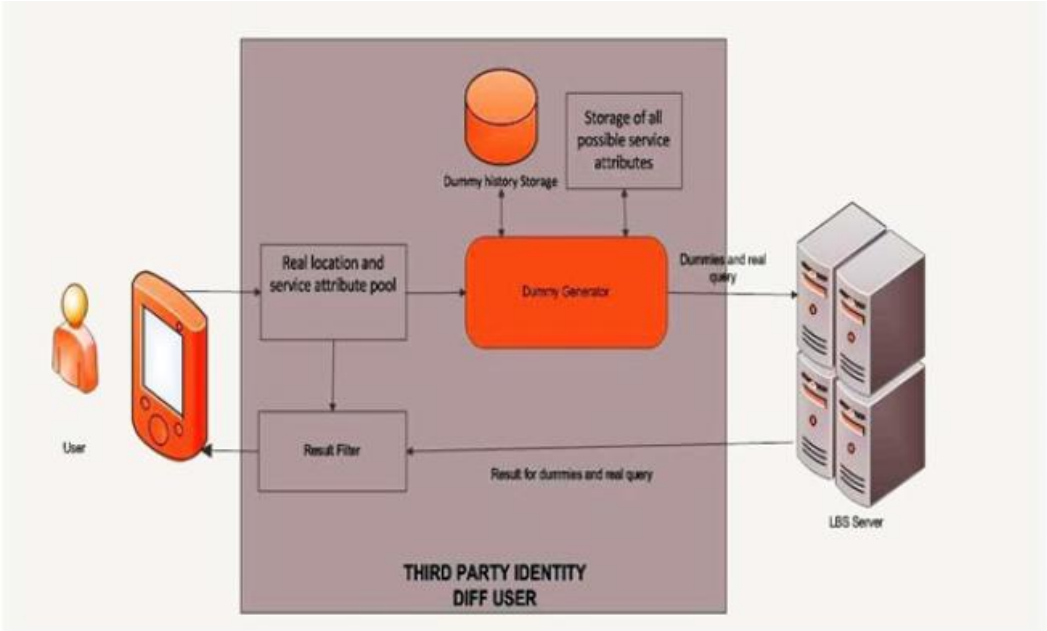


**Fig -6**: Third Party Identity Diffuser

This mathematical equation shows the algorithm for generating the dummy queries. This will make a virtual square grid at which dummy queries and location can be fired.

### 4.4 Algorithm for third party identity diffuser

 

The algorithm for the third party identity diffuser is explained by the mathematical equation mentioned below. We are generating the queries based on these expressions. For the location having longitude and latitude and it is identified with x coordinates and y coordinates in this research work.

$$D_y = \sum R_y + Rand\ [0:100]$$

$$D_x = \sum R_x + Rand\ [0:100]$$

We are generating dummy x coordinates with the original x coordinate of the user location. We are also generating y coordinated with the original y coordinate of the user location.

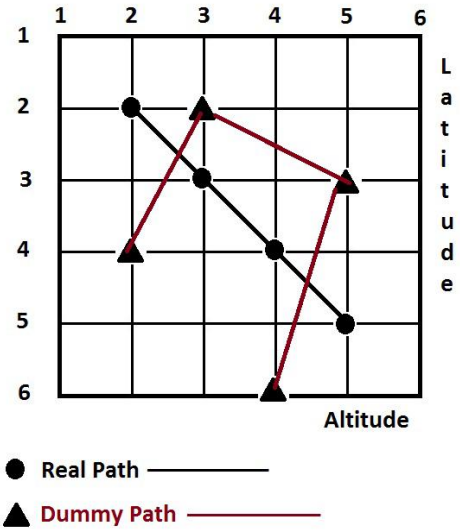


**Fig -7**: Implementation of Third Party Diffuser

The first equation mentioned above is generating the dummy x coordinates with the original x coordinates of the user location. It will add random number between 0 to 100 in the x coordinate of the user location and generates the new dummy location coordinates. The next equation mentioned above will generate the dummy y coordinated with the original y coordinate of the user location. It will add random number between 0 to 100 in the y coordinate of the user location and generates the new dummy location coordinates.

$$L_{xi} = R_x + D_x$$

$$L_{yi} = R_y + D_y$$

This above mentioned equations will generate the dummy location coordinates for each query generated by the user. It will generate dummy x coordinated for each dummy location randomly and y coordinates for each dummy location randomly. The above mentioned equation will generate the dummy locations in square virtual grid which is shown in figure 5.4. It is showing the dummy path as well as original path of the user. This square virtual grid is only showing 1 dummy location generated for each locations. The algorithm on the platform of VB is shown in below mentioned figure.

In above mentioned figure 7, there are three functions for generating the dummy location for the true query generated by the client. The first function of the algorithm will generate the dummy x coordinates for the true x coordinates of the user location. The second function will generate the dummy y coordinated for the true y coordinated of the user location. And the third function will generate the dummy locations combined with latitude and longitude of the user true location. The number of dummy location can be varies according to our algorithm or it can be set according to the need. The location coordinated will be generated on the random basis so that the true location cannot be tracked by the threats. The dummy generation will be generated only on the virtual grid shown in figure 7. It can also be implemented with the circular path or crystal path so that the dummy path of the user can not be detected by the threats.

### 4.5 3P Client Application for query generation

3P Client is a client side simulation of our approach, it received users query and location from user and sends it to our third party identity diffuser. 3P client simulation is implemented using android platform. We have chosen android platform for client side simulation because generally Location based services used on mobile device.

 

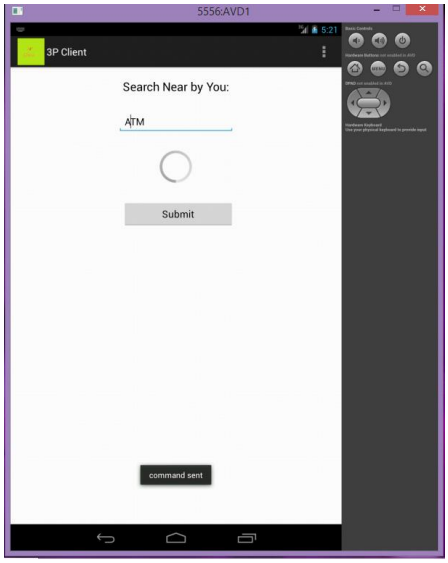


**Fig -8**: 3P Client Application view

Here in this screenshot user search ATM for his service attribute, 3P client sends this service attribute to third party identity diffuser with current location of user.

### 4.6 LBS server simulation

We have used Google map API to visualize result of 3rd party identity diffuser. 3P client sends real location and service attribute to 3rd party identity diffuser and 3rd party identity diffuser add some dummy location and service attribute in original query and send it to LBS server.

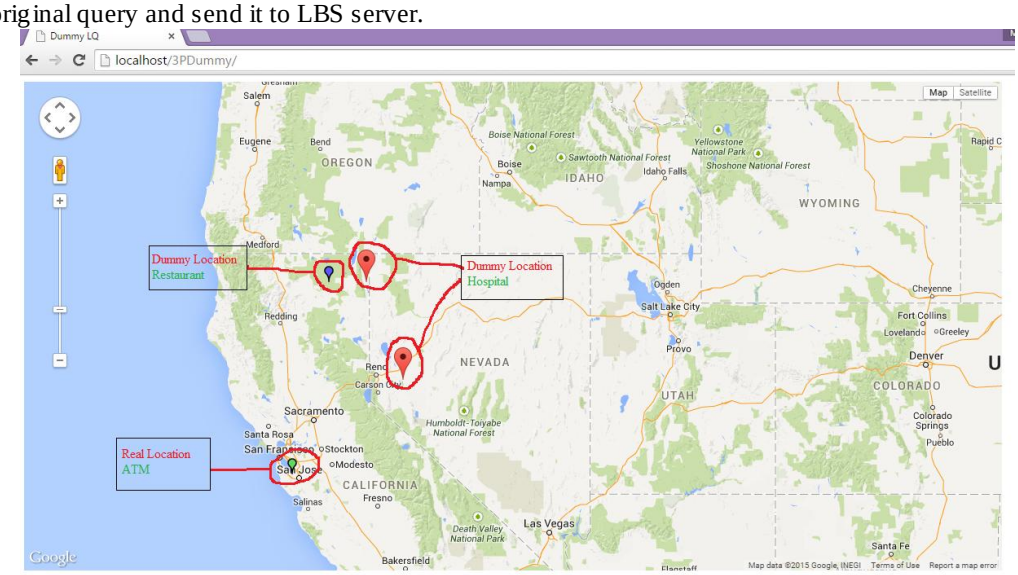


**Fig -9**: LBS server simulation snap

Here in this screenshot we have visualize result of users query ATM which we have search in our 3P client. As we can see real location and service attribute ATM is marked with green color marker and dummy locations and service attributes like hospital and restaurant are marked with red and blue color markers respectively.

## V. FUTURE WORK

In this technique user can have the query in square virtual grid. In future instead of square virtual grid, circle or pyramid grid can also be made so the dummy path cannot be detected. The query and location of the user can be secured from the threats with help of algorithm of circular dummy path. The third party identity diffuser capability can be increased according to the user need and the user data security can be increased.

Table 1 shows the different approaches comparisons

**Table -1:** Comparison of different classes of proposed approaches for location privacy

| *Technique* | *Reference* | *Query type* | *Major strengths* | *Major weaknesses* |
|---|---|---|---|---|
| Centralized cloaking | Mokbel et al. (2006), Gruteser and Grunwald (2003), Gedik and Liu (2005a, 2005b) and Du et al. (2007) | Range/KNN | Spatial query support, support for querying dynamic data | Major privacy leaks, trusting a third party, privacy/quality of service trade-off |
| Decentralized Cloaking | Duckham and Kulik (2005), Kido et al. (2005), Ghinita et al. (2007b, 2007c) and Chow et al. (2006) | Range/KNN | No need for a centralized anonymiser, Stronger privacy support compared to centralized cloaking | Costly communication complexity, assuming all users are trusted, privacy leaks, privacy/quality of services trade-off |
| Non-spatial Transformation | Indyk and Woodruff (2006)and Zhong et al. (2004, 2007) | Customized two-party computation queries (private distance approximate, private co-location comparison, etc.) | Perfect privacy guarantee, very efficient customized Queries | Prohibitive linear computation or communication complexity for classic spatial queries |
| Spatial Transformation | Lin (2006), Khoshgozaran and Shahabi (2007) and Yiu et al. | Range/KNN | Efficient spatial query processing, support for querying dynamic objects | Privacy leaks under certain object distribution, privacy/quality of service trade-off |
| Dummy Location | H. Kido(2005), IEEE | Dummy queries + real Data | Perfect privacy guarantee, Reliable | Network Traffic Overhead, High computation and communication complexity |
| Third Party identity diffuser | Proposed | Range/KNN | Security, Avoiding location of individual, dummy location broadcasting | Traffic intensity increases, more complex |

## VI. CONCLUSION

Approaches proposed for protecting user's location information in LBS. The first class of approaches, based on cloaking and anonymity techniques, offer flexible schemes to support privacy-aware location servers responding to various spatial queries. However, they suffer from multiple privacy leaks under certain user or query distributions. The second classes of approaches are based on transforming the queries to blind the server from knowing a users location while evaluating location queries. With these approaches, users have to trade-off their privacy with the quality of service they receive from location-based services. Finally, the third class of PIR approaches addresses all privacy concerns of the previous approaches. However, they incur expensive computations or rely on a trusted platform to execute the queries. Table summarizes the properties of each category of approaches. Each table column represents the dominant properties shared among the proposed approaches under each category. Location privacy research is still in its infancy. While creative solutions have been proposed to solve the location privacy problem, there are still many challenges to be addressed. Devising a framework that while ensuring perfect privacy, can very efficiently respond to various spatial queries dealing with both static and dynamic objects is still an open problem and far from what the existing approaches offer. Third Party Identity Diffusion is the solution for the security of the user's location. It will be implemented between the user and service provider. This technique is very much beneficial and more efficient technique which will avoid the network overhead.

## REFERENCES

 

[1] M. Gruteser and D. Grunwald. "Anonymous usage of location based services through spatial and temporal cloaking". In Proceedings of the First International Conference on Mobile Systems, Applications, and Services, pages 31-42, 2003.
[2] W.Shinn Ku , Yu Chen , R. Zimmermann, "Privacy Protected Spatial Query Processing for Advanced Location Based Services" Springer Science+Business Media, LLC. 2008.
[3] A. Masoumzadeh, J. Joshi, "An Alternative approach tok-anonymity for Locaion Based Services", Procedia Computer Science 5 (2011) 522-530.
[4] M. Mokbel, C. Chow and W. Aref, (2006), "The new Casper: query processing for location services without compromising privacy", VLDB, pp.763774.
[5] M. Wernke, P. Skvortsov, D. Frank, K. Rothermel, A Classification of Location Privacy Attacks and Approaches., Personal and Ubiquitous Computing manuscript, Springer-Verlag 2013.
[6] P. Indyk and D. Woodruff, Polylogarithmic private approximations and efficient matching TCC, pp.245264 , 2006.
[7] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services." Proceedings of the 21st International Conference on Data Engineering (ICDE 05), 2005 IEEE.
[8] A. Pingley, W. Yu, N. Zhang, X. Fu, W. Zhao,, S.Subramaniam, "Protection of Query Privacy for Continuous Location Based Services.", IEEE INFOCOM 2011.
[9] "Mobile Location Based Service Marketing Whitepaper." , Mobile Marketing Association, October 2011.
[10] K. Liu, J. Zhang, J. Yang, "Dummies and Nearest Neighbor Based Location Privacy Protection.", Journal of Information & Computational Science, 3831-3839, August 10, 2013
[11] C. Chow, M. Mokbel and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based services", ACM-GIS, November 10-11, 2006.
[12] L.Wang, S.Wu, " Protecting Location Privacy through Identity Diffusion", IEEE, ISBN No. 9781-4244-39416/09, September-2009.
[13] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized k- Anonymity: Architecture and Algorithms.", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 1, JANUARY 2008.
[14] A. Khoshgozaran and C. Shahabi, "Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy.", LNCS 4605, pp. 239257, Springer-Verlag ,2007.
[15] M. F. Mokbel, C.Y. Chow, and W. G. Aref. "The New Casper: Query processing for location services without compromising privacy.", VLDB, ACM, 2006.
[16] H. Lu, C. S. Jensen, M. L. Yiu, "Privacy-area aware, dummy-based location privacy in mobile services", In: Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access, 2008, 16-23
[17] M.Wernke , P. Skvortsov, F. Durr and K. Rothermel, "A Classification of Location Privacy Attacks and Approaches", Personal and Ubiquitous Computing, Springer 2013.
[18] N. Kaur, S. Monga, "Comparison of wired and wireless networks"; International Journal of Advanced Engineering Technology, E.ISSN0976, 3945, Sep-2014.

## BIOGRAPHIES

**Megha K. Chavda** received her B.E. degree in Computer Engineering from Govt. Engg. College, Gandhinagar, Gujarat, India. She is pursuing M.E. degree in Computer Engineering from Noble group of Institutions (Junagadh, Gujarat) under Gujarat Technological University (Gujarat).

**Dr. Vipul Vekariya** received her B.E. as well as M.E. degree in Computer Engineering. He has also done Ph.D. in CSE. Currently, he is working as associate professor and Head of department of Computer Engineering and information technology at Noble group of Institutions (Junagadh, Gujarat) under Gujarat Technological University (Gujarat). He is also having teaching experience of more than 10 years.

 