ISSN:0975-9646

User Privacy Preservation in Mobile Cloud Computing by Two Levels of Spatial Cloaking

Lijo V P
School of Computing Science and Engineering
VIT University, Vellore

Revathy Gangadaren
Department Computer Science and Engineering
MES College of Engineering, Kuttippuram

Abstract-The world of Mobile grows day-by-day, even hourly basis to attracts and sustain the mobile users with all types of computing applications. To enrich its capability for giving more computing power mobile combined with the giant of computing world cloud, and derived a novel term 'Mobile Cloud Computing' (MCC). Mobile Cloud Computing means to provide the facility to use mobile phone as an information processing system. Mobile phone will act as a floating server in near future. The mobile serves the users with plenty of services which include location-based services. Users' fear to disclose their exact privacy information to the untrusting location based servers is a barrier to get full strength usage of such services. Anonymity based technique cloaking serves at an extend to protect users privacy. Cloud based Cloaking takes the cloaking task to cloud and freed the mobile from the risk of battery run out by heavy computation task of cloaking. Even though results show it uses less mobile memory and low battery consumption the user has to take risk of trusting third party's cloud instead of location-based servers. To overcome this risk of revealing privacy information to the cloud, make a small level cloaking at mobile phone and a higher level of cloaking at cloud. This two level cloaking improves the trust factor without giving more computational load to the mobile device.

General Terms- Privacy, Cloud Cloaking

Keywords- Mobile Cloud, Spatial Cloaking, Mobile Security.

1. INTRODUCTION

The mobile computing becomes more popular nowadays. New applications arrives markets daily to attracts the users and make them to rely on mobile phone to satisfy most of their computing tasks. The popularity of GPS technology boosts the booming of many location- based services and serve the users better than previous days.

The expeditious growth of mobile industry and the use of resource limited devices, has given rises to many new mobile security issues [5]. The privacy breaches are very high with the tremendous use of location based services in the mobile cloud environment. Protecting the privacy without affecting the quality of the service is a great challenging task. Cloaking is potential to meet this task even this is encroaching the safe stage of memory and battery life. Cloud based cloaking gives relief on these tiresome issues.

Nowadays Cloud computing becomes more popular and most of the IT Industries start to get in to Cloud computing world. It is a type of distributed computing with many fascinating features such as virtualization, scalability, availability, reliability, etc and the term cloud is originated from the earlier large-scale distributed telephone networks which was scalable and virtual in nature. Cloud service providers are ready to serve the costumers with different mode of services. Services may in form of software, computing platform, or hardware infrastructure, etc.

The core concept of cloud computing is reducing the computational and processing burden on the local terminal by taking those tasks to constantly improving data-centers. Cloud Computing helps to satisfy customers' computing needs by compute on some remote centralized facilities, instead on local devices [9]. Cloud computing extends the scope of service oriented architecture to the development platform and the execution infrastructure, and thus cloud computing [1] is typically characterized by the features such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Software as a service is software that is deployed over the internet and this is a pay-as-you-go model. Platform as a Service, provide development environment as a service. Infrastructure as a service delivers a platform virtualization environment as a service. Rather than purchasing servers, software, data-center space or network equipment, clients instead buy those resources as a fully outsourced service.

Mobile platforms gives a space to use Cloud computing and it has invoked a new wave of evolution in mobile world. Mobile Cloud Computing (MCC) [2] or cloud computing for mobile world [3] is a disruptive technology for future mobile applications and it refers to an emerging infrastructure. MCC [2] can be defined as a combination of mobile web and cloud computing, where the data storage and processing will happen inside the cloud and so outside of the mobile devices. So the mobile devices can be a thin client to initiate all the computing tasks and those tasks are transferred and processed in the cloud. Since cloud computing applications go through a browser, the end users mobile operating system does not have any impact on the application. Along with the cloud of benefits, there are a large number of security and privacy issues to be addressed. Mobile Cloud Computing is prone to have issues of network availability and intermittency. Also Mobile Cloud Computing concepts rely on an always-on connectivity and will need to provide a scalable and high quality mobile access.

The mobile security is becoming more and more important as the mobile phone is using as the device for web browsing, accessing location-based services and other computing tasks. The computing power and memory capability of mobile phones are hard to completely meet the requirements of running resource intensive services. In this context we consider mobile users security than mobile data security. In mobile cloud computing, the security systems run in cloud to reduce the memory usage in mobile phone and maintain the battery life by computing resource intensive items.

The scare resources inside the mobile platforms seldom meet the requirements of resource intensive services. Security systems make the situation even worse by running time-consuming and energy devour processes. Antivirus, SIM RM and cloud based intrusion detection are some of the cloud based mobile security systems.

Authentication framework is proposed [4] for mobile users in the clouds. This is identifying all the users uniquely and assigned identification number to each and every user.

Features of Mobile Cloud Computing are summarized as follows:

Mobile device makes use of Cloud storage, all computational tasks are carried out in cloud, extending battery life, improving processing power by in cooperate cloud in computing, dynamic provisioning of resources, multi-tenancy, improved scalability and ease of integration.

Challenges of MCC are to handle heterogeneity in wireless network interfaces, multiple operating systems (Android, iOS, Windows), multiple browsers (Safari, IE, Opera Mini, Fire Fox), multiple devices (Samsung, Sony, Nokia, Apple), limited device memory and storage and limited battery life [5].

2. LITERATURE SURVEY

Ubiquity of positioning technologies lead to the enormous arrival of many Location based services (LBS) [8] in mobile devices. Mobile users are heavily depends on such applications to satisfy many needs, to identify nearest hospital or hotel. For effective utilization of these services the user needs to provide location information to the LBS services provider (SP). Privacy issues arise if the adversary can track out who raise the request and/or the location of the requester.

This privacy threat will be high if the user is unaware about this kind of risks and reveal very sensitive information. To prevent this mobile device itself posses a complex data structure to make all requests are anonymous. The anonymity is achieved by constructing cloaked regions and conceals users' private information in the cloaked area. In device cloaking is using a complex data structure and processing cloaking algorithm in device will consume more device memory and reduce the battery life.

In Mobile Cloud Computing context most of the tedious tasks are transferred to the cloud and cloud will process them and keeps the data in cloud. As Ravathy [5] proposed in recent literature to shift cloaking from mobile device to cloud for saving device memory and battery life.

The mobile users are showing more interest for using location based services. Advancement in positioning techniques such as Global Positioning Devices (GPS), Radio Frequency Identification (RFID) and the wireless short range techniques is the major cause to get rise of many LBS applications. LBS applications are prone to privacy breaches by collecting users' private information such as location, identity information, etc. With widespread use of LBS and recent advances in location tracking technologies the vulnerability to privacy are increasing. With untrustworthy LBS providers, the revealed private location information could be abused by adversaries.

Use of LBS applications without the fear of privacy leakage is a wish of researchers and mobile application designers. So this paper is aimed to analyze different privacy protection techniques.

Privacy preserving techniques for protecting privacy by hiding location identity are based on one of the following concepts.

(a) Space transformation: The user location information and data are transformed into another space in which their exact or approximate spatial relationships are maintained to answer location-based queries.

(b) Use of Dummies:

Propagate fake location (dummies) to location-based server to hide location identity.

(c) Cloaking. The main idea of the cloaking technique is to present data differently to servers to preserve user's privacy. Spatial cloaking uses K-anonymity concept to give a blurring effect on location information.

Spatial cloaking are classified based on their architecture such as peer-to-peer (P2P), distributed and centralized [6].

Mobile users agree to work as a group to make cloaked areas and hide location information by blurring their location, in peer-to-peer model. In this model all of the users are having same level of responsibilities instead to act as centralized or distributed servers.

In the distributed architecture model, the mobile users maintain a complex data structure to anonymize their location information through mixed communication infrastructure, i.e., base stations. It is hard to use this model in highly dynamic location based applications, as it is tedious to maintain this complex data structure.

For the centralized architecture model, a trusted third party, termed location anonymizer, or location trusted server is placed between the user and the location-based service provider. The location anonymizer is responsible for blurring users' exact locations into cloaked areas that satisfy their privacy requirements, and for communicating with the service provider. This architecture model could pose a scalability issue because it requires all the mobile users to periodically report their exact locations to the location anonymizer. Also, storing the user's exact location at a server could pose a privacy breach, i.e., a single point of attacks.

2.1 Peer-to-Peer Architecture Model

The P2P k-anonymity model [7] is proposed by ChiYin Chow et al. The algorithm constitutes the initial peer and other k-1 mobile peers to a group to achieve the users privacy with two important requirements: k and A_{min}. Where, k indicates the indistinguishable degree for the group. So the initiator cannot be distinguished from other k-1 peers and it will be k-anonymity. A_{min} means the

minimum resolution of the cloaked area. The algorithm has several steps:

1) Select a central peer who will act as a agent for the group.
2) The central peer will discover other k-1 different peers via single-hop or multi-hop to compose the group of k users.
3) Find a cloaked region covering all locations that every peer may arrive.
4) Adjust the cloaked region. Once the cloaked region is less than A_{min}, the region will be expanded. Fig 2.1 illustrates the working example of the algorithm.

From the example, the request initiator m10 collects other 5 peers for the users privacy profile *k=6*.

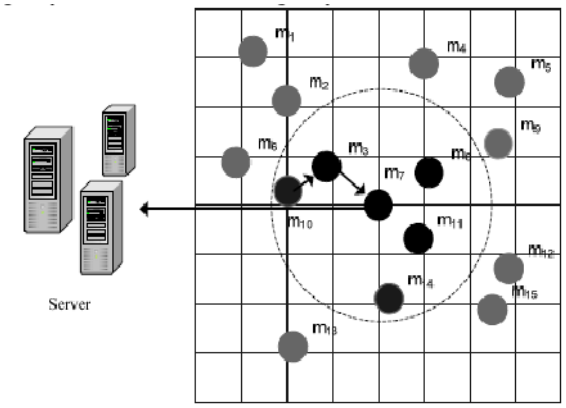


Fig 2.1: P2P Architecture

Firstly, it selects the central peer m_7 as its agent. And then the central peer discovers other 5 peers through one hop (m_3,m_8,m_{11}) searching or two hops searching (m_{14},m_{10}). After the group is created, the initiator will send a query to the agent and the agent forward this query to the server. As a result, the server receives a query from m_7 and the initiator is unknown from the server. Privacy preserved location detection system is proposed in [10]. This is helps to identify the device position in a secure manner without disclosing the privacy information of the user.

2.2 Cloaking Algorithms

Cloaking is a popular Search Engine Optimization technique to present answer set differently to search engine server for preserve users privacy and content secrecy. But spatial cloaking is different by making anonymous query set to hide privacy information of the requester. The P2P k-anonymity model [11] achieves the user's privacy profile effectively. It preserves the unlink ability between initiators ID and its exact location to LBS server. But it is not flawless. One of the problems is that the P2P k-anonymity algorithm builds on a strong inner trust and just considers the anonymity to server. But sometimes a collaborator may be in the group and capture the agent. Another problem is the variable network topology which brings a high disconnect rate and brings down the systems availability. Anonymous architecture is non-central and self organization architecture. In the architecture, all peers are anonymous peers. Anonymous peer is only capable to know from whom a query is received and determine to whom the query will be forwarded in one hop. But it has no knowledge of the initiator and the final receiver. In anonymous architecture, also need to achieve a spatial cloaking area that is larger than A_{min} as well as covers *k* indistinguishable anonymous peers.

The Algorithm 1 outlines the mobile aware algorithm [8] used for selecting peer in anonymous architecture consist of three phases: Peers Discovering, Mobile-aware selecting and Adjustment. In phase1, the initiator will broadcast a hello message to neighbors to discover new peers. Those new peers are stored in a set T. In Phase 2, calculate the disconnect probability of two moving peers, i.e., the ratio of transmission range to the distance between two peers and then the strongest connection peers are selected as next peer. If the discovered peers are not up to k, expand the peer set. In Phase 3, area covering all peers is computed and k value is checked. Phase 1 and Phase2 will be repeated until *k* peers and minimum area covering the peers are satisfied. The mobile-aware algorithm improves the system connectivity remarkably by considering the mobility and selecting a relatively stable peer as its next hop.

```
1:Function Mobile-Aware_Cloaking(k, A_min)
2: Initially, the number of discovered peers k' = 0
while k' < k-1 do
3:      Discovering new peers to a set T.
4:      k' = k' + T
5:      for all peers in T do
                Vi = function to calculate the disconnect
                probability
        end for
6:      if k' < k-1 then
                next = max(V1,V2)
        end if
end while
7: Expand covering area of discovered peer to A_min
```

Algorithm 1: Sample Cloaking Algorithm [5]

The analysis of various conventional and enhanced cloaking algorithms reveal drawback of the traditional cloaking techniques and the way they are rectified in enhanced algorithms. In the mobile-aware cloaking techniques the privacy and connectivity are getting improved. In the case of resource-aware cloaking, it aims to minimize the communication and computational cost, while the quality-aware algorithm aims to minimize the size of the cloaked areas in order to generate more accurate aggregate locations. In-device cloaking device will be advantageous in many situation; it aims to provide more safe cloaking with minimized communication cost. The dual-active approach uses the least anonymizing time and the best anonymization success rate at the expense of acceptable communication cost [11].

3. PROPOSED METHOD

Mobile Cloaking gives many advantages over in-device cloaking, such freeing of device memory and increasing of battery life by taking cloaking task to the cloud. In this scenario, the mobile user is sending raw request to the

cloud and cloud construct the cloaking region and a query set, this anonymous query set send to the untrustworthy LBS. Cloud will segregate the answer set from the LBS and send relevant answer to the requester. Here, the mobile user trusts on cloud to give his location information. Here is a very big risk of get cheat by cloud. This risk can be solved in a considerable level by constructing a small level of cloaking (thin cloaking) in device without affecting more of its resources and construct the small query set which hides users' exact location by blurring it by including some peers in his cloaking region. Then send this query set to the cloud. This will protect mobile users privacy concerns from untrustworthy LBS and even from cloud. Fig 3.1 illustrates the outline of the two level cloaking and Fig 3.2 shows Two Levels Cloak Regions.

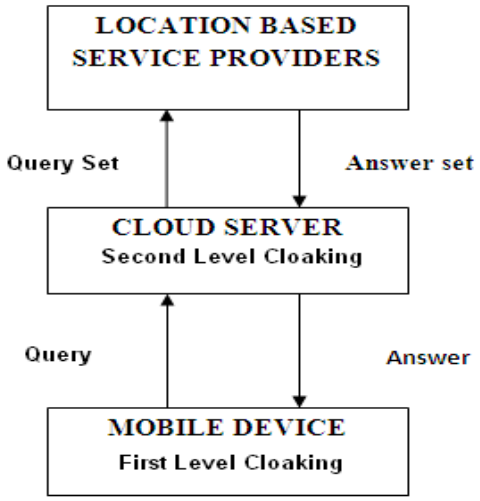


Fig 3.1: Outline of Two Level Cloaking

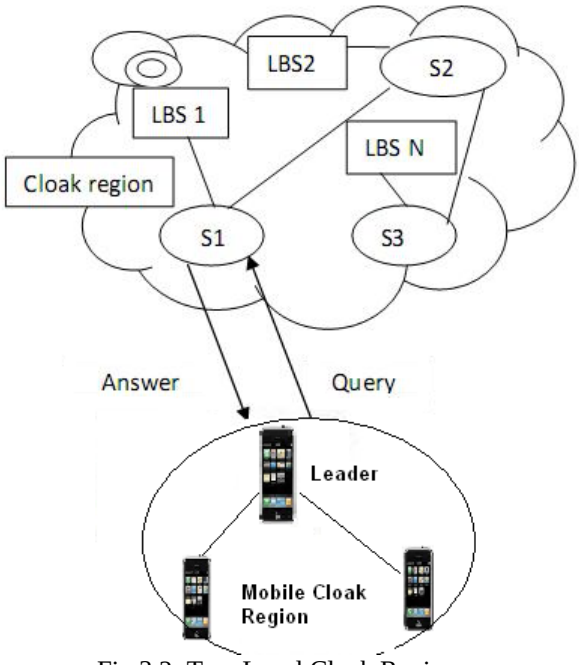


Fig 3.2: Two Level Cloak Regions.

3.1 Working Principle

Two level Cloaking is a combination of the in-device spatial cloaking [12] and cloud cloaking [5]. In-device cloaking can be a thin-cloaking which is resource-aware [10] cloaking and the cloud cloaking will be a thick-cloaking which is quality-aware cloaking [10]. The mobile device execute a cloaking algorithm which will resource-aware, that is the complexity of the cloaking result set is depending on the availability of the resources such as memory, CPU speed and battery back-up. In mobile cloaked region they identify a leader by executing the leader selection algorithm and this leader will construct the query set and send the same to the cloud. Cloud will identify the user's nearest LBS and transfer the request to the cloud server which is nearest to that LBS. That cloud server will prepare a cloak region and make a bigger query set which will forward to the LBS.

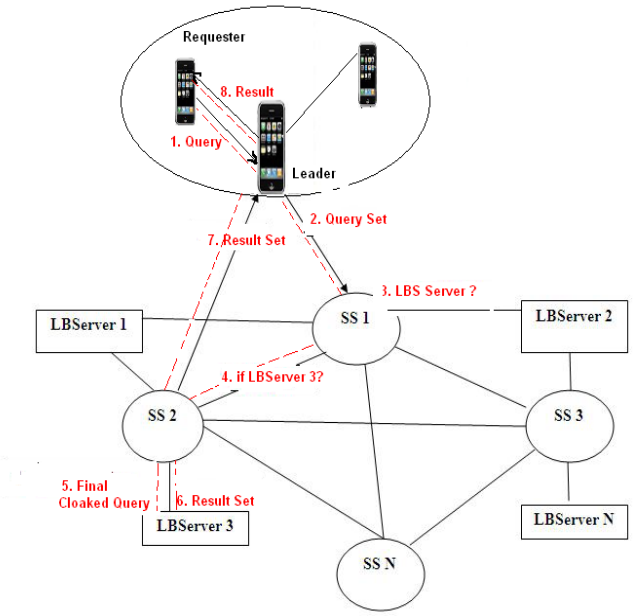


Fig 3.3: Two Level Cloaking Working Scenario.

The LBS (for example in Fig. 3.3, LBServer 3) executes this query set and prepare a answer set which send back to the cloud server. This server will segregate the answers with the users ID and forward to corresponding mobile leader. The leader will segregate this small answer set and direct relevant answer to the requester.

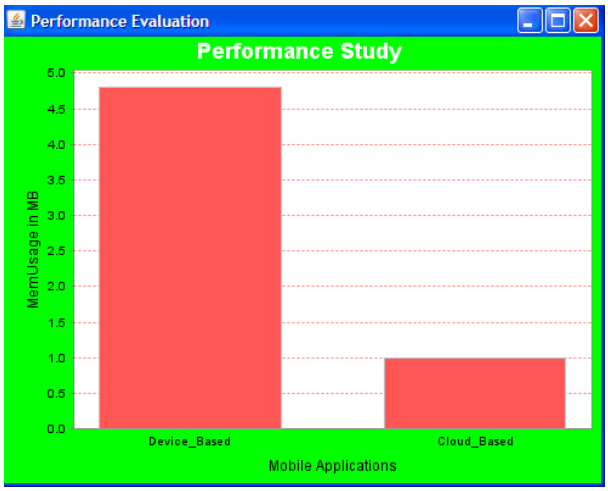
In this case of location based services the input to this system is range queries and the mobile should receive location based services.

4. RESULTS

4.1 Performance Improvement

Cloud is enriched with data centers which are having vey high processing power and plenty of storage. This will improve the performance of the mobile by executing the cloaking algorithm in a faster mode and keep all complex data structures in its data center. Even though cloud is taking care of major part of cloaking, mobile device is conducting a small level cloaking. So it will use some part of memory and its processing power. So the overall performance is better than the performance of the device-based cloaking and lesser than the cloud cloaking system

performance. Fig 4.1 shows the comparison between memory usage in cloud cloaking and device based cloaking.



4.1: Memory Usage

Fig 4.2: Battery Usage

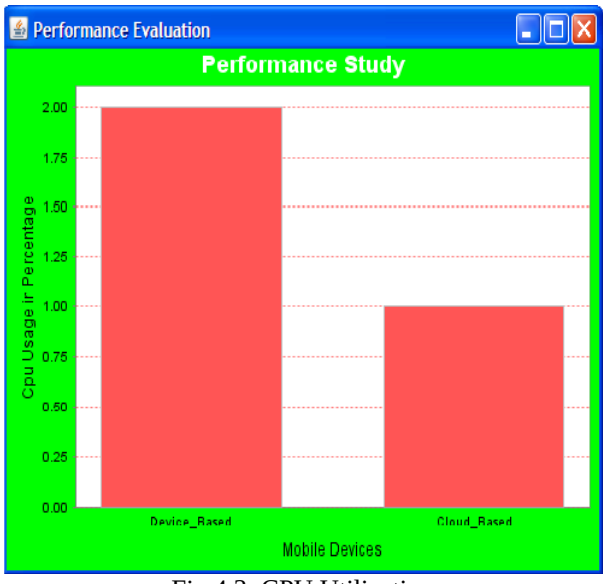


Fig 4.3: CPU Utilization

4.2 Battery Life Extension

The application performance management **(**APM) metric is used for measuring the amount of power consumed by a cloaking task. Initially interrogate the APM metric before the cloaking task at the device is initiated, interrogate it again after the cloaking completes, and report the difference. Alternately, we could completely charge a battery, repeatedly run the task until the battery dies, and divide 100% battery life by the number of Battery executions required to drain the battery. These experiments done in both the device based and cloud based cloaking techniques; it shows that up to 45% of energy consumption can be reduced for cloud based cloaking [5]. In case of two levels of cloaking battery charge consumption is a little more than the charge consumption in device based cloaking. It is experimentally figured as 27% lesser than the charge consumption in device based cloaking.

Fig 4.2 illustrates the battery usage analysis and Fig 4.3 gives analysis on CPU utilization.

4.3 Large Data Storage

The Mobile Cloud Computing is derived to have unlimited computing power and infinite storage capacity, these resources accessible through wireless devices by mobile phone. In the cloaking procedure all the live user density information and cloaking algorithm are stored on the cloud. So with cloud, the user can save considerable amount of storage space on the mobile device.

5. Conclusions And Future Work

Mobile world attracts the mobile users by introducing new features and new applications day by day. To accommodate resource sensitive applications mobile world get collaborated with cloud computing world. With this attempt will boost many dynamic location based applications and those using cloud effectively through mobile phone. User has to trust cloud servers to execute the cloak algorithms and access dynamic location based applications. This may lead to a risk of privacy breach by cloud servers. To avoid this the system can have a device based cloaking in addition to the cloud cloaking. This device level cloaking is considering less number of peers than the number of peers in k anonymity architecture to reduce the processing and storage burden in mobile device. With this multi level spatial cloaking the resources effectively using without compromising privacy preferences. It is necessary to analyze other methods of privacy preserving to improve the efficient use of mobile resources by avoiding device level cloaking.

Acknowledgments

My thanks to Jasmin T Jose who has contributed towards completion of this work. I am extend my gratitude to my colleagues in VIT University Vellore and friends in MES College of Engineeiring, Kuttippuram for their valuable guiding and sharing.

References

[1] Wei-Tek Tsai, Qihong Shao, Xin Sun, Jay Elston, “Real Time Service Oriented Cloud Computing”, in proceedings of the IEEE 6th World Conference on Services, 2010.

[2] H. Dinh, C. Lee, D.Niyato, and P. Wang," A survey of mobile cloud computing: architecture, applications, and approaches", Wiley Online.

[3] Chetan S, Gautham Kumar5, Dinesh, Mathew K, and Abhimanyu M.A., “Cloud Computing for Mobile World”, journal available at chetan.ueuo.com, 2010.

[4] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, “Authentication in the clouds: a framework and its application to mobile users," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop, ACM, 2010, pp. 1-6.

[5] Revathy Gangadaren and Lijo V P , “Privacy by Cloud Cloaking in Mobile Computing”, International Conference on Computer Science and Information Technology, 17th Feb, 2013, Coimbatore, ISBN:978-93-82208-62-4

[6] X. Lin., “Survey on cloud based mobile security and a new framework for improvement," in proceedings of IEEE International Conference on Information and Automation (ICIA), 2011, pp. 710-715.

[7] C.Y.Chow, M.Mokbel, andX. Liu, "Spatial cloaking for anonymous location-based services in mobile peer to peer environments", GeoInformatica, Springer,2011.

[8] J.Xu, Jin, M. Zheng, "Mobile-Aware Anonymous Peer Selecting Algorithm for Enhancing Privacy and Connectivity in Location-Based Service", in Proceedingsof the IEEE 7th Conference on e-Business Engineering, 2010.

[9] Lijo V P, Saidalavi Kalady “User-Centric Desighn for Privacy Preservation in Cloud Environment”, International Journal of Information Processing, 2012.

[10] C.Y.Chow, M.F. Mokbel, and T. He,"A privacy preserving location monitoring system for wireless sensor networks", IEEE Transactions on Mobile Computing, 2011.

[11] Y.Che, Q.Yang, and X.Hong, "A dual-active spatial cloaking algorithm for location privacy preserving in mobile peer-to-peer networks", in Proceedings of the IEEE on Wireless Communications, 2012.

[12] S.Wang, and X. Wang, "In-device spatial cloaking for mobile user privacy assisted by the cloud", in Proceedings of the 11th IEEE International Conference on Mobile Data Management (MDM), 2010.