# Comparative analysis of user location based anonymization of mobile computing

**M.K.Patil[1], M.N.Sonawane[2] and R.A.Mandlik[3]**

[1,2,3] Department of computer engineering, Loknete Gopinathji Munde Institude of Engineering Education and Research, Nashik, India.

**Email -** mamtap.1993@gmail.com

**Abstract:** In this paper we have discussed numerous of papers which are based on mobile computing we also have done comparative analysis of those paper with different parameter which include domain, application ,issue within them. Futher we also sugget next generation system in future scope for user location anonymization.

**Key Words:** Mobile computing, domain, GPS receiver, anonymize.

## Introduction:

As per the growth of mobile devices related with a GPS receiver, a large number of location based services (LBSs) have been launched. Since location information may private information, preserving location privacy has become a significant issue. Previously studied methods to preserve a users' privacy; physical constraints are not taken in consideration for most of them. In this paper, we constantly focus on such constraints and purpose of a location privacy preservation method which can be applicable to a real environment. In particular, our method anonymizes the user's location which generates dummies which we simulate to behave like an real human. The model also considers traceability of the user's locations which can quickly recover from an accidental reveal of the user's location. We are conducting an experiment using five users' real GPS trajectories and are compared our method relating to previous studies. The results shows that our method establish to anonymize the user's location within a pre-determined range. It also avoids fixing the relative positions of the user and dummies, it can also give a hint to an LBS provider which can identify the real users. In addition, we can conduct a user experiment with 22 participants to evaluate the power or heptiness of our method against humans. Weak participants to observe movements of a user and dummies and try to find the real user. As a result, we confirmed that our method can anonymize the users' locations even against human's observation.

Following are two requirements to arrange a system to preserve users' location privacy 1) it consider a closed system,i.e.,being executable on the user's mobile device in outside not to leak the user's location information and 2) it doesn't consider disturb benefits of the user and LBSs. The second requirement is important to have the entire ecosystem beneficial, otherwise, no users and LBSs would use the privacy preservation system. In results show that we proposed method can ensure that the user's location can be anonymous within the range of a required area size. It Also show that the proposed method avoids fixing connected positions of the user and dummies, which decreases a possibility to be inferred which location is the user's.

## Previous Work:

In [11] relational databases the k-anonimity concept was originally used. Initially M. Grusteser and D. Grunwald was used the idea of location k-anonimity, where k value was constant for all the users in system. M. Grusteser and D. Grunwald .was introduced the value of k .The mobile user was more protected by I-diversity and more protected from homogeneity attack. A. Machanavajjhala, J Gehrke, D. Kifer and M Venkitasubramaniam was introduced the concept of I- diversity. Our work is more different than client server and peer to peer approach. In [12] From more last few years, location privacy become more popular topic of research. In that we can the user location information and avoid the use to find the it favourite places. There are two general fields of privacy in LBSs(1)Identity privacy (2)Location privacy. The location is not protected by this technique but for user who reporting to it then the location become meaningless and this location is not associated with the single user. Location privacy means to share the information of user location ,in this the information is share depends upon the user decision.

In [13] LBS, the spatial cloaking techniques are widely used to protect the user location privacy. The spatial cloaking techniques depends upon the fully trusted third party (TTP),between user and the service provider the term location anonymizer. The anonymizer blur the user's exact location into a cloaked area when the user is subscribes to LBS .Mostly cloaked area include k-1 users because to satisfy the k-anonymity. some spatial techniques are applied to peer to peer environment. In [14] this the work is depends upon the two methods such

as local estimation method and leave-one-out method.. Which is used to shown the produce estimator and it is less conclusive than bootstrap approach. In this method the two parameters are used such as precision parameter and UNC parameter. Precision parameter is not used to compare the location techniques. In paper [15] Location confusion aided by query anonymization has been the common approach. To conserve location and problem of privacy. propose to identify responsive and non-responsive areas that all queries in the user's anonymity set have the same service aspect value, then query privacy will be neglect. In [16]A fake or dummy information can protect privacy and security in many different systems such as web search anonymous communications authentication systems and statistical analysis In all these scenarios, the main challenge and the still open problem is to generate text-dependent fake information that resembles real user-produced data and also provides an acceptable level of service while enhancing privacy of users. In location-based services, location confusion is a prevalent. There are few simple techniques proposed so long: adding independently selected locations drawn. In [17] There are mainly three application of proposals on providing location privacy in normal LBSs that do not specifically target common applications. First is geographical and temporal where in accurate location and time is sent to the server instead of the exact values. The foreknowledge here is that this prevents accurate identification of the locations of the users, or hides the user This approach, however, hurts the accuracy and timeliness of the responses from the server, In [18] the location is estimate by using three samples (k size) .It compromise between the accuracy estimation and the application performance .When the number is increase then it slightly reduces the distance error. Then can we compute the mean of three ensuring samples as the input for the network. However, the application can adjust the frequency for measurements that are taken, when uncertainty increases. Since every second the readings are taken, by using three samples. In [19] a policy-based approach is focused by location privacy. In telematics or telecommunication domain is specialized. The privacy preferences are specify by the policies used by the user . These policies store a location information sharing on which data can be collected and shared, when and for what purpose the data can be used, and how and to whom it can be distributed. The private location information is protected by LBSs for mobile users. The location *k*-anonymity based approach is another approach for location privacy. In [20] From last years, many location based services become more popular. One example is Guide system that provide the information of city by using tourist guide. In hospital the system is used to locate peers and devices tasks. The efforts we made for communication in hospital's staff.

## Comparative Study:

| Paper Parameter | Paper [1] | Paper [2] | Paper [3] | Paper [4] | Paper [5] | Paper [6] | Paper [7] | Paper [8] | Paper [9] | Paper [10] |
|---|---|---|---|---|---|---|---|---|---|---|
| **Domain Area** | Mobile Computing | Security | Mobile Computing | Cloud Computing | Mobile Computing | Mobile Computing | Networking | Big Data | Mobile Computing | Big Data |
| **Solution** | 1]novel suite of algorithm called mobipriv, 2]k-anonymity | Geographical queries without any privacy protection technique implemented. | User-Defined Privacy Grid System called dynamic grid system. | Nonparametric statistically procedure for diagonosis of the finger print model | DUMMY-Q adummy query generation scheme which takes into account the user motion. | Metrics that captured both geographic and semantic featured of real location trace. | 1]In datail to even defend against colluding, 2]mallicious proxies. | Users using RF signals and neural network can offer solution | To work as part of the perturbatin engine we experimentally study the behaviour of our clique clock algorithm | There are also active RFID tags with transmission distances of over 100 feet that use a battery to power the chip's circuitry and broadcast a signal to a reade |
| **Techniques** | Anonymization | PIR-Private Information Retrieval | TTP | Finger print/bootstrap resampling | Novel technique to protect the privacy of | Obfuscation | PIR | estimation | Perturbation technique | optimization |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | service attribute | | | | | |
| **Mapping** | Many to many | Based private information retrieval | many to many | nonlinear | | Between location | 1]Location to an encrypted index, 2]index to encrypted location | Many to many | One to one | Many to many |
| **Network** | wireless | Wireless | wireless | wireless | wireless | Social | Social | wireless | wireless | Wireless |
| **Database** | 1]location database, 2]mobile user database, 3]relational database | Geographic | Spatial database management | Rss measurement whose location are known | POI is the remote database | 1]CDRs database, 2]image database | Context of database | It use the row and column | Information is recorded in database tables | Drug information database |
| **Algorithm** | 1]Realistic-dummy-generation, 2]cloakLessk, 3]cloaked | MaPIR algorithm is ctiptographic of PIR. | 1]Symmetric encryption, 2]base line | Fingerprint algorithm | Pool_builder, greedy algorithm | 1]Clustering algorithm, 2]dynamic programming algorithm. | LBS | 1]Leven berg marquardt, 2]viterbi algorih m | 1]Clique clock algorithm, 2]quad tree based algorithm | 1]backpropogation algorithm, 2]neighbour algorithm |
| **Issues** | Corollary history attack | Privacy | In our system a user never transmit actual location information. | This is a non trivial issue because of the complexity of the radio propogation typical in the indoor scenario | LBS issue related to query privacy. | To generate context dependent fake information that resembles genuine user produced data | One subtle issue in processing nearest neighbor queries with this approach. | Location of Mobile device does not consider this issue | The message processing time maybecome a critical issue | Privacy |
| **Future scope** | To deploy Mobipriv system to be used as the middleware for transitGenie | MaPIR: Mapping-Based Private Information Retrieval base privacy protection technique. | QS trying to determine the position of user through IP location. | The spatial temporal correlation of the Rss indoor distribution. | The query adversary still cannot compromised the real services attribute value with probability exceeding a pre determin | Our synthetic traces also preserve useful feature of real traces and can be useful in 5 popular geo_data analysis task. | User efficiently transform all their locations shared with the server and encrypt all location data stored | One of the main benefits of this approach is the scalability,as well as its low cost | Telecommunication board on IT road map to geospatial future | improve the estimation by tracking the user over time rather than relying only on individual samples. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | ed threshold | | on the server. | | | |
| **Domain Area** | Mobile Computing | Security | Mobile Computing | Cloud Computing | Mobile Computing | Mobile Computing | Networking | Big Data | Mobile Computing | Big Data |

**Mobile system location privacy:"Mobipriv" a robust k anonymous system[1].**
et al author F . Liu, K. Hua, Y. Cai. Consider Current k-anonymous techniques that uses the AS concept will under-perform if k-l another users are not present at the time of request. These AS systems accept the user to define their own level of privacy by specifying the k in k-anonymity. Location based services (LBS) are applications that take the geographic location into consideration. LBS is increase by the rapid improvement of the mobile phone capabilities such as GPS and multimedia. for Example of location based services are Transit Genie, NextBus ,Google Latitude.

**MaPIR: Mapping-Based Private Information Retrieval for Location Privacy in LBISs[2].**

et al A. Perez, M. Labrador and P. Wightman consider provide users with information based on their geographical direction, which can be display from the mobile device they are moving and from which they are accepting the service, or using a manually defined location, Location-Based Information Systems in year 2011.At the same time, location privacy has become a most critical task for ensuring users' right to protection. protect the location information is not to secure it. In this paper introduces MaPIR, a mapping-based private information retrieve technique that uses mathematically generated mapping to create repetition in order to provide number of answers to a user with an undistinguishable location.

**User-Defined Privacy Grid System for Continuous Location-Based Services[3].**
B. Gedik and L. Liu can Protecting location privacy with personalized k-anonymity in 2008 developing number of user use location-based services (LBS) to resources information relevantly to their current locations from a different service providers. We tracking the requests of a person it is possible to build a evaluation profile which can protected information about a user's work.

**Nonparametric Model Comparison and Uncertainty Evaluation for Signal Strength Indoor Location[4].**
F. Gustafsson and F. Gunnarsson we consider Mobile positioning using wireless networks in July 2005in that it consists of evaluating the physical position of mobile terminals inside a network and the effective an potential service. This approach depends on finding functional dependence means interaction between the RSS ( received signal strength) and the position of the mobile device.
**Protection of Query Privacy for Continuous Location Based Services[5].**

F. Liu, K. Hua, and Y. Cai. describe the source of real-time information and guidance the potential fault of users sensitive secret data by an LBS server is elaborate into a serious task.. In this paper are computationally and communication wise useful, require storage of footprint, and do not upset the accuracy of LBS query result.
**Synthesizing Plausible Privacy-Preserving Location Traces[6].**

Camouflaging user's actual location with fakes is a frequent obfuscation application for protecting location privacy. We display the protection algorithm based on the ad-hoc techniques for generating fake locations are easily broken by assumption attacks.

**Preserving Location Privacy in Geo-Social Applications[7].**
In geo-social applications, such as FourSquare, millions of people interact with their environment through their people and their recommendations. The purpose of LocX (short for location to index mapping), a different approach to achieving user privacy while maintaining accuracy in location-based social applications.
**Reducing the Uncertainty on Location Estimation of Mobile Users to Support Hospital Work[8].**

The use of electronic patient records list and the acceptance of handheld computers are two of the most important direction transforming the use of computers in hospitals. Much of the research manipulation on determining the location of mobile devices does not consider this problem, and uses only the information received from sensors at a specific time in detail.
**Location Privacy in Mobile Systems: A Personalized Anonymization Model[9].**

We describes a personalized k-anonymity model for securing location privacy against different privacy threads through location information sharing. To reduce location privacy hazards is to promote k-anonymity protecting

maintenance of location information and develop coefficient and modular system-level facilities for protecting location privacy with location k-anonymity.

**Location-Aware Access to Hospital Information and Services[10].**
In this paper Hospital workers are high level mobile they are continuously changing location to perform their routine work, which includes staying patients, locating resources, such as medical records, or instructive with other specialists. Artifacts are used in hospitals to support the staff's allocation or as distributed achieve of information.

## Conclusion:

We conclude that the we have discuss the numerous paper issues and with grid formation we can change the position of grid then change all dummies position in particular position. We consider the reliability of locations on a road network in successive queries and also related positions of a user in a grid formation. Therefore, we suggest dummy based method is robust against assumption attacks based on geographical constraints, i.e. an attacker cannot distinguish a user from dummies using the geographical constraints take location acceptable into user account.

## Reference:


1. F . Liu, K. Hua, Y. Cai. Query I-Diveristy in Location Based Services. International Conference On Mobile Data Management,2009.
2. A Perez, M. Labrador and P. Wightman, Location-Based Information Systems. USA. CRC Computer and Information Science Series. CRC Press, 2011.
3. B Gedik and L. Liu, "Protecting location privacy with personalized k anonymity: Architecture and algorithms," IEEE TMC, 2008.
4. A Kushki and A. V. K.N. Plataniotis, "Kernel-based positioning in wireless local area networks," IEEE Trans. on Mobile Computing, June 2007.
5. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, Tan, and KianLee. Private queries in location based services: Anonymizers are not necessary. In SIGMOD, 2008.
6. G. Acs, C. Castelluccia, and R. Chen, "Differentially private histogram publishing through lossy compression," in Data Mining (ICDM), 2012 IEEE 12th International Conference on. IEEE, 2012.
7. M. Hendrickson, "The state of location-based social networking," 2008.
8. E. B. Moran, M. Tentori, V. M. Gonzalez, J. Favela, and A. I. MartinezGarcia, "Mobility in hospital work: Towards a pervasive computing hospital environment," 72–89, 2006.
9. Computer Science and Telecommunications Board. IT Roadmap to a Geospatial Future. The National Academics Press, November 2003.
10. M. Muñoz, M. Rodriguez, J. Favela, V. M. Gonzalez, and A. I. Martinez-Garcia, "Context-aware mobile communication in hospitals," IEEE Computer. , Sept. 2003.
11. B. Gedik, L. Lui ,Mobile Systems Location Privacy: "MobiPriv" A Robust K Anonymous System,2010.
12. P. M. Wightman, M. Zurbarán , MaPIR: Mapping-Based Private Information Retrieval for Location Privacy in LBISs.,2013.
13. Roman Schlegel, Chi-Yin Chow, Qiong Huang,User-Defined Privacy Grid System for Continuous Location-Based Services
14. Carlos Figuera, Inmaculada Mora-Jiménez, Alicia Guerrero-Curieses , Nonparametric Model Comparison and Uncertainty Evaluation for Signal Strength Indoor Location,2009.
15. Aniket Pingley∗, Nan Zhang∗, Xinwen Fu , Protection of Query Privacy for Continuous Location Based Services , 2011
16. E. Lui and R. Pass, Preserving Location Privacy in Geo-Social Applications , 2016.
17. *Krishna P. N. Puttaswamy∗, Shiyuan Wang, Troy Steinbauer,Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. Zhao*Preserving , Location Privacy in Geo-Social Applications , 2012.
18. Luis A. Castro and Jesus Favela , Reducing the Uncertainty on Location Estimation of Mobile Users to Support Hospital Work.,2008.
19. S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez , Location Privacy in Mobile Systems: A Personalized Anonymization Model , 2005.
20. Jesus Favela, Edgar A. Martínez, Location-Aware Access to Hospital Information and Services, 2004.