Chapter 3
Hybrid Cryptographic Based Approach for Privacy Preservation in Location-Based Services

Ajaysinh Rathod and Vivaksha Jariwala

3.1 Introduction

The information society is mainly founded on the information and communications technologies (ICTs). The members of the information society want to obtain the information as fast as possible, from everywhere and at any time [1]. Emergency services, LBS reminder, map navigation, location-based marketing, location-based search, and location-based advertisement are examples of location-based services. LBSs are available on a variety of mobile platforms like mobile devices, PDAs, GPS devices, and other devices because they are ubiquitous. Nowadays, the growth of LBS users is very fast. In location-based application, users provide their highly personalized information like their identification information and location information to the service provider causing vulnerability to their privacy, e.g., an attacker can also get the current location of the user and also track user's daily activities. Due to the tracking capability, it opens many possibilities of computer based crimes like kidnapping, harassment, car theft, and many more. Varieties of attacks are already possible, so there is a big challenge to protect location privacy with minimum cost.

A. Rathod (✉)
Department of Computer Engineering, RDIC, C. U. Shah University, Wadhwan, Gujarat, India

V. Jariwala
Department of Information Technology, Sarvajanik College of Engineering and Technology, Surat, Gujarat, India

I. Woungang, S. K. Dhurandher (eds.), *2nd International Conference on Wireless Intelligent and Distributed Environment for Communication*, Lecture Notes on Data Engineering and Communications Technologies 27,
https://doi.org/10.1007/978-3-030-11437-4_3

3.2 Literature Survey

In this section, we analyze popular category of crypto-based privacy model for location-based service that has been proposed by different authors.

3.2.1 Categorization of Crypto-Based Privacy Model for LBS

In the simple form of communication between an LBS user and LBS provider, the former sends a simple query (Q) containing an ID and his location (L) and a request for information (I) that he wants to retrieve from provider P [2]. A user provides his identity and location to provider, but provider is not always trust worthy.

Most schemas within this category adopt a centralized model for privacy [3]. There are many solutions that are already proposed by using TTP based schemas [4–19]. TTP based schemas are used very often and easy to deploy. This schema has many drawbacks so do not rely on TTP [1]. Many schemas are already proposed as TTP free schemas [20–24].

3.2.1.1 TTP Free Schema

Without the help of trusted third party, all users jointly compute the task which will improve the privacy of the users.

Collaborative-Based Schema

It is a fully distributed schema. The trust is scattered among the nodes that form an ad-hoc network. All peers work collaboratively as shown in Fig. 3.1 to achieve privacy among untrusted entities. Various algorithms are already proposed by Solanas et al. [7–9]. The advantage of this approach is that it does not rely on TTP, it is distributed and also guarantees us privacy, but it has issues with cost and scalability.

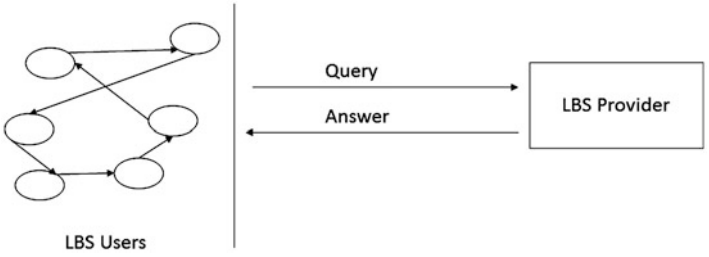

Fig. 3.1 The communication schema of collaborative method between users and LBS provider [3]

3.3 Motivation of Proposed Approach

Many schemas have been already proposed by different authors but they pose and open challenges that need to be solved, such as reducing communication cost, reducing computational cost, and poor scalability. Our aim is to propose a novel solution that provides location privacy to the LBS users. The main goal of the research is to achieve features such as TTP free, hybrid approach (centralized and decentralized), improve scalability, reduce cost in resource constraint devices, collision free, and enhance privacy.

Figure 3.2 represents the system architecture of proposed schema. It contains two main components: (1) LBS users and (2) LBS provider. Each user has their private information on their mobile like UserID U_{id} and location information (Lg_i, Lt_i). There is a need of preserving the privacy of LBS users. As our first step, we are finding the number of Users U_i in cloaking region who are requesting for location-based information. Next, we generate random region [25] R_i based on the clustering algorithms for users in spatial cloaking region. This procedure creates different cluster as shown in Fig. 3.2. All users will add some random value in their original location information because any malicious user can collude with location-based service provider. To avoid this attack, each user will add random value in their actual location by using secrete share function and perform a secure data aggregation using privacy homomorphism *PH* [10] in each random region R_i which uses centralized approach that is shown in Fig. 3.2 with blue edges. Next, we use the decentralized approach to perform random chaining *RC* for all distributed random region R_i to compute the secure centroid *C* as shown in Fig. 3.2 with green edges. The last user, *U*, sends the encrypted sum of location *C* to LBS provider *P* as shown in Fig. 3.2 with red edge. LBS provider will decrypt this sum of location by his own private key.

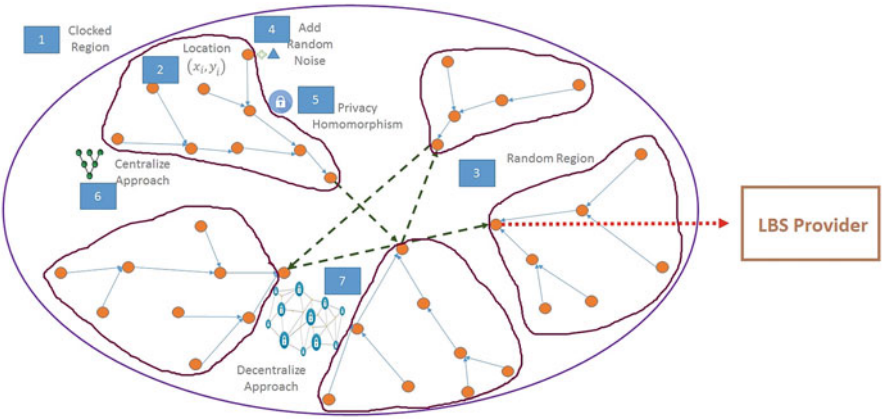

Fig. 3.2 Proposed communication schema of hybrid approach between users and LBS provider

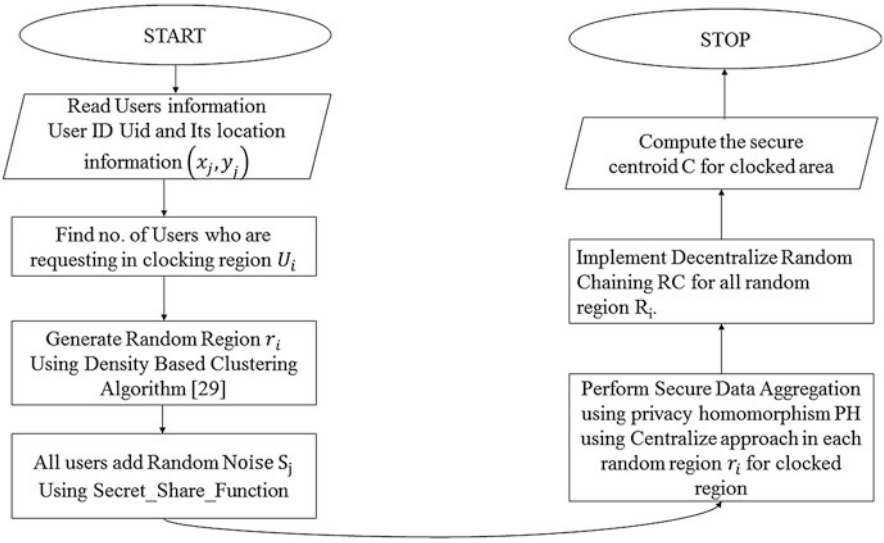

Fig. 3.3 Flowchart for proposed protocol schema

Algorithm 1 Users Communicate Using Proposed Model

Input: LBS Users U_i (User Identification U_{id}, Position information (Lg_i, Lt_i)).
Output: Compute Secure Centroid C.
1: Find LBS requesting Users in cloaking region U_i.
2: Create Region R_i using Clustering Algorithms in spatial cloaking region.
3: All users add random noise in their current location using Secret Share function.
4: Perform Secure Data Aggregation using privacy homomorphism [27, 28] PH using Centralized approach in each random region R_i for cloaked area.
5: Perform Decentralized Random Chaining RC for all random region R_i and compute the secure centroid C for cloaked area.
6: The Last User, U send encrypted sum C centroid to LBS provider P.
7: LBS Provider P perform decryption using his own private key and Find Centroid.

The main aim is to hide the user's location within the other users and also give inaccurate location information to the LBS provider. We use hybrid approach that includes distributed method to achieve minimum cost and improve scalability. In this paper, we propose a protocol schema that preserves privacy between users and LBS provider [26]. Proposed protocol schema is shown in Fig. 3.3.

3.4 Experimental Results and Evaluation

We have developed the simulation scenario and implemented the same in Java. We evaluated it on an Intel Core i3 2.30 GHz machine with 2 GB of RAM running Windows 7 OS. We experimented the performance with different density based clustering algorithm and different dataset of users. Performance metrics is measured in average computation time taken by the processes.

3.4.1 Datasets

In our simulation, we use dataset of Weeplaces,[1] which contain check-in activity of the users in location-based social network. It is also integrated with the API of other location-based social network (LSBN) like Facebook place (see footnote 1), Gowalla,[2] etc. Users have to login in location-based social network and they can connect with the other friends in this network, those who have already registered in this application. This dataset contains 7,658,368 check-ins generated by 15,799 users over 971,309 locations [2]. We use this dataset because users can connect with Weeplaces datasets and connect with their friends. They can also perform location-based search.

3.4.2 Density Based Clustering Algorithms

It is the process of making the groups of points together, which are close for the given dataset/set of points in space. This is called as density based clustering. Examples of density based clustering [29–31] are DBSCAN, OPTICS, etc. We use density based clustering algorithm DBSCAN and Optics to create random region in cloaked area.

3.4.3 Results

We have analyzed the performance of our model for various parameters like execution time and number of clusters based on various users as shown in Figs. 3.4 and 3.5 and Table 3.1. OPTICS algorithm gives better results as compared to DBSCAN clustering algorithm.

[1] http://www.yongliu.org/datasets/.

[2] http://techcrunch.com/2011/12/02/report-facebook-has-acquiredgowalla/.

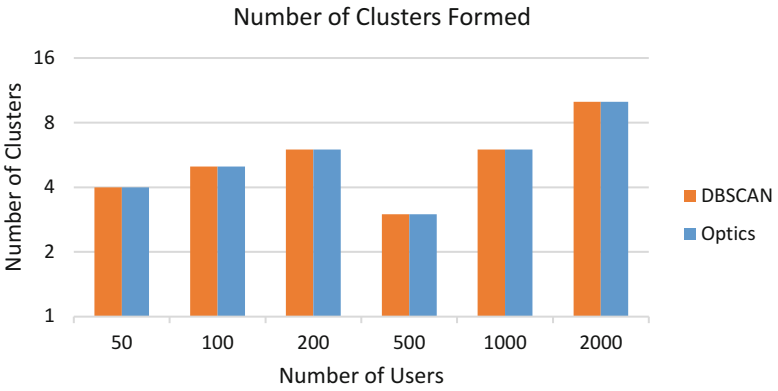

Fig. 3.4 Total execution time over number of users for Weeplaces dataset

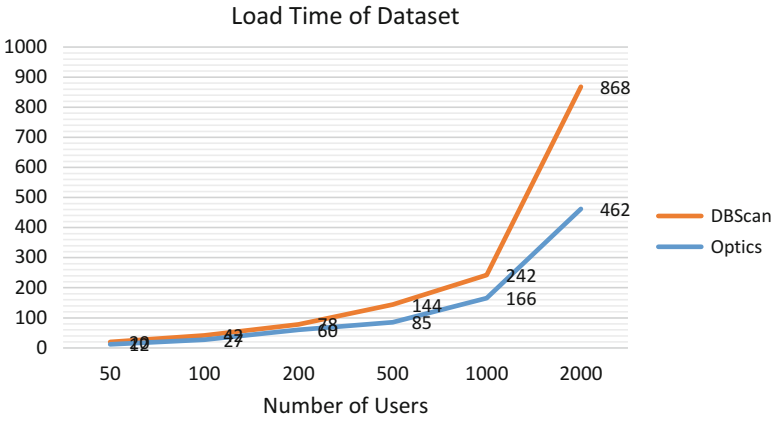

Fig. 3.5 Number of clusters over number of users for Weeplaces dataset

Table 3.1 Result of various parameters of Weeplaces dataset

No.	Number of users	Clustering algorithms	Total time (ms)	Number of clusters
1	50	DBSCAN	20	4
2	100		42	5
3	200		78	6
4	500		144	3
5	1000		242	6
6	2000		868	10
7	50	OPTICS	12	4
8	100		27	5
9	200		60	6
10	500		85	3
11	1000		166	6
12	2000		462	10

3.5 Conclusion

In location-based services, users will get some important information based on their location by providing their highly personalized data like user's identity, user's location information, etc. Privacy preservation is of paramount importance with the rapid growth of LBS users. In this paper, we address the benefits and issues of both TTP based and TTP free schema. In our proposed approach we select hybrid tech-nique to take advantage of centralized and centralized schema. This schema gives the guarantee of privacy of the users with improves scalability and reduces the cost. We have created random region from the given set of input dataset by using basic density based clustering algorithms—DBSCAN and OPTICS clustering algorithms. We have analyzed the performance of our model for various parameters like execution time and number of clusters based on various users. OPTICS algorithm gives 60% better result compared to DBSCAN. In future, we will perform homomorphic encryption, construct tree topology, and distributed random chaining approach as per our proposed schema.

References

1. R. Padmanaban, Location privacy in location based services: unsolved problem and challenge. Int. J. Adv. Remote Sens. GIS **2**(1), 398–404 (2013)
2. Y. Liu, W. Wei, A. Sun, C. Miao, Exploiting geographical neighborhood characteristics for location recommendation, in *Proceedings of the 23rd ACM International Conference on Information and Knowledge Management (CIKM'14)* (ACM, 2014), pp. 739–748
3. E. Magkos, Cryptographic approaches for privacy preservation in location-based services: a survey. Int. J. Inf. Technol. Syst. Approach **4**(2), 48–69 (2011)
4. M. Wernke, P. Skvortsov, F. Durr, K. Rothermel, A classification of location privacy attacks and approaches. Pers. Ubiquit. Comput. **18**(1), 163–175 (2014)
5. Y. Wang, F. Li, B. Xu, L2P2: Location-aware location privacy protection for location-based services, in *Proceedings - IEEE INFOCOM,* 2012, pp. 1996–2004
6. G. Yang, J. Li, S. Zhang, H. Zhou, A survey of location-based privacy preserving. J. Convergence Inf. Technol. **8**(11), 27–33 (2013)
7. A. Solanas, J. Domingo-Ferrer, A. Martinez-Ballest, Location privacy in location-based services: beyond TTP-based schemes, in *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications*, October 2008
8. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, K.-L. Tan, Private queries in location based services: anonymizers are not necessary, in *ACM SIGMOD International Conference on Management of Data*, 2008, pp. 121–132. ISBN: 978-1-60558-102-6
9. G. Ghinita, P. Kalnis, M. Kantarcioglu, E. Bertino, A hybrid technique for private location-based queries with database protection, in *Advances in Spatial and Temporal Databases Volume 5644 of the Series Lecture Notes in Computer Science* (Springer, Berlin, 2009), pp. 98–116. ISBN: 978-3-642-02982-0
10. A. Solanas, A. Martinez-Balleste, Privacy protection in location-based services through a public-key privacy homomorphism, in *Proceedings of the 4th European Conference on Public Key Infrastructure: Theory and Practice* (Springer, 2007). ISBN: 3-540-73407-4 978-3-540-73407-9

11. Y. Huang, R. Vishwanathan, Privacy preserving group nearest neighbor queries in location-based services using cryptographic techniques, in *IEEE Global Telecommunications Conference GLOBECOM*, 2010
12. R. Gupta, U.P. Rao, An exploration to location based service and its privacy preserving techniques: a survey. J. Wireless Pers. Commun. **96**(2), 1973–2007 (2017)
13. B. Amro, Y. Saygin, A. Levi, Enhancing privacy in collaborative traffic-monitoring systems using autonomous location update. IET Intell. Transp. Syst. **7**(4), 388–395 (2013)
14. M. Ashouri-Talouki, A. Baraani-Dastjerdi, Homomorphic encryption to preserve location privacy. Int. J. Secur. Appl. **6**(4), 183–189 (2012)
15. A.K. Tyagi, D.N. Sreenath, Preserving location privacy in location based services against Sybil attacks. Int. J. Secur. Appl. **9**(12), 175–196 (2015)
16. S. Patil, S. Ramayane, M. Jadhav, P. Pachorkar, Hiding user privacy in location base services through mobile collaboration: a review, in *International Conference on Computational Intelligence and Communication Networks IEEE*, 2015
17. T. Peng, Q. Liu, G. Wang, Enhanced location privacy preserving scheme in location-based services. IEEE Syst. J. **11**(99), 1–12 (2014)
18. R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, J.-P. Hubaux, Hiding in the mobile crowd: location privacy through collaboration, in *IEEE Transactions on Dependable and Secure Computing, Special Issue on "Security and Privacy in Mobile Platforms"*, 2014
19. A.K. Tyagi, N. Sreenath, Future challenging issues in location based services. Int. J. Comput. Appl. **114**(5), 51–56 (2015)
20. N. Yang, Y. Cao, Q. Liu, J. Zheng, A novel personalized TTP-free location privacy preserving method. Int. J. Secur. Appl. **8**(2), 388 (2014)
21. A. Solanas, A. Martinez-Balleste, A TTP-free protocol for location privacy in location-based services. Trans. Comput. Commun. **31**(6), 1181–1191 (2008)
22. C. Bettini, X. Sean Wang, S. Jajodia, Protecting privacy against location-based personal identification, in *Workshop on Secure Data Management SDM 2005: Secure Data Management*, 2006, pp. 185–199
23. G. Yang, J. Li, S. Zhang, H. Zhou, A survey of location-based privacy preserving. J. Convergence Inf. Technol. **8**(11), 27 (2013)
24. M. Wernke, P. Skvortsov, F. Durr, K. Rothermel, A classification of location privacy attacks and approaches. Pers. Ubiquit. Comput. **18**(1), 163–175 (2014)
25. S.R. Shastry, P.K. Deshmukh, A.B. Bagwan, Generating: random regions in Spatial cloaking algorithm for location privacy preservation. IOSR J. Comput. Eng. **9**(4), 46–49 (2013)
26. A. Rathod, V. Jariwala, Investigation of privacy issues in location-based services, in *Recent Findings in Intelligent Computing Techniques. Advances in Intelligent Systems and Computing*, vol. 707 (Springer, Singapore, 2018), pp. 55–65
27. V. Jariwala, D. Jinwala, Evaluating homomorphic encryption algorithms for privacy in wireless sensor network. Int. J. Adv. Comput. Technol. **3**(6), 1–11 (2011)
28. X. Zhu, Y. Lu, X. Zhu, S. Qiu, A location privacy-preserving protocol based on homomorphic encryption and key agreement, in *International Conference on Information Science and Cloud Computing Companion IEEE*, 2014
29. R.J. Patil, K.K. Joshi, S. Raksha, Analysis on preserving location privacy. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **5**(3), 562–566 (2015)
30. J. Liu, J. Luo, J.Z. Huang, X. Li, *Privacy Preserving Distributed DBSCAN Clustering* (ACM, Berlin, 2012)
31. P. Batra Nagpal, P. Ahlawat Mann, Comparative study of density based clustering algorithms. Int. J. Comput. Appl. **27**(11), 421–435 (2011)