International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Centralized TTP Free Privacy Approach for Location Based Services for Social Media

Ajaysinh Rathod*1, Vivaksha Jariwala2

Submitted: 10/09/2022 **Accepted:** 20/12/2022

Abstract: Location based service is one of the most promising fields in the information & communication society. The use of ubiquitous devices increases because they are enabled with various location based system, i.e. mobile phone, GPS enabled devices, Laptops, PDAs, etc. Moreover, LBS users use their location information to get important information from the service providers. i.e. location based search, emergency service, location based social networking, friend finding services, etc. Due to the advancement in technology the usage of LBS become more demanding because of its several advantages. So growth of LBS users increases more. Users need to provide his/her identity, location information to the service provider that is highly personalized information. Location information directly related to the privacy of the LBS users. Location privacy is a critical issue that needs to be solved. Collaborative TTP free model is the best model where users work together for location privacy in LBS. Location based Social Media is currently one of the fastest growing networks where growth of the LBS users increase rapidly. Many approaches are already proposed by various authors that provide location privacy. But none of them provide location privacy of the users that support growth of the network with the least cost. In this paper, the attempt is to propose a complete solution that provides location privacy with the least cost and improved scalability using a centralized approach.

Keywords: *Location-Based Services, Location Privacy, TTP Free, Privacy Homomorphism*

1. Introduction

1.1. Information and communication technologies are playing a vital role in computer and information society. Due to innovation and rapid growth, location enables devices are becoming very popular nowadays. Location Based Services (LBSs) are gaining popularity because of advances in mobile network & positioning systems. These devices are ubiquitous & use location information systems so the user can get highly personalized information at any time. E.g. location based tourist information, location based search, location based social networking, etc. Users will send a query to the service provider to get their desired information based on their location information. i.e. “Show me the list of hotels nearby me”, also perform social networking based queries to take help. i.e. “Suggest best Italian pizza based restaurant nearby me”. With the query, the user needs to send some personalized or sensitive information under some situations. i.e. personal identification, location information, etc. they don’t want to disclose such kind of information to the service provider. Any malicious or adversary may obtain highly personalized information of the user. Location privacy is one of the most critical issues in location based services. User’s location information can be determined by the attacker and based on that they may infer many things. E.g. trace the user, infer the habit of users, daily routine, etc. due to the tracking capabilities, it opens many possibilities. All users to access location based on the services without compromising their location privacy.

[1] *Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India.*
ORCID ID : 0000-0003-1656-943X
[2] *Sarvajanik College of Engg. and Technology, Surat, Gujarat, India*
ORCID ID : 0000-0003-3332-2033
** Corresponding Author Email: ajay58886@gmail.com*

2. APPLICATIONS: LOCATION BASED SOCIAL MEDIA

Users are very active on social media on internet and using variety of applications that are available on that platform. i.e. Facebook, Twitter, Myspace, whrrl etc. User finds new way to communicate and keep in touch with their friends, family members and others. Initially people are connected on social media and then they start sharing their location information on social media by using their GPS enabled ubiquitous devices.

i.e. ‘Check in’ activity means sharing your important location information to others or large groups of people that are connected with each other through social media.

Geo social networking allow users to connect & communicate with each other and also attract the people by proving new services, their recommendation information based on their location, plan their events. i.e. Food sourcing, Location-planning, mood sourcing, adhoc networking, social shopping, etc.

3. Theoretical Background

The section contains the description of location based services, the information flow models that are widely used, various security and others parameters and types of cryptographic model for privacy in LBS that has been proposed by various authors.

3.1. Types of Cryptographic Based model for Privacy in LBS

In this section, discussion is done regarding various approaches for location privacy that are proposed by the various authors. It has been analyzed information flow model, study of various parameters requires for the LBS, types of cryptographic model for privacy in LBS.

3.1.1. Location Privacy

LBS user's location information should not be revealed to the unauthorized users/ attacker. Location privacy is the most critical issues nowadays. Users' needs some techniques that provide the highest location privacy with some features.

3.1.2. TTP Free Schema

Users will compute some tasks without taking the help of third party/ others. TTP cannot always trustworthy so he/she can infer the user's location by applying some technique.

3.1.3. Collaborative-Based Schema

This privacy schema does not rely on an intermediate entity of a trusted third party. Collaborative schema is totally distributed or collaborative where the trust will be scattered among all nodes in a given ad-hoc network & they perform together to complete their task with the strongest privacy.

Location privacy is one of the central points of contention that should be unraveled. There are different diagrams proposed by various authors [1, 6, 7, 8, 9, 10, 11, 13, 14, 22-24]. Collaborative TTP Free model [1-6, 9-11] is probably the best strategy for the strongest location privacy. Though schemas [1-6, 9-11] have the advantages, there are as yet open issues that require consideration. Hence, there is a need for a methodology that gives lower communication and computation cost, improves scalability along with privacy that is not proposed until now. Consequently, in this area, a novel methodology is proposed for privacy preserving LBS schema that is TTP free, support scalability, lower execution cost, and furthermore improves privacy.

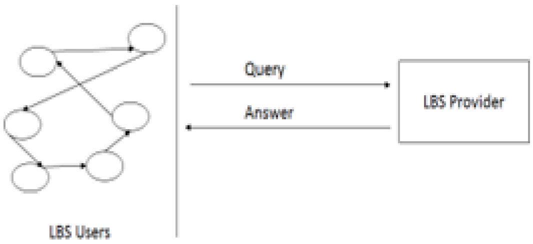

Fig.1. Communication schema of collaborative method [3]

4. Problem Statement & Proposed Approach

There are many open challenges that need to be solved, such as execution cost, data transmission cost, issues with increasing size of the network, etc. There is a need of effective approach that gives promise of the privacy of LBS users with improve scalability with minimum cost. It's a challenge to design computationally efficient and practical solution that provides strong privacy by reducing the processing overhead with improved scalability [20]. Proposed approach uses centralized approach for location privacy of the users.

The proposed approach has following advantages:

1. Improved Scalability - Easy to increase the size of the network.
2. Reduced Cost- It provides low communication cost and computational cost. It will reduce the number of data aggregation operation.

Proposed system architecture is represented in Fig 2. It contains two essential parts, for example a) LBS Clients and b) Location based service provider. Every client sends their private data to a LBS provider like his/her identity Uid & location (x_i,y_i).

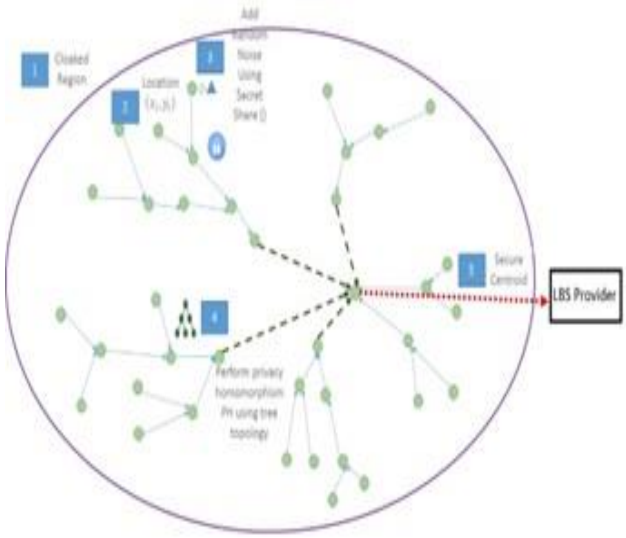

Fig 2. Proposed schema between LBS Users, and LBS provider

In the technique, the primary perception is to find out the range of Users Ui inside the cloaking place who're soliciting for location-based information. Then all users will add noises by using the random secret share function. One of the users will be elected as Secure Aggregator (SA). After this, users will perform secure data aggregation using privacy homomorphism PH [5, 16, 17, 18, 19] in region R using tree topology that is shown in Fig. 2. All users will send their secure sum to the Secure Aggregator SA. Then, last Secure Aggregator SA will compute the encrypted secure sum SS. Then, Secure Aggregator SA, sends the results to the LBS service provider P as shown.

The main aim is to hide the exact location information of the user from the other users and also give imprecise location information to the LBS provider. The approach is based on centralize approach that provides minimum cost, parallel execution, and support scalability.

Proposed Algorithm:

Algorithm 1 - Proposed Algorithm for Secure Sum in PPLBS using Secret Sharing, Paillier Homomorphic Encryption Schema

1. *Input: LBS Users NU_k (User ID U_{id}, Location Information (x_i,y_i))*
2. *Output: Secure Sum SS*
3. *Any LBS user takes initiative and fined their companion in their cloaked region R*
4. *Let p=0, i=0, NU, k=0*

5. *$NU(k)$ where k number of users in cloaked region R*
6. *Select any user works as Secure Aggregator $SA \in NU(k)$*

7. ***//Phase-1 Random Secrete Sharing***
8. *Each user will add some random secrete share in their original location*
9. *Secure Aggregator SA call random secrete sharing function*
10. *Call Random_Secret_Share_Function;*
11. *Each user has added some noise in their original location information*

12. ***//Phase-2 Homomorphic Encryption using Paillier Homomorphic Encryption [19] Schema***
13. ***foreach** user NU_i**do***
14. *Each user $NU(k)$ make use of public key infrastructure and request to public key authority PKA for Public Key of LBS provider LBS_p;*
15. *Public key authority PKA will provide valid public key Pk of LBS provider LBS_p;*
16. *Each user $NU(k)$ will encrypt his/her noisy location information (x_r, y_r) using Paillier- Homomorphic Encryption Algorithm [20] $(Epk\ (x_p), Epk\ (y_p))$ where x_p, y_p is the encrypted noisy location information of user NU*
17. ***end***

18. ***//Phase-3 Compute Secure Sum of Location using Centralized Approach in Cloaked Region R***
19. *Secure Aggregator SA is construct the tree topology in cloaked region R*
20. ***foreach** user $U_p$do*
21. *Every child nodes will send their encrypted location to their parent node using tree topology;*
22. *Perform secure data aggregation using Centralized approach in cloaked region R $(Epk(\sum_{p=1}^{n}(x_p)), Epk(\sum_{p=1}^{n}(y_p)))$;*
23. *Last, Secure Aggregator SA will receive the secure centroid*
24. *$ESC = (Epk(\sum_{i=1}^{k}(x_i)), Epk(\sum_{i=1}^{k}(y_i)))$;*
25. ***end***

26. ***//Phase 4 Secure Aggregator SA will send this encrypted secure sum to the LBS provider LBS_p and find the Secure Sum of location in that cloaked region R***
27. *Secure Aggregator SA will send a message (ESC, K) to LBS Provider LBS_p.*
28. *LBS provider LBS_p will decrypt the value by using his/her Private Key PR_k and find $\sum_{i=1}^{k}(x_i), \sum_{i=1}^{k}(y_i)$*
29. *LBS provider LBS_p will find secure sum SS by using $x_{ss} = \frac{\sum_{i=1}^{k}(x_i)}{k}, y_{ss} = \frac{\sum_{i=1}^{k}(y_i)}{k}$*

Function: Random Secret Share

---

1. *Secure Aggregator SA generate the random share as per number of users RS_x and RS_y such that, $(\sum_{m=1}^{NU}(RS_{m,x}) = 0), \sum_{m=1}^{NU}(RS_{m,y}) = 0))$*
2. *Secure Aggregator SA distribute the share randomly to all the users LBS User NU*
3. ***foreach** user $\in NU(k)$ do*
4. ***for** i=0;i<kl ;i++do*
5. *$(x_r, y_r) = ((x_i + RS_{i,x}), (y_i + RS_{i,y}))$;*
6. ***end***
7. *return (x_r, y_r);*
8. *End*

---

5. Implementation Methodology

In this section, discussion is done regarding experimental setup, datasets and various parameters for the evaluation. Simulation scenario was implemented in Java. In order to this, experimental evaluation with average computation time taken by the processes was performed with the proposed approach with different dataset of users.

5.1. Dataset

Some benchmark datasets i.e. Gowalla datasets [23], Weeplace dataset [22] have been used in the simulation. Weeplace [22] is integrated with the API of other location-based social network (LSBN) like Facebook place1, Gowalla, etc. Gowalla dataset [21] is based on a popular location based social network. Various dataset of mobile users was generated.

5.2. Performance Results and Analysis

Various parameters as i.e. scalability, communication cost, computation cost were considered for evaluation purpose for the proposed approach in location based services. Moreover to that experimental evaluation of the approach, with, total time is taken to execute all steps, total execution time of the approach are calculated.

Table 1. Time Complexity Comparison of Approach of All Dataset

No of Users	*Datasets*	*Proposed Approach –Total Time (ms)*
50	Gowalla	107
100		149
200		321
500		618
1000		1101
2000		1923
50	Weeplaces	88
100		149
200		189
500		436
1000		827
2000		1782

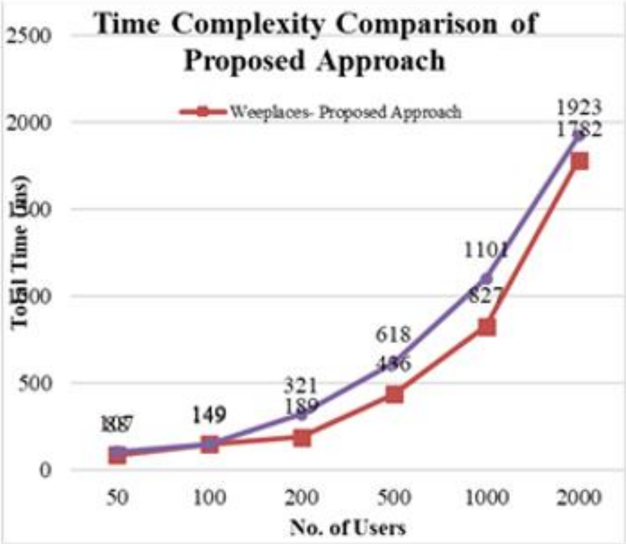

Fig. 3. Time Complexity Comparison of Proposed Approach of All Dataset

Fig. 3 shows time complexity comparison of proposed approach for various data sets.

6. Conclusion

Location privacy is absolutely critical to the quick development of LBS users. The collaborative TTP free model is one of the promising methodologies in LBS but that also contains open research issues. Hence the proposed approach provides location privacy of the user with minimum cost and improves scalability. Proposed approach uses centralized approach and homomorphic encryption. All the steps were performed on benchmark datasets. It is observed from the analysis and results that the approach gives better results in term of execution cost, support scalability and also preserve location privacy users.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Emmanouil Magkos,"Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey", International Journal of Information Technologies and Systems Approach (IJITSA), IGI Global, vol. 4(2), pages 48-69, 2011.

[2] AgustiSolanas, Josep Domingo-Ferrer, and AntoniMart´ınez-Ballest, "Location Privacy in Location-Based Services: Beyond TTP-based Schemes", projects TSI2007-65406-C03-01"E-AEGIS", 2010.

[3] AgustiSolanas, AntoniMartı´nez-Balleste,"A TTP-free protocol for location privacy in location-based services", Elsevier Transactions on Computer Communications, 2008.

[4] 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 (Springer), ISBN" 3-540-73407-4 978-3-540-73407-9, 2007.

[5] Vivksha Jariwala, Devesh Jinwala, 'Evaluating Homomorphic Encryption Algorithms for Privacy in Wireless Sensor Network', International Journal of Advancements in computing Technology, Volume 3, Number 6, 2011.

[6] Marius Wernke, Pavel Skvortsov ,FrankD¨urr, Kurt Rothermel, "A Classification of Location Privacy Attacks and Approaches, Personal and Ubiquitous Computing, Springer-Verlag, 2013.

[7] Rajchandar Padmanaban,"Location Privacy in Location Based Services" Unsolved Problem and Challenge", International Journal of Advanced Remote Sensing and GIS, Volume 2, Issue 1, pp. 398-404 , 2013.

[8] Nianhua Yang, Yuru Cao, Qing Liu and Jiming Zheng, "A Novel Personalized TTP-free Location Privacy Preserving Method", International Journal of Security and Its Applications Vol.8, No.2, 2014.

[9] Gaoming Yang, Jingzhao Li, Shunxiang Zhang, Huaping Zhou, 'A Survey of Location-Based Privacy Preserving', JCIT, 2013.

[10] Amit Kumar Tyagi, N.Sreenath, 'Future Challenging Issues in Location based Services', International Journal of Computer Applications (0975 – 8887) Volume 114 – No. 5, 2015.

[11] Xiaoling Zhu*, Yang Lu, Xiaojuan Zhu, ShuweiQiu, 'A Location Privacy-Preserving Protocol Based on Homomorphic Encryption and Key Agreemen', International Conference on Information Science and Cloud Computing Companion IEEE, 2013.

[12] N. Yang, Y. Cao, Q. Liu, J. Zheng, "A novel personalized TTP-free location privacy preserving method", Int. J. Secure Appl. 8(2), 388, 2014.

[13] Pepsi M, B. B. ., V. . S, and A. . A. "Tree Based Boosting Algorithm to Tackle the Overfitting in Healthcare Data". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 41-47, doi:10.17762/ijritcc.v10i5.5552.

[14] M. Ashouri-Talouki, A. Baraani-Dastjerdi, 'Homomorphic encryption to preserve location privacy'. Int. J. Secur. Appl. 6(4), 183–189, 2012.

[15] Gill, D. R. . (2022). A Study of Framework of Behavioural Driven Development: Methodologies, Advantages, and Challenges. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 09–12. https://doi.org/10.17762/ijfrcsce.v8i2.2068

[16] Ipsa Das, Md Imran Alam, JayantiDansana,'A Survey on Location Based Services in Data Mining', International Journal of Soft Computing and Engineering (IJSCE) ISSN' 2231-2307, Volume-4, Issue-2, 2014.

[17] [Rathod A., Jariwala V., "Investigation of Privacy Issues in Location-Based Services". In: Sa P., Bakshi S., Hatzilygeroudis I., Sahoo M. (eds) Recent Findings in Intelligent Computing Techniques. Advances in Intelligent Systems and Computing, vol 707. Springer, Singapore, 2019.

[18] Alabdulrazzaq, H., & Alenezi, M. N. (2022). Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish. International Journal of Communication Networks and Information Security (IJCNIS), 14(1). https://doi.org/10.17762/ijcnis.v14i1.5262

[19] Payal V Parmar, Shraddha B Padhar, Shafika N Patel, Niyatee I Bhatt and Rutvij H Jhaveri, "Survey of Various Homomorphic Encryption algorithms and Schemes", International Journal of Computer Applications 91(8)"26-32, 2014.

[20] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti, "A survey on homomorphic encryption schemes: theory and implementation", ACM Comput. Surv. V, N, Article A, Januar, 2017.

[21] Baes, A. M. M. ., Adoptante, A. J. M. ., Catilo, J. C. A. ., Lucero, P. K. L. ., Peralta, J. F. P., & de Ocampo, A. L. P. (2022). A Novel Screening Tool System for Depressive Disorders using Social Media and Artificial Neural Network. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 116–121. https://doi.org/10.18201/ijisae.2022.274

[22] Lifang Zhang, Yan Zheng, Raimo Kantoa, “A Review of Homomor-phic Encryption and its Applications”, International Journal of Computer Applications (0975 – 8887) NCIT, 2015.

[23] Rathod A., Shah S., Jariwala V. , “Evaluating Performance of Asymmetric Homomorphic Encryption Algorithms for Privacy Preservation in Location Based Services”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, 2019.

[24] Yong Liu, Wei Wei, Aixin Sun, Chunyan Miao, “Exploiting Geographical Neighborhood Characteristics for Location Recommendation”, In Proceedings of the 23rd ACM International Conference on Information and Knowledge Management (CIKM’14), pp. 739-748. ACM, 2014.

[25] Xin Liu, Yong Liu, Karl Aberer, Chunyan Miao, “Personalized Point-of-Interest Recommendation by Mining Users’ Preference Transition”, In Proceedings of the 22nd ACM International Conference on Information and Knowledge Management (CIKM’13), pp. 733-738. ACM, 2013.

[26] Sina Shaham; Ming Ding; Bo Liu; Shuping Dang; Zihuai Lin; Jun Li, “Privacy Preservation in Location-Based Services: A Novel Metric and Attack Model”, IEEE Transactions on Mobile Computing, Volume: 20 Issue: 10,2020.

[27] Dlay Parmar, Udai PratapRao, “Towards Privacy-Preserving Dummy Generation in Location-Based Services”, Procedia Computer Science, Volume 171, 2020, Pages 1323-1326.

[28] Qingqi Pei, Lichuan Ma, “Privacy Preservation for Location-Based Services”, Encyclopedia of Wireless Networks pp 1100–1102, 2020.