SCALABLE COLLABORATIVE APPROACH FOR PRIVACY PRESERVATION IN LOCATION BASED SERVICES

Ajaysinh Rathod

Department of Computer Science & Engineering,
Krishna School of Emerging Technology,
KPGU, Vadodara, Gujarat, India.
ajay58886@gmail.com

Vivaksha Jariwala

Department of Information Technology,
Sarvajanik College of Engg. and Technology,
Surat, Gujarat, India
vivakshajariwala@gmail.com

Abstract

Location based services have potential due to promising technologies in mobile communication, and information services. LBS users use their location information to get important information from the service providers. There are many popular applications like maps & navigation, information services, Tourist information service, social networking, etc. LBS users need to submit their location and personal information to the location based service providers. i.e.: Location Information & Personal Identity. Location privacy refers to unauthorized users who should not be able to trace the exact location information of the user. Unauthorized users should not be known or reveal the private information of the users during communication. Location and communication privacy & security are the most challenging issues in LBS. Collaborative approach is the fully distributed approach where trusts are distributed among each peer that performs their task mutually. It uses cryptographic approaches that provide highest location privacy and security in LBS. Nowadays; the growth of LBS users is increasing rapidly. Currently, none of the approaches are there that support scalability features. It's a challenge to design a computationally efficient and practical solution that provides strong privacy by reducing the processing overhead that improves scalability. The proposed approach provides privacy, high fault tolerance, strong resilience against security and privacy attacks, support scalability and reduced cost.

***Keywords*: Collaborative, TTP Free, LBS, Privacy, Scalability, Homomorphic Encryption.**

1. Introduction

Information & communication technologies are playing a very important role in the computer & information society. The advancement in new technologies & development in new functionalities to search, store & share the information in recent years have been increased [1]. Location based services are the most important part of geographical information based systems that support integration of spatial location into business processes. The main goal of LBS is to utilize location information to enhance business processes, increase analytical capability or customer services using a wide range of advanced technology. Location based services (LBS) refer to a set of applications that exploit the knowledge of the geographical location from various devices in order to provide important services based on that. In LBS, users will get their required information based on their current positioning system. Some of such popular examples of location based services are tourist information services, emergency support services, LBS search, and location based social networking. Devices used in LBSs are ubiquitous & location enabled like mobiles, PDAs, Laptops, GPS enabled devices and other devices. So users can get highly personalized information any time anywhere. Location based services can be available on various platforms based on their localization technologies.

Location plays the huge role in improving human life as well as their tasks that are performed in their daily life. Users will send a query to the service provider to get their desired information based on their current location. LBS users will organize their tasks which are essential for them by using the LBS application. i.e. "Which is the

best restaurant nearby me?", "Tourist place finder". Users can handle their daily task easily at any time and any place, based on their location.

2. Related Works

In LBS, user need to provide some personalized or sensitive information under some situations with the query i.e. person identification, location information, etc. They don't want to reveal such information to the LBS provider. Any malicious or adversary may obtain highly personalized information from the user. Attackers can determine the location information of the user and based on that also infer important information [2] i.e. trace the user; infer habit of users, daily routine, etc. Attackers or malicious users are able to derive much information because of the tracking capabilities. There are possibilities of varieties of attacks. That opens up many possibilities.

1.1. *Categories of Location based services*

Cryptography is the method to protect the confidential information for storing the data and transmitting the data. Cryptographic techniques are widely used to provide security related services.
Location based services are divided into two categories as Trusted Third Party [4, 5] (TTP based) & without Trusted Third Party (TTP free) [3, 5, 6]. Both categories use cryptography based approaches. In a centralized approach, all the resources and processes are managed by a single entity. Most of the approaches used a centralized model for privacy preservation. Trusted Third Party (TTP) model gives assurance of user's privacy in LBS.

TTP can be malicious so users cannot rely on trusting intermediate entities. In the TTP free model, trust assumption is very weak or completely removed. In the TTP free approach, it is assumed that all users are capable of performing their task without seeking the help of a trusted third party (TTP). Various authors have proposed various approaches in the literature that focus on finding the secure centroid in a cloaked region without TTP.

TTP free approach is classified as
a) ***Client- server approach*** [2] where communication is done between user and untrusted LBS Provider.

b) ***Collaborative approach*** [3, 4] is the fully distributed approach where trusts are distributed among each peer that performs their task mutually.

C) ***User-centric approach*** [3], where the user controls access to their location information without taking help of TTP.

1.2. *Important requirement of Location based services*

Location information directly related to the privacy of the LBS users. Security and privacy of the user's information are becoming critical issues for the LBS users. Security requirement and privacy requirement and efficiency requirement are the most challenging issues for the location based services.

2.2.1. Location Privacy Requirement

Users have to share his/her location information with the service provider or in location based services [3]. On the basis of that, adversaries can infer various information i.e. their exact location, what they are doing, how much time they spent there, what they like and much more information. Adversaries can also infer their everyday work, their workplace, their habits, and their individual interest etc. Adversaries can steal that personal information and misuse it later. Location based services are extensively used in our daily life regularly so users require maintaining their privacy. Location privacy is the most critical issue for the LBS users.

2.2.2. Efficiency Requirement

Efficiency is the key element for mobile users. For any privacy preservation schema for LBS application, it should be efficient in terms of message cost and execution cost [3].

1.3. *Application of LBS*

2.3.1. Location Based Social Networking

Users are very active on social media on the internet and using a variety of applications that are available on that platform. i.e., Facebook, Twitter, Myspace, Whrrl etc. Users find new ways to communicate and keep in touch

with their friends, family members and others. Initially people connect 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 allows users to connect & communicate with each other and also attract the people by providing new services, recommending information based on their location, and planning their events. i.e., Food Finding, Location-Planning, Mood Finding, Adhoc Networking, Social Shopping, etc.

2.3.2. Information Services

Users will get the most important information based on their location, time specific and user's need/activities. As an innovation in wireless networking, mobile phones & information society, the growth of LBS information users are increasing rapidly. Users can reach their important information based on their point of interest, or based on their Geo location. i.e., restaurants, hotels, emergency services, tourist information, traffic data, map navigation. This service uses a pull based method. For example: recommendation of restaurants, location based social networking (i.e., Gowalla, Foursquare, Facebook Place) or Geo based suggestion (i.e., Google place, yahoo local, yelp).

3. Problem Definitions

Location based services have potential due to emerging technologies in the mobile communication and information services. An LBS user uses their location information to get important information from the service providers. There are many popular applications like maps & navigation, information services, etc. LBS users need to submit their location and personal information to the location based service providers. i.e.: Location Information & Personal Identity. Location privacy refers to unauthorized users who should not infer exact location information of the user. Unauthorized users should not be known or reveal the private information of the users during communication.

Location based services are gaining popularity due to the increase in location based information required by the users. Collaborative TTP free model is the best model where users work together for location privacy in LBS. Hence scalability of the system along with location privacy is the most challenging issue today. The proposed approach provides privacy based on much stronger assumptions while eliminating the bottleneck of TTP based approach. It also provides high fault tolerance and strong resilience against security and privacy attacks. It uses cryptographic approaches to secure and achieve highest location privacy. There is a need for an effective approach that gives promise of the privacy of LBS users with improved scalability with minimum cost. It's a challenge to design a computationally efficient and practical solution that provides strong privacy by reducing the processing overhead and improves scalability.

1.4. *Objectives*

The main objective of this research is to allow all users to access location based services without compromising their location privacy. In addition, the take out approach also offers improved scalability with minimum cost.
So, a novel solution is proposed that provides the following features as described below.

Following are the key motivations for current work; TTP Free, Hybrid approaches, Improve scalability, Reduce Overall Cost, Enhance Privacy, Parallel Execution, and Collusion Free.

3.1.1. TTP Free

To remove trust assumption, TTP free schema is the one of the best schema in location based services. All interested users will compute the task without getting help from a trusted third party/centralized server.

3.1.2. Reduce Cost

One of the main objectives is to reduce the overall cost for LBS users. The main objective is to minimize the communication cost and computational cost .

3.1.3. Improve Execution

To improve the overall execution of the framework is one of the main objectives. It should be working in a parallel, efficient and fast manner.

3.1.4. Improve scalability

Hence, scalability is one of the main issues. The main objective is to increase the size of the network in an easier manner.

3.1.5. Privacy

Privacy of LBS users is the most critical issue. Malicious users should not be able to infer sensitive information from the user. For privacy requirements, Homomorphic encryption algorithms are used to achieve security as well as privacy of LBS users. It is essential to investigate most suitable algorithms that offer the strongest location privacy.

3.1.6. Collusion Free

Privacy homomorphism has a loop hall due to collusion problems. The main objective is to make some strategy to avoid collusion free attack and make the framework secure.

4. Proposed Approach

The existing approaches for privacy preservation in location based services were observed. Some approaches are TTP based [2] and some of them are TTP free [3]. Most of the approaches of above categories are providing the location privacy of the LBS users. In LBS, efficiency requirement and scalability is the biggest challenge against increasing popularity of LBS users. LBS users work commonly with each other to compute the tasks in a collaborative approach. All participating users have to trust each other and execute the task mutually like secure data aggregation, secure sum, etc. The novel approach was proposed that provides TTP free location privacy, high fault tolerance and strong resilience against security and privacy attacks, improved scalability with minimum cost.

1.5. *Proposed Communication Schema*

A novel solution that provides location privacy to the LBS users is proposed.

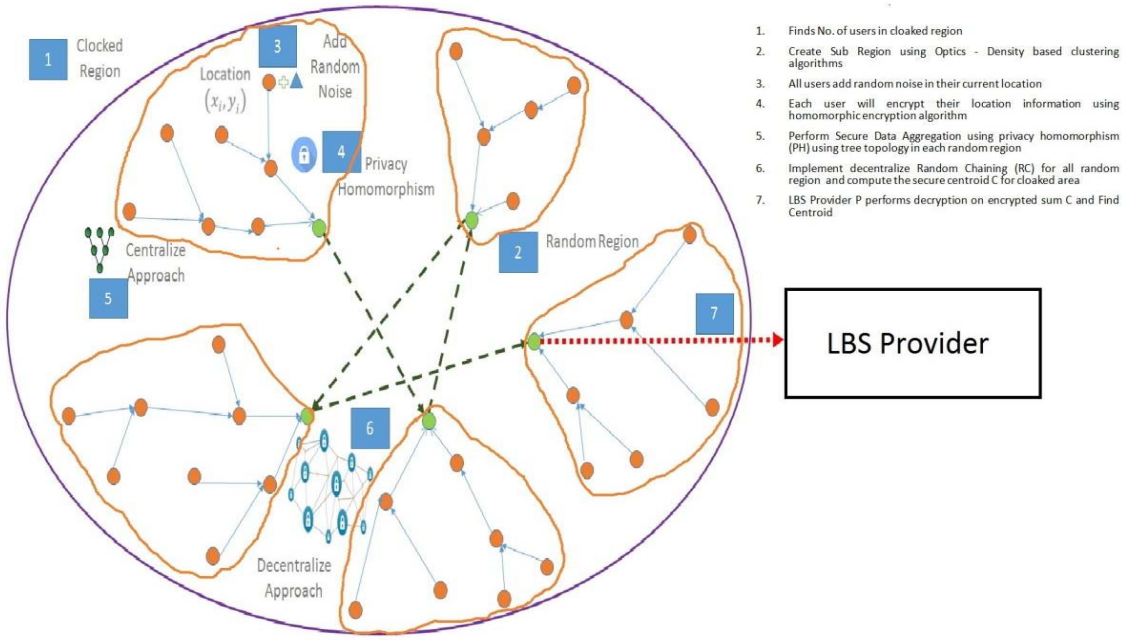

Fig.1 Proposed Communication schema between Users, LBS Provider using Hybrid Approach

Communication schema is proposed between Users, LBS Provider that uses a hybrid approach in fig. 1. Initially, creating a sub region using optics - density based clustering algorithm [6] that helps to execute the algorithms parallel within the sub region as shown in Fig. 1 with label 2 with orange color circle. As part of Phase 1, Random_Partition_Function() is called (Line 8 in algorithm 1). In Phase-2, every user will perturb their location information by adding a random secret split as shown in Fig. 1 with label 3 (Line 9-16 in algorithm 1). In phase-3, each user will perform the secure sum of the location within random partition RP_i using privacy homomorphism (PH) that uses a centralized method as shown in Fig. 1 with label 4, 5 with blue color line (Line 17-22 in algorithm 1). In phase-4, selected location aggregator LA will compute encrypted secure sum of location by using decentralize random selection (RS) between all random partition RP_ias shown in Fig. 1 with label 6 with green color dotted line (Line 23-30 in algorithm 1).Last, LBS Provider, P will perform the decryption of the encrypted sum of location ESL and find secure centroid in that cloaked region in Phase-5 as shown in Fig. 1 with label 7 with red color dotted line (Line 31-32 in algorithm 1).

1.6. *Proposed Algorithm*

Algorithm 1 - Proposed algorithm to find Secure Sum of Location in PPLBS using Hybrid Approach

1. **Input***: LBS Users $LBSU_i$ (User Identity U_i, Location Information (x_i, y_i))*
2. **Output***: Secure Sum of LocationSSL.*
3. *Here, Any LBS User U_i take initiative and send the message to other users $U_{i-1}$to form the centroid*
4. *Interested user give response to LBS User U_i, Here all the users require location based information*
5. *i=0,ctr=0;*
6. *Here, SSL is Secure Sum of Location, RP_i is a random partition in cloaked region where i= 0 to N, TU is the total number of LBS users, LA is a location aggregator within random partition RP_i, ESP is a encrypted sum of location information of a random partition RP_i,TRP is a total number of random partition, ESL is a encrypted sum of location information of LBS User U_i,ctr is counter variable;*
7. *Each LBS user has to enable their positioning system to get the exact location information of the LBS Users(x_i, y_i).*

//Phase-1 Create random partition RP_i based on location of LBS users in the cloaked region

8. *Call Random_Partition_Function();*

//Phase-2 every user will perturb their location information by adding random secret split

9. *Construct the random split as per LBS User U_i*
   Let S and T be a secret,
10. *Generate $[S]_x$ and $[T]_y$ where ($\sum_{i=1}^{TU} (S_{i,x}) = 0), \sum_{i=1}^{TU} (T_{i,y}) = 0))$;*
11. *Distribution of the random split to all the LBS User U_i;*
12. *All LBS Users U_i will add this random split $(S_{i,x}, T_{i,y})$ with location information*
13. ***for** i=0;i<TU ;i++do*
14. *$(x_j, y_j) = ((x_i + S_{i,x}), (y_i + T_{i,y}))$;*
15. ***end***
16. *Each LBs user contain their perturb their location information,*
    $$(x_j, y_j) = ((x_i + S_{i,x}), (y_i + T_{i,y}));$$

//Phase-3 Perform Secure Sum of Location within Random Partition RP_i using Privacy Homomorphism (PH) that uses Centralized method

17. *Compute Secure Sum of Location SSL within Random Partition RP_i;*
18. *From each Random Partition RP_i, select any user who work as a Location Aggregator LA*
19. ***Foreach** Random Partition RP_i**do***
20. *Call Centralized_Data_Aggregation_Function()*
21. *Location Aggregator LA will get encrypted secure sum of location $Epk(x_{rp_i}, y_{rp_i})$of Random PartitionRP_i;*
22. ***end***

//Phase-4 Compute Encrypted Secure Sum of Location by using Decentralize Random Selection (RS) between all Random Partition RP_i

23. *Any randomly selected Location Aggregator LA of Random Partition RP will create list L for remaining Random Partition RP_s,*

24. ***While*** *List L ≠ empty* ***do***
25. *Any Random Partition RP_s is selected randomly;*
26. *ctr++;*
27. *Perform Secure Data Aggregation between Random Partition*
Encrypted Sum of Location ESL=$Epk(\sum_{ctr=1}^{trp} (x_{ctr})), Epk(\sum_{ctr=1}^{trp} (y_{ctr}))$;
28. *Remove selected Random Partition $RP_s$from List L;*
29. ***End***
30. *LastLocation Aggregator LA will send $(ESL, tu)$to LBS Provider P*

//Phase-5 LBS Provider P will perform decryption of Encrypted Sum of Location ESL and find secure centroid in that cloaked region

31. *LBS provider P will decrypt the Encrypted Sum of Location ESL by using his/her Private Key PR_k*
32. *LBS provider will get $\sum_{i=1}^{tu} (x_i), \sum_{i=1}^{tu} (y_i)$;*
33. *Find Secure Sum of Location$SSLx_{SSL} = \frac{\sum_{i=1}^{tu} (x_i)}{u}$, $y_{SSL} = \frac{\sum_{i=1}^{tu} (y_i)}{tu}$*

Function 1 :Random_Partition_Function 0

---

1. ***INPUT****: location information of LBS User $U_{i(x_i,y_i)}$, Minimum number of User to form the cluster MU, Epsilon E;*
2. ***OUTPUT****: Random Partition RP_i:*
3. *Set the Parameter $MU = 2$ and $E = 0.05$*

4. ***for*** *(Every LBS UserU_i)* ***do***
5. *//Use Optics- Density Based Clustering Algorithm to formed the Cluster [25]*
6. *Formed the Random Partition RP_i:*

7. end

8. ***return*** *Random Partition RP_i:*

Function 2: Centralized_Data_Aggregation_Function()

---

1. ***INPUT****: Location information LBS User $U_{i(x_j,y_j)}$, Key Size= 256, Public Key of LBS Provider K_{Pub} ;*
2. ***OUTPUT****: Encrypted Secured Sum of location within Random Partition RP_i:*

3. *Location Aggregator LA will construct Tree Topology in their Random Partition RP_i:*
4. *Every node will encrypt their location information using Paillier - Homomorphic Cryptosystem [27];*
5. ***for*** *i= 1; i<= Random Partition RP_i.Level ; i++****do***
6. *Every child user will send their encrypted location info to their parent user*
7. *Parent user will add their child user's location information and compute Secure Sum Of Location using Tree Topology within their Random PartitionRP_i*
$Epk((x_{rp}, y_{rp})) = Epk((x_{rp}, y_{rp})) + Epk(\sum_{i=1}^{n} (x_i)), Epk(\sum_{i=1}^{n} (y_i))$+..;
8. ***End***
Last, Location Aggregator LA will receive the encrypted sum of location information of the LBS users within their Random PartitionRP_i
9. *ESP = $Epk(x_{rp}, y_{rp}) = Epk(\sum_{i=1}^{n} (x_i)), Epk(\sum_{i=1}^{n} (y_i))$;*
10. ***Return ESP;***

---

5. Results and Comparisons

In this section, implementation and performance evaluation are discussed. In addition to this platform and tools for the evaluation is also described. The logic of the approach with the help of various graphs generated for the configuration with test output is illustrated.

1.7. *Platform and Tools Used*

The simulation scenario is developed in Java that runs on an Intel Core i3 2.30 GHz machine with 2 GB of RAM running Windows7 OS. Here, the major focus is on location based privacy [24-26]. But in the approach, the main goal is to focus on cost, scalability along with location privacy. Hence, in this section, discussion is done regarding creating a random sub region (to decrease computational and communicational cost) in a spatial cloaking region using density based clustering algorithms [5-6] that are not available in the literature.

In order to do this, experimental evaluation with the total computational time taken by the processes is performed. Various density based clustering algorithms with the dataset of various users are experimented. In order to do this, experimental evaluation with the average computational time taken by the processes is performed.

1.8. *Data sets*

Some benchmark datasets, the brinkhoff network based traffic generator simulator [103] generated dataset, Gowalla datasets [112], Weeplace dataset [105] are used.

1.9. *The Test Application*

As discussed earlier, the application is tested for location based service that is implemented in java. This application contains a collection of modules, configurations, and interfaces. Some benchmark datasets are used to test the application. For experimental purposes, no. of user's datasets is taken those are interested to get some information based on their location.

In order to perform experimental evaluation of the approach, with the total time taken to execute all steps, total execution time of the proposed approach.

No of Users	Datasets	RR (ms)	SS&HE (ms)	DA (ms)	CA (ms)	Decryption Time (ms)	Total Time (ms)
50	Brinkhoff	112	144	1	12	10	279
100		192	229	1	14	10	436
200		367	444	1	16	10	828
500		551	2708	1	21	10	3281
1000		788	4169	1	24	10	4982
2000		1100	6352	2	26	11	7480
50	Gowalla	95	86	3	10	11	194
100		183	86	4	11	11	284
200		206	96	4	13	11	319
500		499	96	8	15	11	618
1000		944	123	16	19	11	1102
2000		3826	1289	27	20	11	5162
50	Weeplaces	83	73	3	12	12	171
100		231	129	4	16	12	380
200		460	164	6	19	12	649
500		535	408	10	19	12	972
1000		664	632	15	20	12	1331
2000		3344	1750	20	20	12	5134

Table 1: Result of various parameters of all three dataset

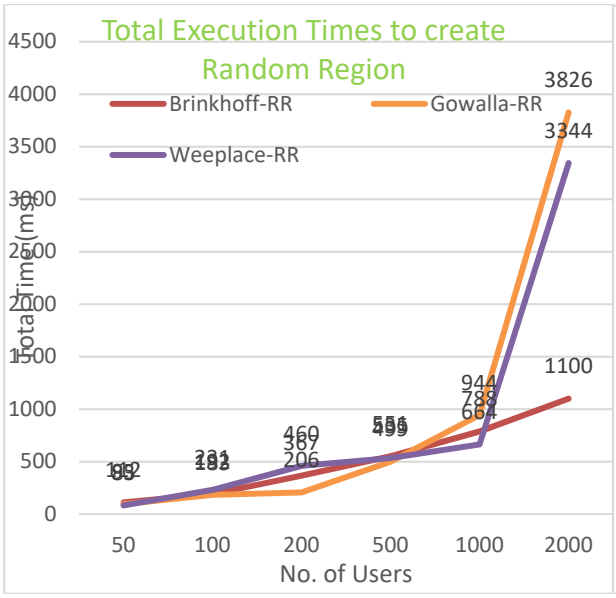

Fig. 2. Total Computational cost to create a random region with no. of no. users for all datasets

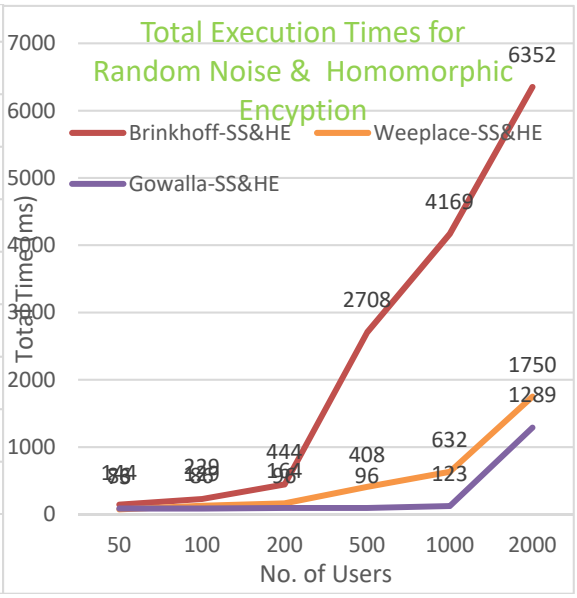

Fig. 3. Total Computational cost for random noise region with and homomorphic encryption for all datasets.

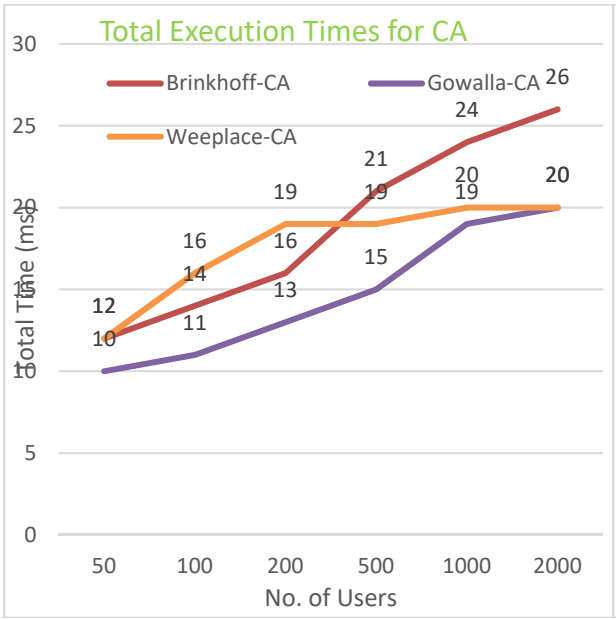

Fig. 4. Perform a centralized approach using tree topology in each sub region all datasets.

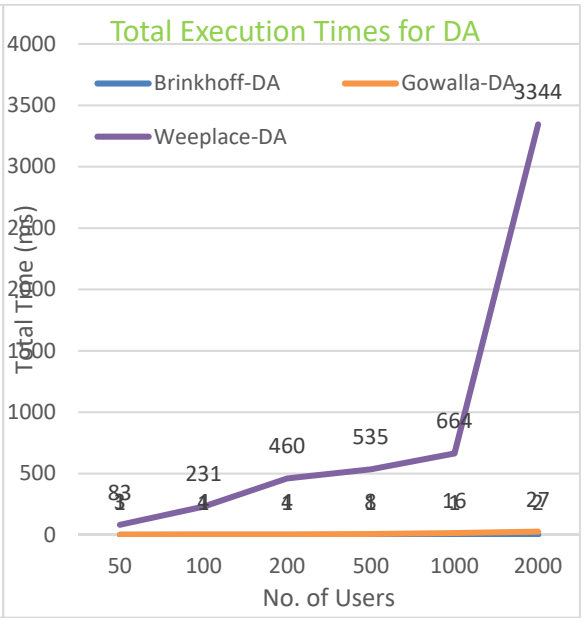

Fig. 5. Total computational cost for decentralized random chaining in all sub-regions of all datasets.

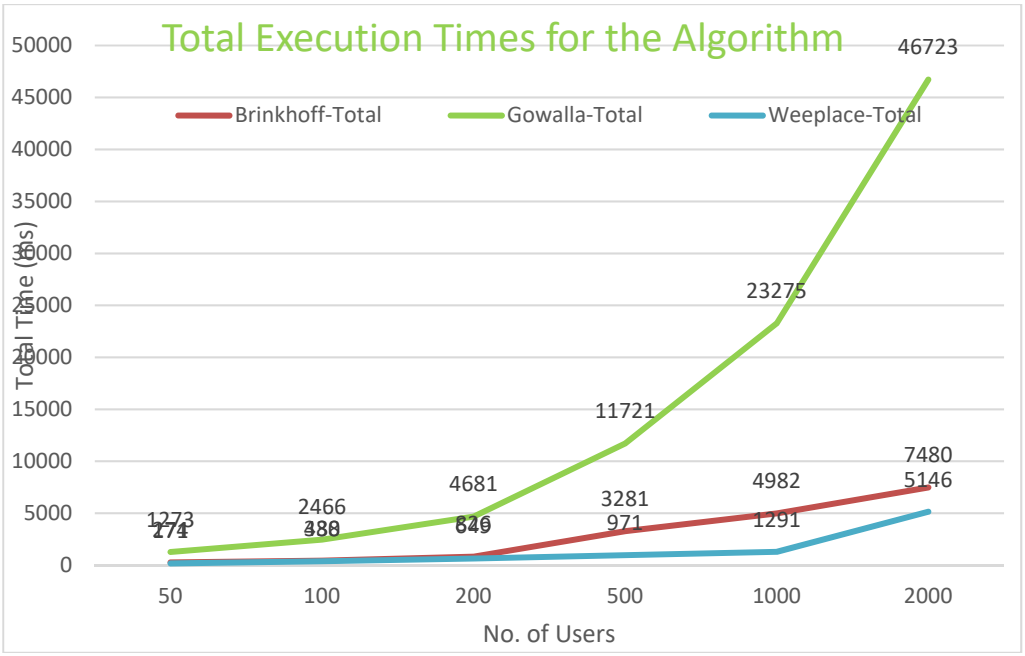

Fig. 6. Total execution time for the decentralized TTP free approach for privacy preservation for LBS for all three datasets.

The evaluation shows the total execution time is taken to perform all the given steps as per the algorithms. Fig 6 shows the average computation time for calculating secured centroid for different numbers of users for all datasets.

6. Conclusions

The Location Based Services LBS is very popular, on demand and has tremendous potential for being useful in various LBS applications like location based navigation, location based search and location based social networking, etc. TTP based cryptography approach to provide location privacy of the user. But Trusted Third Party (TTP) is not reliable because they may contain malicious content. TTP free collaborative approach is one of the best approaches for location privacy of LBS users that uses cryptography techniques. In this approach all the users work mutually to perform assigned tasks together without seeking help of trusted parties (TTP). Nowadays, the growth of LBS users is increasing rapidly so providing the user's privacy with minimum cost is the biggest challenge. Hence, significant effort in research that focuses on proposing and enhancing the privacy of LBS users to find secure centroids. Outcome of the research shows that none of the research exists that provides location privacy of the user with minimum cost and improves scalability. By considering the above problem, that motivates us in the research by proposing a novel approach that uses clustering technique, homomorphic encryption, secret sharing and hybrid approach (centralize and decentralize) for location based services (LBS). Extensive simulation, experiments and detailed analysis were carried out in order to prove the approaches for finding secure centroids using secure data aggregation. The proposed approaches are used to find secure centroid in cloaked regions being secure data aggregation in peer-to-peer collaborative mechanisms that have the features like TTP free, parallel execution, reduce the execution cost, hybrid technique, support scalability, collusion free and enhance the privacy of LBS users.

[1] References

[2] Emmanouil Magkos (2011), “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.
[3] Agusti Solanas, Josep Domingo-Ferrer, and Antoni Mart´ınez-Ballest´ (2010) , “Location Privacy in Location-Based Services: Beyond TTP-based Schemes”, projects TSI2007-65406-C03-01“E-AEGIS”.
[4] Gaoming Yang, Jingzhao Li, Shunxiang Zhang, Huaping Zhou (2013), “A Survey of Location-Based Privacy Preserving”, JCIT.
[5] G. Yang, J. Li, S. Zhang, H. Zhou, “A survey of location-based privacy preserving”. J. Convergence Inf. Technol. 8(11), 27–33, 2013.
[6] M. Wernke, P. Skvortsov, F. Durr, K. Rothermel (2014) “A classification of location privacy attacks and approaches”. Pers. Ubiquit. Comput. 18(1), 163–175.
[7] Rathod A., Jariwala V.(2019) “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.
[8] A. Solanas and A. Mart´ınez-Ballest´e (2008), “A ttp-free protocol for location privacy in location-based services,” vol. 31, no. 6. Elsevier, , pp. 1181–1191.
[9] N. Yang, Y. Cao, Q. Liu, J. Zheng, (2014) “A novel personalized TTP-free location privacy preserving method”, Int. J. Secure Appl. 8(2), 388.

[10] Ajaysinh Rathod, Dr. Vivaksha Jariwala (2019) "Decentralized Collaborative TTP Free Approach for Privacy Preservation in Location Based Services" in International Journal of Electrical and Computer Engineering (IJECE), ISSN: 2088-8708, Vol 9, No 6: (Part II).
[11] Jha S., Kruger L., McDaniel P. (2005) "Privacy Preserving Clustering", In: di Vimercati S. C., Syverson P., Gollmann D. (eds) Computer Security – ESORICS 2005. ESORICS 2005. Lecture Notes in Computer Science, vol 3679. Springer, Berlin, Heidelberg.
[12] Pooja Batra Nagpal, Priyanka Ahlawat Mann (2011) "Comparative Study of Density based Clustering Algorithms", International Journal of Computer Applications (0975 – 8887) Volume 27– No.11.
[13] N. Raghu Kisore, CH. B Koteswaraiah (2017) "Improving ATM coverage area using density based clustering algorithm and voronoi diagrams", Information Sciences 376 pp. 1–20.
[14] M. Ashouri-Talouki, A. Baraani-Dastjerdi (2012) "Homomorphic encryption to preserve location privacy". Int. J. Secur. Appl. 6(4), 183–189.
[15] Ajaysinh Rathod, Dr. Saurabh Shah, Dr. Vivaksha Jariwala (2019) "Evaluating Performance Of Asymmetric Homomorphic Encryption Algorithms For Privacy Preservation In Location Based Services" in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-3, pg. 2191-2194.
[16] Ajaysinh Rathod, Dr. Saurabh Shah, Dr. Vivaksha Jariwala, (2019) "Evaluating Performance Of Asymmetric Homomorphic Encryption Algorithms For Privacy Preservation In Location Based Services" in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-3, pg. 2191-2194.
[17] Xiaoling Zhu*, Yang Lu, Xiaojuan Zhu, Shuwei Qiu (2013) "A Location Privacy-Preserving Protocol Based on Homomorphic Encryption and Key Agreement", International Conference on Information Science and Cloud Computing Companion.
[18] M. Ashouri-Talouki, A. Baraani-Dastjerdi, (2012) "Homomorphic encryption to preserve location privacy". Int. J. Secur. Appl. 6(4), 183–189.
[19] Udai Pratap Rao ; Harshal Girme (2015) "A Novel Framework For Privacy Preserving In Location Based Services", 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
[20] Reza Shokri, George Theodorakopoulos, Panos Papadimitratos, Ehsan Kazemi, Jean-Pierre Hubaux (2014) "Hiding in the Mobile Crowd" Location Privacy through Collaboration", IEEE Transactions On Dependable And Secure Computing, Special Issue On "Security And Privacy In Mobile Platforms.
[21] Belal Amro, Yucel Saygin, Albert Levi (2013) "Enhancing privacy in collaborative traffic-monitoring systems using autonomous location update", IET Intell. Transp. Syst., 2013, Vol. 7, Iss. 4, pp. 388–395.
[22] Paulien Coppens, Laurence Claeys, Carina Veeckman and Jo Pierson (2014) "Privacy in location-based social networks" Researching the interrelatedness of scripts and usage", Symposium on Usable Privacy and Security (SOUPS) 2014,Menlo Park, CA.
[23] Fournier-Viger P. et al. (2016) "The SPMF Open-Source Data Mining Library Version 2". In: Berendt B. et al. (eds) Machine Learning and Knowledge Discovery in Databases. ECML PKDD 2016. Lecture Notes in Computer Science, vol 9853. Springer, Cham.
[24] Ruchika Gupta, Udai Pratap Rao (2017) "A Hybrid Location Privacy Solution for Mobile LBS", Hindawi Mobile Information SystemsVolume.
[25] R. Rothblum (2011) "Homomorphic encryption: From private-key to public key," in Theory of Cryptography Conference. Springer, pp. 219–234.
[26] Vivksha Jariwala, Devesh Jinwala (2011) "Evaluating Homomorphice Encryption Algorithms for Privacy in Wireless Sensor Network", International Journal of Advancements in computing Technology, Volume 3, Number 6.
[27] P. Paillier (1999) "Public-key cryptosystems based on composite degree residuosity classes," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 223–238.
[28] Brinkhoff, T., "A Framework for Generating Network-Based Moving Objects", GeoInformation", https://doi.org/10.1023/A"1015231126594.
[29] http://www.yongliu.org/datasets/
[30] https://foursquare.com/

Authors Profile

Dr. Ajaysinh Rathod is currently working as an Assistant Professor in Department of Computer Science & Engineering, Krishna School Of Emerging Technology, KPGU, Vadodara, Gujarat, India. His research interests include Privacy & Cryptography, Information & Communication Security, Privacy issues in Location Based Services, Big Data Analytics, and Internet of Things.

Dr. Vivaksha Jariwala is currently working as an Associate Professor in the Information Technology Department with Sarvajanik College of Engineering and Technology, Surat (India). Her major areas of interest are Information Security Issues in Resource Constrained Environment, IoT and Software Engineering.