International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 6, December 2019, pp. 5376~5385
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp5376-5385

Decentralized collaborative TTP free approach for privacy preservation in location based services

Ajaysinh Rathod[1], Saurabh Shah[2], Vivaksha Jariwala[2]
[1,2]Department of Computer Engineering, RDIC, C U Shah University, India
[3]Department of Information Technology, Sarvajanik College of Engineering and Technology, India

Article Info

Article history:

Received Nov 3, 2018
Revised Apr 24, 2019
Accepted Jun 26, 2019

Keywords:

Collaborative TTP free
Cryptography
Density based clustering
Location based services
Privacy preservation
Privacy homomorphism

ABSTRACT

In recent trends, growth of location based services have been increased due to the large usage of cell phones, personal digital assistant and other devices like location based navigation, emergency services, location based social networking, location based advertisement, etc. Users are provided with important information based on location to the service provider that results the compromise with their personal information like user's identity, location privacy etc. To achieve location privacy of the user, cryptographic technique is one of the best technique which gives assurance. Location based services are classified as Trusted Third Party (TTP) & without Trusted Third Party that uses cryptographic approaches. TTP free is one of the prominent approach in which it uses peer-to-peer model. In this approach, important users mutually connect with each other to form a network to work without the use of any person/server. There are many existing approaches in literature for privacy preserving location based services, but their solutions are at high cost or not supporting scalability. In this paper, our aim is to propose an approach along with algorithms that will help the location based services (LBS) users to provide location privacy with minimum cost and improve scalability.

Corresponding Author:

Ajaysinh Rathod,
Department of Computer Engineering,
RDIC, C U Shah University,
Wadhwan City, Gujarat, India.
Email: ajay58886@gmail.com

1. INTRODUCTION

Location Based Services (LBS) are winding up progressively with area empowered user's devices like mobile phones, GPS devices, PDAs or other devices. Users can make inquiries to area servers/users those are interested to use and Location based Services (LBS) have pulled in much enthusiasm from both industry and research. For example, a man can discover a few places that draw them from other individuals' travel courses, consequently, design an intriguing and proficient trip in view of different clients' encounters. e.g., Tourist Place Finder, Location-based store discoverer, Emergency Service, area based climate estimate data, area based movement reports, area based ads, advancements and Location-based geo fencing are examples of LBS.

There is always a threat that attacker may able to deduce rich individual data about clients and their versatility. Specifically, a portion of the conceivable deductions exhibited are: User's daily routine through its spatiotemporal data & their movement, Infer habits of the users, Infer absent/present of the user on some particular place at a particular time, also get the user's frequency to visit that particular place, also find out meaningful information about his/her family members / friends based on co-location.

Collaborative TTP free approach is one of the best approach which location privacy of the users. But the main challanges in this approach is high cost, scalability issues along with location privacy of the users. Our apporoch is providing a solution which provide location privacy with reduce cost and improve scalability.

a) Related Work

In this section, we discuss the approaches proposed by the various authors in privacy preserving LBS. Based on that, we studied popular information flow model, privacy requirement in LBS, efficiency requirement, crypto based privacy model, density based clustering and privacy homomorphism.

1) Location privacy

The protocol does not reveal the (extract) user's location information to the LBS provider [1]. In this, attacker is not able to access/infer real location of the users. If an attacker can get the location of the users, then the attacker will derive much personal information like user's habits, infer user's present/absent at a particular time with place and many other information which is highly personalized.

2) Peer-to-peer model

An optional model is the peer-to-peer model where the users of each node would like to communicate with each other without seeking the help of any other centralize node/server to compute the tasks. This distributed model widely used to compute any task together without the help of outsiders. All users have to trust on each other and also perform this task in a secure manner. Figure 1 show the communication schema between a set of collaborative users and LBS provider.

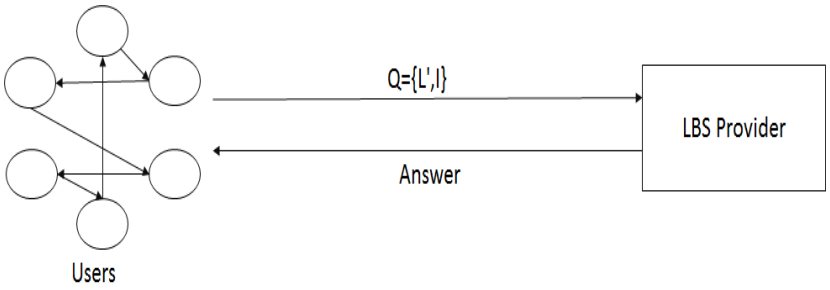

Figure 1. Communication schema between a set of collaborative users and LBS provider [2]

3) TTP free collaborative-based schema

Figure 2 shows the collaborative method between two users. This schema is fully distributed schema. The trust is scattered among the nodes that forms an ad-hoc network. All peers work collaboratively to achieve privacy among untrusted entities. Various algorithms are already proposed as Solanas & Balleste, Rebollo-Monedero, Ardagna etal, Etc [3-9]. The advantage of this approach is that it does not rely on TTP, it is distributed and also guarantees user's privacy. The main disadvantage of this method is related to the Computation & Communication cost and Scalability issues.

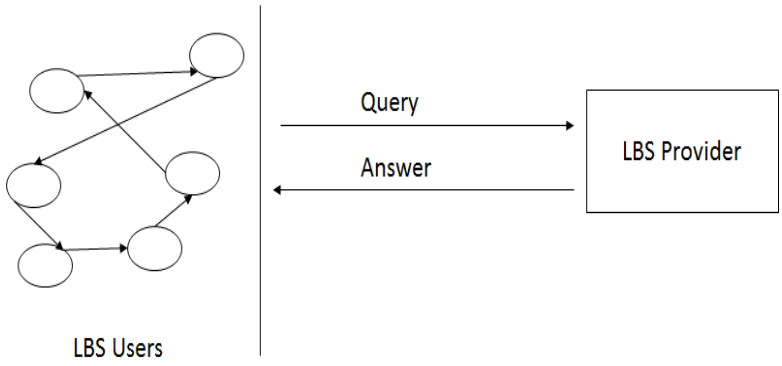

Figure 2. The communication schema of Collaborative Method between Users, LBS Provider [2]

4) Density based clustering algorithms

Density based clustering algorithms is a process of making the group of objects which share the common property called as clustering. It provides the benefit to find out different groups based on their properties. A clustering technique widely used in various applications like Data Mining, Text Mining, Location Based Services, Image Processing, Web Mining and many more.

It is the process of making the groups of points together, which are close to the given dataset/set of points in space. This is known as density based clustering. Example of density based clustering are DBSCAN & OPTICS [10, 11]. In DBscan [10, 11] algorithm, cluster of the data object is generated based on their density. DBscan is popular algorithm and wildly use to find non-spherical shape clustering from the given dataset. DBscan is quite faster for processing & widely suitable for non-changeable density based objects. Optics [10, 11] uses the concept of identification of the implicit clustering for given set of point in dataset. It creates an ordering of the data set objects and also store the distances and reachability to other nodes with distance.

5) Homomorphic encryption

Homomorphic encryption is a schema which performs the various computations on encrypted data. Homomorphic encryption technique is widely used to preserve privacy and security in various area. Privacy homomorphism will provide a guarantee of location privacy of the users [12-17]. Privacy homomorphism has both types of function: Encryption and Decryption. With the use of Homomorphic encryption, user is not able to see the actual location of the companion.

6) Random chaining

Due to collision problem, privacy homomorphism is not much secure. To avoid this problem, random chaining is one of the best approach [13]. In this method, users will randomly select the companion from interested users. The main goal behind the random chaining is to avoid sending messages to the central collector/main aggregator node. This approach will also provide more security against collusion attack in distributed computation of the sum of the location.

b) The problem statement

Location privacy is one of the key issues that needs to be solved. There are various schemas proposed by different researchers [8, 9, 18-23]. Out of that Collaborative TTP Free model [24-26] is one of the best technique to provide highest location privacy. Though schemas [24-26] have the advantages, there are still open issues that require attention. Location based services are gaining popularity due to the increase in location based information required by the users. Hence cost and the scalability of the system is the most challenging issue need to be focused. So, there is a need of an approach that provides lower communication and computational cost, improves scalability also provides privacy that is not done till now. Hence, in this section we propose the privacy preserving LBS schema that is TTP free, improves scalability, lower cost, robust against the collision of users and also provides privacy.

2. PRAPOSED APPROACH

In this section, we propose a novel solution that provides location privacy to the LBS users. The main goal of research is to achieve features that does not rely on TTP and randomize approach and also improves scalability, reduce cost in resource constraint devices, and enhance security & privacy. Figure 3 represents the system architecture of proposed schema [27]. It contains two main components as a) LBS users and b) LBS provider. Each user has their private information on their mobile like UserID Uid, location information (Lgi, Lti). In our approach, our primary focus is to find out the number of Users Ui in cloaking region who are requesting for location-based information. As shown in Figure 3, we are generating random region [28, 29] Ri based on the density based clustering algorithm optics [10, 11] and Dbscan [10, 11] for users in spatial cloaked region. Then all users will add random noise by using the secret share function. After this, we use decentralize approach to perform secure data aggregation using privacy homomorphism PH [13] in each random region Ri using random chaining that is shown in Figure 3 with red edges. Then, we used the decentralized approach to perform random chaining RC for all distributed random region Ri to compute the secure centroid C as shown in Figure 3 with green edges. After this, the last user, U sends the encrypted sum of location C to LBS provider P as shown in Figure 3 with black edge.

The main aim of our approach is to hide the user's location from the other users and also give inaccurate location information to the LBS provider. Our approach is based on decentralize approach, that use distributed method to achieve minimum cost and scalability. In this paper, we propose a protocol schema for privacy preservation between users and LBS provider.

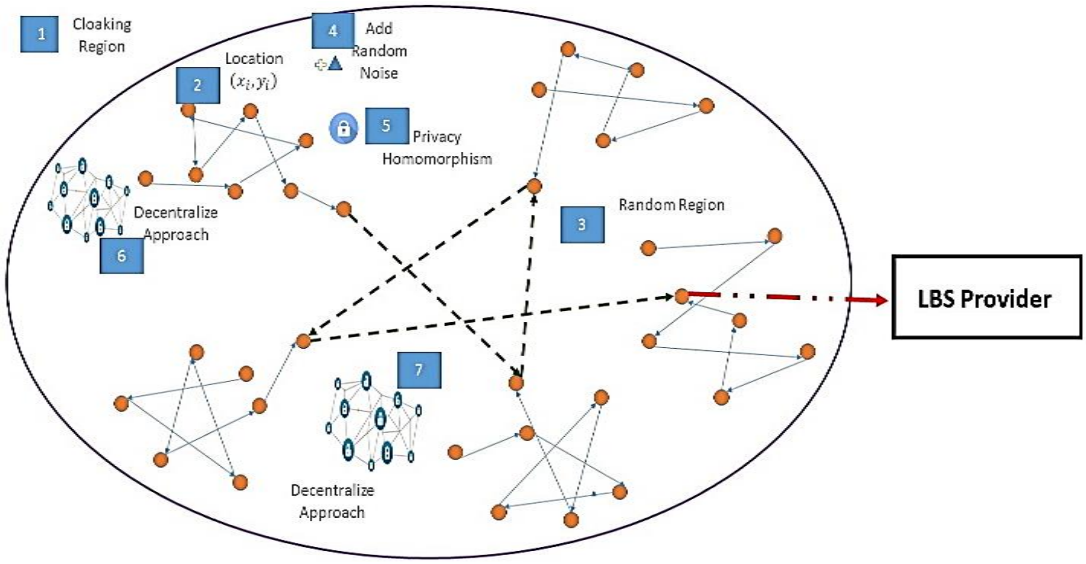

Figure 3. Proposed communication schema of decentralized method between users, LBS provider

a) Proposed Protocol Schema

Our proposed protocol schema divided in 5 phase as follows:

1) Phase-1 Create Random Region in the cloaked region N

Users need important information based on their location. An initiator will send the message to all the users in the cloaked region till K no. of users will respond him/her. Any one user will call Random Region() to create sub-region by using density based clustering algorithms. By end of this phase, different sub regions r_i are created.

2) Phase-2 All users add random noise in their current location

In this phase, each user will add random noise s_j on their actual location by using Secret_Share (). All users will add random noise$(x_j, y_j) = ((x_j + s_j), (y_j + s_j))$. In each random region r_i , the user selects any user as aggregator executor AE to perform the next computation where AE $\in r_i$.

3) Phase-3 Perform Secure Data Aggregation using privacy homomorphism (-PH) using random chaining method in each random region

In each random region r_i, aggregator executor AE will perform secure data aggregation using privacy homomorphism PH. All users will call Secure_Data_Aggregation() to perform computation. Here, by using decentralize approach, the user will select a random user using Random_Region () from each random region r_i to avoid collision attack. After the end of this phase, all AE will have secure sum of their random region r_i $(Epk(\sum_{m=1}^{n}(x_m)), Epk(\sum_{m=1}^{n}(y_m)))$.

4) Phase-4 Implement decentralize Random Chaining (RC) for all random region r_i and compute the secure centroid C for cloaked area

In this phase, User U will select a random AE from each region r_i and perform secure sum for each random regionr_i. Last user will compute secure centroid $(Epk(\sum_{i=1}^{k}(x_i)), Epk(\sum_{i=1}^{k}(y_i)))$. Last user will send secure centroid C to the LBS provider P.

5) Phase-5 LBS Provider P performs decryption on encrypted sum C and Find Centroid.

Finally, Location based services (LBS) provider P decrypting secure centroid $(Epk(\sum_{i=1}^{k}(x_i)), Epk(\sum_{i=1}^{k}(y_i)))$ using his/her private key. The provider will obtain the value $(\sum_{i=1}^{k}(x_i), \sum_{i=1}^{k}(y_i))$. Last, Provider P will divide it by K & find centroid C.

Considerations and Assumptions:

i. Using Public key infrastructure (PKI), User will get the public key of LBS provider from directory/authority.

ii. Mobile user have to enable location based services to get his/her location information.

b) Proposed Algorithms

Algorithm 1: Users communicate using Proposed Model

Input: LBS Users U_i (User IdentificationU_{id}, Position information (x_i, y_i))
Output: Compute Secure Centroid C.
1- User U_i starts and send query to Provider P & N represents the minimum number of user require to create centroid C;
2- Let K is the no. of interested user who responded, m is the no. of users in random region, r_i is a random region where i=1 to N;
3- Start, C=0, i=0, k=0;
4-Lets each users are having their location information as (x_j, y_j) ;

//**Phase-1 Create Random Region in cloaked region**
5-Mobile user U_i CALL Random_Region_Function;
6- **For** each random region r_i**do**
For j FROM 1 TO cluster r_i.size **do**

//Phase-2 All users add random noise in their current location
Call Secret_Share_Function;
$(x_j, y_j) = ((x_j + s_j), (y_j + s_j))$;
User U, select a random node as aggregator executor AE, AE ∈ r_i**;**

//Phase-3 Perform Secure Data Aggregation using privacy homomorphism PH using random chaining method in each random region
Perform secure sum within region Ri, Call Secure_Data_Aggregation;
$(Epk(\sum_{m=1}^{n}(x_m)), Epk(\sum_{m=1}^{n}(y_m)))$;
End for
End for

//Phase 4 - Implement decentralize Random Chaining RC for all random region r_i and compute the secure centroid C for cloaked area.
7-**ForEach** random region r_i**do**
User U, select a random AE from each region r_i;
Perform secure sum and find secure centroid $(Epk(\sum_{i=1}^{k}(x_i)), Epk(\sum_{i=1}^{k}(y_i)))$;
8-**End for**
9-Last AE send encrypted result Centroid $Epk(\sum_{i=1}^{k}(x_i)), Epk(\sum_{i=1}^{k}(y_i)))$ to provider;

// Phase 5: LBS Provider P perform decryption on encrypted sum C and Find Centroid.
10- Provider P decrypt the sum of location by applying his/her private key.

Algorithm 2: Random_Region_Function

Input: Users , MinPts, Radius.
Output: New Clusters r_i.

1-Lets Set MinPts=2, Eps=0.005;
2- Apply Density based clustering algorithms;
3-**For** (each user K) **do**
4- Formed cluster r_i;
5-**End for**
6-Return r_i;

Algorithm 3: Secret_Share_Function

1- AE select and divide large random shares S for users such that $\sum_1^j S_j = 0$;
2- AE send all secret share value to all users ϵ r_i ;

Algorithm 4: Random Chain approach

Input: Users, MinPts, Radius.
Output: Select Random Companion.
1- User u build chain C by identifying no of users U_i ;
2- **While** rs ≠ Empty **do**
3- User u randomly select companion;
4- Delete selected companion from list;
5-**End do**
6-Return random_ companion;

Algorithm 5: Secure Data Aggregation

Input: Users, Location info, Public key of Providers
Output: Encrypted Sum of Location.
1- Call Random_Chaining;
2-Apply Homomorphic Encryption Algorithms;
3-Return Encrypted Centroid;

3. RESULTS AND ANALYSIS

We have implemented and experimented our proposed approach in Java. We run it on an Intel Core i3 2.30 GHz machine with 2 GB of RAM running Windows7 OS. In literature, major focus is on location based privacy [24-26]. But in our approach, our mail goal is to focus on cost, scalability along with location privacy. Hence in this section, we have discussed the results for creating random sub region (to decrease computational and communicational cost) in spatial cloacking region using density based clustering algorithms [10, 11] that is not available in literature.

We experimented the performance with different density based clustering algorithm and different dataset of users. To measure performance metrics, we use average computation time taken by the processes.

a) Datasets

We have used two datasets: 1) Brinkhoff Traffic Dataset [30, 31] and 2) Gowalla dataset [32].

1) Brinkhoff traffic dataset

By using this standard dataset in our simulation when a user is sending their queries to LBS providers. We use Brinkhoff [30] network-based traffic generator simulator. We randomly generate various dataset of 50, 100,200, 500, 1000, 2000 mobile users that was simulated on the real road map of Ahmedabad city in india. For our experimental purpose, we generate 5 synthetic datasets: dataset1, dataset2, dataset3, dataset4, dataset5 using Brinkhoff's traffic data generator tool [31]. Figure 4 shows the footprints of 1, 000 mobile users in the real road map of Oldenberg, Germany, generated via Brinkhoff Traffic generator.

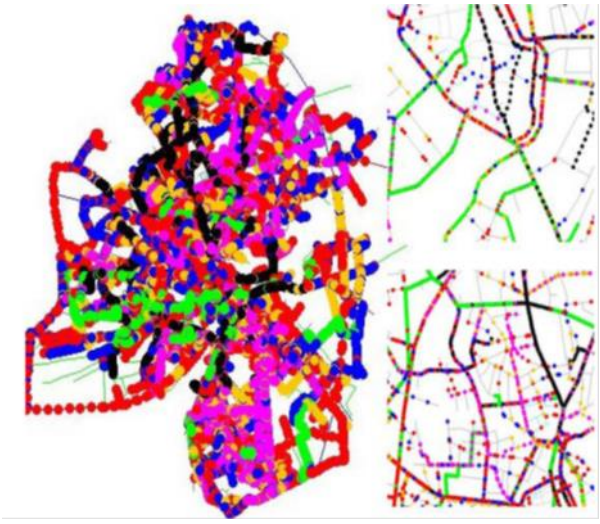

Figure 4. The footprints of 1, 000 mobile users in the real road map of Oldenberg, Germany, generated via Brinkhoff Traffic generator

2) Gowalla dataset

We use Gowalla dataset [32] based on a popular location based social network. This dataset contain more than 600000 Facebook users since November, 2010. To generate this dataset, they used Gowalla APIs to collect various information like user's profile, user friendship, location profiles, and user's check-in history made before January, 2011 of the user's based on social networking site: Facebook. This dataset contain 36,001,959 check-in by 319,063 users over 2,844,076 different locations [32] based on various categories of Food, Entertainment, Community, Shopping, Travel, Nightlife, etc. We use different datasets of 50,100,200, 500, 1000, 2000 user's based on food dataset category for our research.

b) Results

In this section, we discuss the results of our proposed approach with two data sets

1) Brinkhoff Traffic Dataset [30, 31]
2) Gowalla dataset [32].

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 Figures 5 - 10. OPTICS algorithm gives better result as compared to DBSCAN clustering algorithm.

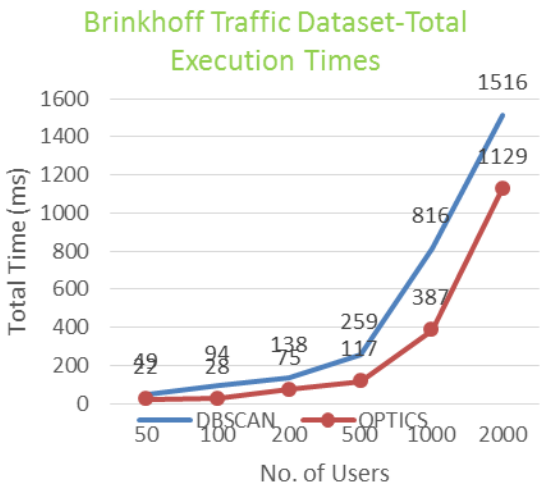

Figure 5. Total execution time over no. of users for Brinkhoff Dataset

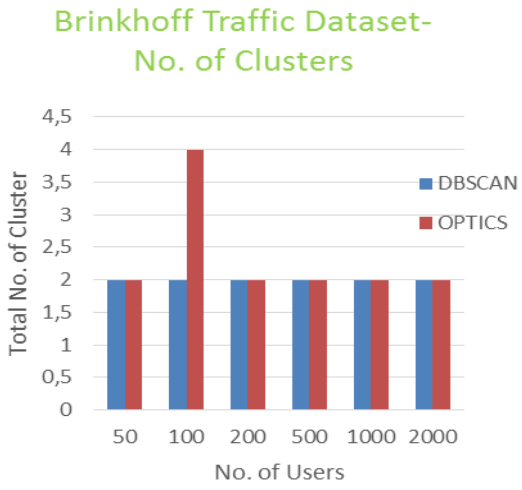

Figure 6. No. of Cluster over no. of users for Brinkhof Dataset

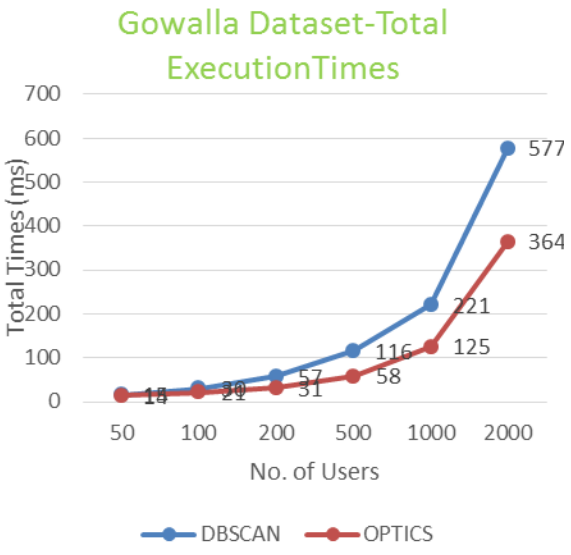

Figure 7. Total Execution time over no. of users for Gowalla Dataset

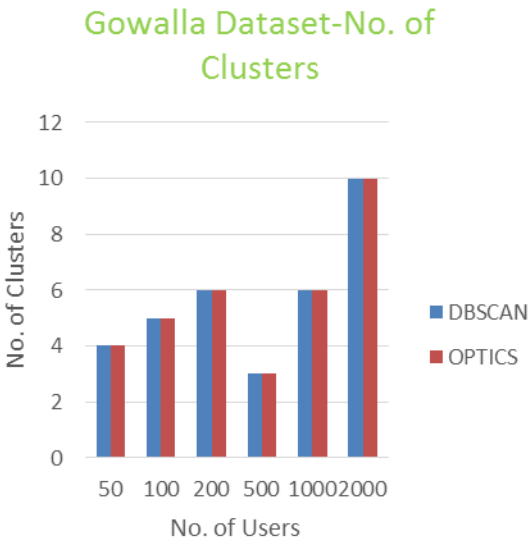

Figure 8. No. of Cluster over no. of users for Gowalla Dataset

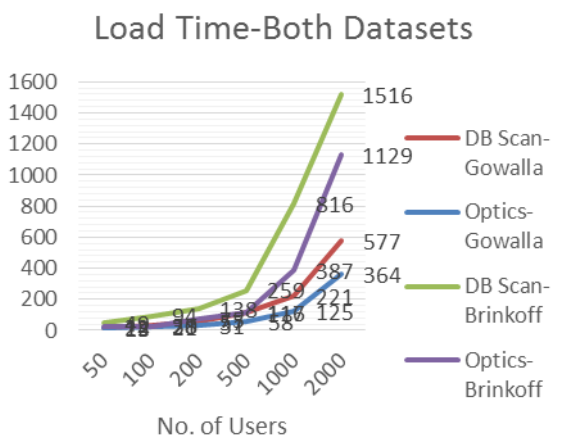

Figure 9. Total Execution time over no. of users for Both Dataset

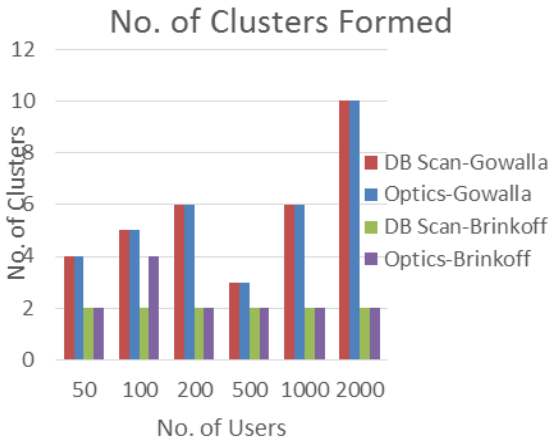

Figure 10. No. of Cluster Created over no. of users for Both Dataset

4. CONCLUSION AND FUTURE WORK

Location privacy is of the utmost importance with the rapid growth of LBS users. In this paper, we deliberated various related work which was proposed by various authors. This paper addressed the issues in Collaborative TTP free model and also presented proposed approach that uses density based clustering, homomorphic encryption and randomize approach. We have an approach that performs various steps on benchmark datasets. We create a clusters from a given set of input dataset by using basic density based clustering algorithms- DBSCAN & OPTICS. We have analyzed the performance of our model for various parameters like execution time and no. of clusters based on various users. From our analysis and result, we can say that OPTICS algorithm gives better result compared to DBSCAN. Our future work, will focus on homomorphic encryption and distributed random chaining in our proposed schema.

REFERENCES

[1] R. Padmanaban, "Location Privacy in Location Based Services: Unsolved Problem and Challenge," *International Journal of Advanced Remote Sensing and GIS*, vol. 2, pp. 398-404, 2013.
[2] E. Magkos, "Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey," *International Journal of Information Technologies and Systems Approach (ACM)*, vol 4, 2011.
[3] G. Yang, et al., "A Survey of Location-Based Privacy Preserving," *Journal of Convergence Information Technology*, vol. 8, 2013.
[4] N. Yang, et al., "A Novel Personalized TTP-free Location Privacy Preserving Method," *International Journal of Security and Its Applications*, vol. 8, 2014.
[5] A. Solanas, et al., "Location Privacy in Location-Based Services: Beyond TTP-based Schemes," *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications*, 2008.
[6] G. Ghinita, et al., "Private Queries in Location Based Services: Anonymizers are not Necessary," *ACM SIGMOD international conference on Management of data*, pp. 121-132, 2008.
[7] G. Ghinita, et al., "A Hybrid Technique for Private Location-Based Queries with Database Protection," *Springer Advances in Spatial and Temporal Databases Volume 5644 of the series Lecture Notes in Computer Science*, pp 98-116, 2009.
[8] C. Bettini, et al., "Protecting Privacy Against Location-based Personal Identification," *Workshop on Secure Data Management SDM 2005: Secure Data Management*, pp. 185-199, 2006.
[9] G. Yang, et al., "A Survey of Location-Based Privacy Preserving," *Journal of Convergence Information Technology*, vol. 8, 2013.
[10] J. Liu, et al., "Privacy Preserving Distributed DBSCAN Clustering," *ACM*, 2012.
[11] P. B. Nagpal and P. A. Mann, "Comparative Study of Density based Clustering Algorithms," *International Journal of Computer Applications*, vol. 27, 2011.
[12] A. Solanas and A. M. Balleste, "A TTP-free protocol for location privacy in location-based services," *Elsevier Transactions on Computer Communications*, vol. 31, pp. 1181-1191, 2008.
[13] A. Solanas and A. M. Balleste, "Privacy Protection in Location-Based Services through a Public-Key Privacy Homomorphism," *Proceedings of the 4th European conference on Public Key Infrastructure: theory and practice Springer*, 2007.
[14] Y. Huang and R. Vishwanathan, "Privacy Preserving Group Nearest Neighbor Queries in Location-Based Services Using Cryptographic Techniques," *IEEE Global Telecommunications Conference GLOBECOM*, 2010.

[15] V. Jariwala and D. Jinwala, "Evaluating Homomorphice Encryption Algorithms for Privacy in Wireless Sensor Network," *International Journal of Advancements in computing Technology*, vol. 3, 2011.
[16] X. Zhu, et al., "A Location Privacy-Preserving Protocol Based on Homomorphic Encryption and Key Agreement," *International Conference on Information Science and Cloud Computing Companion IEEE*, 2014.
[17] M. A. Talouki and A. B. Dastjerdi, "Homomorphic Encryption to Preserve Location Privacy," *International Journal of Security and Its Applications*, vol. 6, 2012.
[18] M. Wernke, et al., "A Classification of Location Privacy Attacks and Approaches," *Personal and Ubiquitous Computing, Springer-Verlag*, vol. 18, pp 163-175, 2014.
[19] R. Gupta and U. P. Rao, "An Exploration to Location Based Service and Its Privacy Preserving Techniques: A Survey," *Journal Wireless Personal Communications: An International Journal archive*, vol. 96, pp. 1973-2007, 2017.
[20] A. K. Tyagi and N. Sreenath, "Preserving Location Privacy in Location Based Services against Sybil Attacks," *International Journal of Security and Its Applications*, vol. 9, 2015.
[21] T. Peng, et al., "Enhanced Location Privacy Preserving Scheme in Location-Based Services," *IEEE SYSTEMS JOURNAL*, 2014.
[22] A. K. Tyagi and N. Sreenath, "Future Challenging Issues in Location based Services," *International Journal of Computer Applications*, vol. 114, 2015.
[23] R. J. Patil, et al., "Analysis on Preserving Location Privacy," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, 2015.
[24] B. Amro, et al., "Enhancing privacy in collaborative traffic-monitoring systems using autonomous location update," *IET Intelligent Transport Systems*, vol. 7, pp. 388-395, 2013.
[25] S. Patil, et al., "Hiding User Privacy in Location Base Services Through Mobile Collaboration: A Review," *International Conference on Computational Intelligence and Communication Networks IEEE*, 2015.
[26] R. Shokri, et al., "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*, 2014.
[27] Rathod A. and Jariwala V., "Hybrid Cryptographic Based Approach for Privacy Preservation in Location-Based Services," in Woungang I. and Dhurandher S. (eds), *2nd International Conference on Wireless Intelligent and Distributed Environment for Communication. WIDECOM 2018. Lecture Notes on Data Engineering and Communications Technologies*, Springer, Cham, vol. 27, 2019.
[28] S. R. Shastry, et al., "Generating: random regions in Spatial cloaking algorithm for location privacy preservation," *IOSR Journal of Computer Engineering, IOSR-JCE.*, vol. 9, pp. 46-49, 2013.
[29] Rathod A. and Jariwala V., "Investigation of Privacy Issues in Location-Based Services," in Sa P., et al., (eds), "Recent Findings in Intelligent Computing Techniques," *Advances in Intelligent Systems and Computing*, Springer, Singapore, vol. 707, 2019.
[30] M. Wernke, et al., "A Classification of Location Privacy Attacks and Approaches," *Springer*, vol. 18, pp. 163-175, 2014.
[31] Y. Wang, et al., "Location-aware Location Privacy Protection for Location-based Services," *Proceedings - IEEE INFOCOM*, pp. 1996-2004, 2012.
[32] Y. Liu, et al., "Exploiting Geographical Neighborhood Characteristics for Location Recommendation," *Proceedings of the 23rd ACM International Conference on Information and Knowledge Management (CIKM'14)*, ACM, pp. 739-748, 2014.

BIOGRAPHIES OF AUTHORS

Mr. Ajaysinh Rathod was born on 19th November 1983. He is currently working as Ph.D Research Scholar in Department of Computer Engineering, RDIC, C U Shah University, Wadhwan City, 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. Saurabh Shah is currently working as Professor & Director in Department of Computer Engineering, RDIC, C U Shah University, Wadhwan City, Gujarat, India. His research interests include Privacy & Cryptography, Computer Intelligence, Image Mining and Image Processing

Dr. Vivaksha Jariwala was born on 23rd November 1980. She is an Associate Professor in 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.