

# Progressive Collaborative Method for Protecting Users Privacy in Location-Based Services

K Ramakrishna Reddy<sup>1,\*</sup>, V.K. Sharma<sup>2</sup>, M. Anusha<sup>3</sup>, Srinivas Jhade<sup>4</sup>, B.Dhanasekaran<sup>5</sup>

<sup>1</sup>CSE Department, KG Reddy College of Engineering and Technology, Hyderabad, Telangana, India.

<sup>2</sup>Département of EEE, Bhagwant University, Rajasthan-India.

<sup>3</sup>Département of ECM, JBIET, Hyderabad-Telangana, India.

<sup>4</sup>CSE Department, KG Reddy College of Engineering and Technology, Hyderabad, Telangana, India.

<sup>5</sup>Département of EEE, Bhagwant University, Rajasthan-India.

**Abstract.** The development of new mobile communication and information service technologies has opened up exciting possibilities for location-based services. Users of location-based services (LBS) can access vital data from their service providers by utilizing their location data. Maps and navigation, information services, tourist information services, social networking, and many more popular applications are available. A user's location and other personal details must be submitted to the providers of location-based services in order for them to work. For example, details about one's whereabouts and identity. By "location privacy," we mean the idea that third parties shouldn't be able to track a user's precise whereabouts. It is important that users' sensitive information be hidden from unauthorized individuals when communicating. Most difficult in LBS are concerns about the privacy and security of location-based communications and data. Each peer does their duty reciprocally in a collaborative method, which is a completely distributed technique. For the most secure and private location-based services (LBS), it employs cryptographic methods. The number of people using LBS is growing at a rapid pace these days. At this time, there isn't a single method available that has scalability capabilities. Building a realistic and computationally efficient solution that offers high privacy while decreasing processing overhead and improving scalability is a challenging task. The suggested method is cost-effective, supports scaling, is highly resilient against security and privacy assaults, and ensures privacy.

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

## 1 Introduction

The computer and information society is greatly reliant on information and communication technologies. In recent years, there has been an uptick in the creation of new functions and

---

\* Corresponding author: [Krkreddy20@gmail.com](mailto:Krkreddy20@gmail.com)

advancements in technology that make it easier to find, save, and exchange information [1]. When it comes to GIS-based systems that facilitate the incorporation of physical location into operational procedures, location-based services are king. The primary objective of location-based services (LBS) is to improve company operations, analytical capabilities, and customer services by leveraging location data through various forms of cutting-edge technology. The term "location based services" (LBS) describes a group of programs that make use of the devices' location data to offer useful services. With LBS, users may access the data they need by just pointing their device's GPS at it. Services that provide information to tourists, help in times of emergency, provide location-based social networking, and conduct location-based search are all examples of location-based services. All sorts of location-enabled devices, such as smart phones, PDAs, laptops, and other gadgets, are utilized in LBSs. In this way, consumers can get highly tailored data whenever and wherever they like. Depending on their localization technologies, several platforms may offer location-based services.

A person's life and the things they do on a daily basis are greatly impacted by their location. In order to acquire the information they want, users will submit a query to the service provider using their current location. By utilizing the LBS application, users will be able to arrange their vital chores in a systematic manner. like, "Which one is the

"Tourist place finder" and "best restaurant nearby me?" Users are able to effortlessly complete their everyday tasks regardless of their location, regardless of time or place.

## 2 Related works

In certain cases, users may be asked to disclose sensitive information (such as their identity or location) when using LBS for a query. They would prefer not to give the LBS provider such details. Anyone with ill intentions could potentially gain access to sensitive user data. The user's location data can be used by attackers to deduce critical information, such as their habits, daily routines, etc. [2]. Because of the tracking capabilities, attackers or malevolent users can deduce a lot of information. Multiple assault types are possible. In doing so, numerous doors are opened.

### 2.1 Categories of Location based services.

When storing or transferring sensitive information, cryptography is the way to go. The provision of security-related services makes extensive use of cryptographic techniques. There are two main types of location-based services: those that rely on a Trusted Third Party (TTP)[4,5] and those that do not [3,5, 6]. Both groups rely on methods that are based on cryptography. One entity manages all the resources and procedures in a centralized way. The majority of the methods relied on a centralized mechanism to protect user privacy. To guarantee user privacy in LBS, the Trusted Third Party (TTP) approach is employed.

Users should not put their faith in intermediaries because TTP can be harmful. The premise of trust is either severely reduced or eliminated in the TTP free approach. It is believed that all users may complete their task without involving a trusted third party (TTP) in the TTP free approach. Several writers have put up different methods in the literature for locating the safe centroid in a hidden area that does not use 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.

## 2.2 Important requirement of Location based services

Users' privacy is directly affected by location data. Users of LBS are increasingly concerned about the security and privacy of their information. The most difficult problems for location-based services to solve are the needs for efficiency, privacy, and security. Need for Location-Based Privacy. In location-based services, users are required to provide their precise whereabouts to the service provider [3]. From that, their enemies can deduce a great deal, including their precise whereabouts, activities, the amount of time spent there, preferences, and more. Their adversaries can also deduce their daily tasks, location of employment, habits, interests, etc. Criminals may get their hands on such private data and utilize it for their own ends. Users need that location-based services respect their privacy because of how often we use them in our daily lives. For LBS users, location privacy is of utmost importance. Essentiality of Efficiency For people who utilize mobile devices, efficiency is paramount. The message cost and execution cost of any privacy preservation scheme for LBS applications should be efficient [3].

## 2.3 Application of LBS

Using GPS to Connect with People

Internet users are very engaged in social media and the many applications accessible on that platform. platforms such as Facebook, Twitter, Myspace, Whrrl, and etc. Novel means of interaction and communication are discovered by users.

in the company of their loved ones and acquaintances. People first meet on social media, and then they begin to share their whereabouts on those platforms using the ubiquitous GPS-enabled smartphones.

i.e., engaging in "check in" activities entails divulging crucial location data to other individuals or big groups of interconnected social media users. Through geosocial networking, users are able to not only converse and connect with one another, but also to plan events, receive location-based recommendations, and access new services. For example, social shopping, adhoc networking, mood discovery, food discovery, location planning, etc. Data Processing

According to the user's location, the time of day, and their needs and activities, they will receive the most necessary information. Users of location-based services (LBS) are on the rise due to this technological advancement in the realms of wireless networking, mobile phones, and the information society. Depending on their point of interest or geolocation, users can get their critical information. e.g., lodging, dining, transportation, emergency services, tourist info, traffic reports, and directions. A pull-based approach is used by this service. Take, for instance, geo-based suggestions (like Google Places, Yahoo! Local, or Yelp), location-based social networks (like Gowalla, Foursquare, or Facebook Place), or recommendations for eateries.

### 3 Problem Statement

New innovations in mobile communication and information services are opening up exciting possibilities for location-based applications. By sharing their precise location with LBS providers, users can get a wealth of useful data. Maps and navigation, information services, and many more popular applications are available. A user's location and other personal details must be submitted to the providers of location-based services in order for them to work. For example, details about one's whereabouts and identity. The term "location privacy" describes the practice of ensuring that third parties cannot deduce a user's precise whereabouts. It is important that users' sensitive information be hidden from unauthorized individuals when communicating.

As users want more location-based information, location-based services are becoming more popular. The most effective approach for collaborative TTP free location privacy in LBS is the one in which users cooperate. Therefore, two of the most pressing problems now are system scalability and location privacy. By doing away with the weakness of the TTP-based method, the suggested method ensures privacy based on substantially more robust assumptions. Not only that, it offers great resilience against security and privacy assaults and has high fault tolerance. To ensure maximum privacy and security, it employs cryptographic methods. A low-cost, high-performance solution is required to guarantee LBS users' privacy while also improving scalability. Strong privacy with reduced processing cost and improved scalability is difficult to achieve with current computationally efficient and practical solutions.

#### 3.1 Objectives

The primary goal of this study is to find a way to make location-based services accessible to everyone without letting their location privacy be compromised. Better scalability at low cost is another benefit of the takeout method.

The following features are provided via an innovative solution that is discussed below.

Key reasons for the current study include keeping TTP free, improving scalability, reducing overall cost, enhancing privacy, enabling parallel execution, and avoiding collusion. No-Tax Partnership

One of the greatest schemas for location-based services that aims to eliminate trust assumptions is the TTP free schema. Everyone who is interested will be able to complete the assignment independently, without relying on a central server or trustworthy third party. Save Money

Lowering the total cost for LBS users is one of the primary goals. Finding the sweet spot between communication cost and computing cost is the major goal. Boost Performance

Improving the framework's overall execution is one of the primary goals. All of its processes ought to be running quickly, efficiently, and in parallel. Get scalability better

Therefore, scalability is a major concern. The primary goal is to expand the network in a more manageable way. Privacy

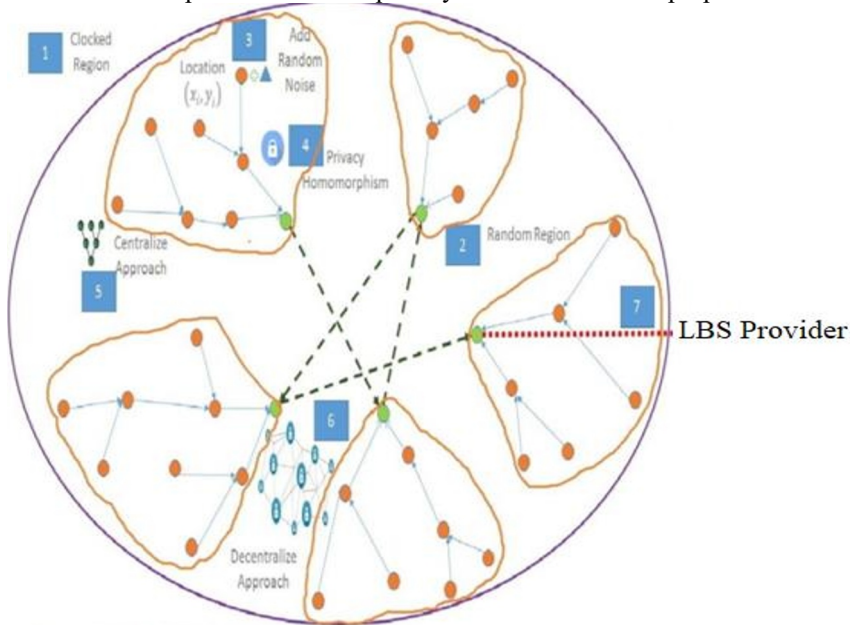
The utmost important concern is the privacy of LBS users. The user's sensitive information should not be inferable by malicious users. To ensure the security and privacy of LBS users, homomorphic encryption methods are utilized. Researching the best algorithms that provide the highest level of location privacy is crucial. Because of issues with collusion, the Collusion-Free Privacy Homomorphism has a loop hole. In order to make the framework secure and prevent collusion-free attacks, we need to devise a plan.

## 4 Proposed Methodology

We looked at the current methods for protecting users' privacy in location-based services. Methods can be either TTP-based [2] or TTP-free [3]. Providing location privacy for LBS users is a primary goal of most of the aforementioned techniques. When it comes to LBS, the main obstacle to its growing user base is meeting efficiency requirements and ensuring scalability. It is not uncommon for LBS users to collaborate in order to compute the tasks. In order to complete tasks such as secure data aggregation or secure sum, etc., all users involved must have faith in one another and work together. There was a proposal for a new method that would increase scalability while reducing costs, offer location privacy without transport tokens (TTP), and have high fault tolerance and resilience against privacy and security assaults.

### 4.1 Proposed Communication Schema

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



1. Finds No. of users in cloaked region
2. Create Sub Region using Optics - Density based clustering algorithms
3. All users add random noise in their current location
4. Each user will encrypt their location information using homomorphic encryption algorithm
5. Perform Secure Data Aggregation using privacy homomorphism (PH) using tree topology in each random region
6. Implement decentralize Random Chaining (RC) for all random region and compute the secure centroid C for cloaked area
7. LBS Provider P performs decryption on encrypted sum C and Find Centroid

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

Figure 1 shows the proposed hybrid strategy to communication between users and LBS providers. To begin, as illustrated in Figure 1 with label 2 and the orange circle, we create a subregion using an optics-density based clustering technique [6]. This subregion then allows us to run the algorithms in parallel. Line 8 of algorithm 1 calls Random Partition Function as part of Phase 1. In the second phase, labeled "3" (Line 9-16 in method 1), each user will alter their location data by inserting a secret, random split. This process is illustrated in Figure 1. As seen in Figure 1 (labeled 4, 5 with the blue line, which corresponds to Lines 17-22 in algorithm 1), in phase 3, every user will execute the safe sum of the locations within the random partition  $RP_i$  using the centralized method of privacy homomorphism (PH). Fig. 1 shows label 6, the green dotted line (Line 23-30 in algorithm 1), and the chosen location aggregator LA will use decentralize random selection (RS) to calculate an encrypted, safe sum of locations in phase 4. The final step in Phase-5 is for the LBS Provider, P, to decrypt the encrypted sum of location ESL and locate the secure centroid in the cloaked region, as seen in Figure 1 with label 7, the red dotted line representing Line 31-32 in system 1.

## 4.2 Proposed Algorithm

---

### Function 1: Random\_Partition\_Function ()

---

**INPUT:** location information of LBS User  $U_{i(x_i, y_i)}$ , Minimum number of User to form the cluster  $MU$ , Epsilon  $E$ ;

1. **OUTPUT:** Random Partition  $RP_i$ ;
  2. Set the Parameter  $MU = 2$  and  $E = 0.05$
  3. **for** (Every LBS User  $U_i$ ) **do**
  4. //Use Optics- Density Based Clustering Algorithm to formed the Cluster [25]
  5. Formed the Random Partition  $RP_i$ ;
  6. **end**
  7. **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**  $i = 1; i \leq \text{Random Partition } RP_i.\text{Level}; i++$  **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 Partition  $RP_i$   

$$Epk((x_{rp}, y_{rp})) = Epk((x_{rp}, y_{rp})) + Epk(\sum_{i=1}^n(x_i)), Epk(\sum_{i=1}^n(y_i)) + \dots;$$
8. **End**  
 Last, Location Aggregator  $LA$  will receive the encrypted sum of location information of the LBS users within their Random Partition  $RP_i$
9.  $ESP = Epk(x_{rp}, y_{rp}) = Epk(\sum_{i=1}^n(x_i)), Epk(\sum_{i=1}^n(y_i));$
10. **Return**  $ESP$ ;

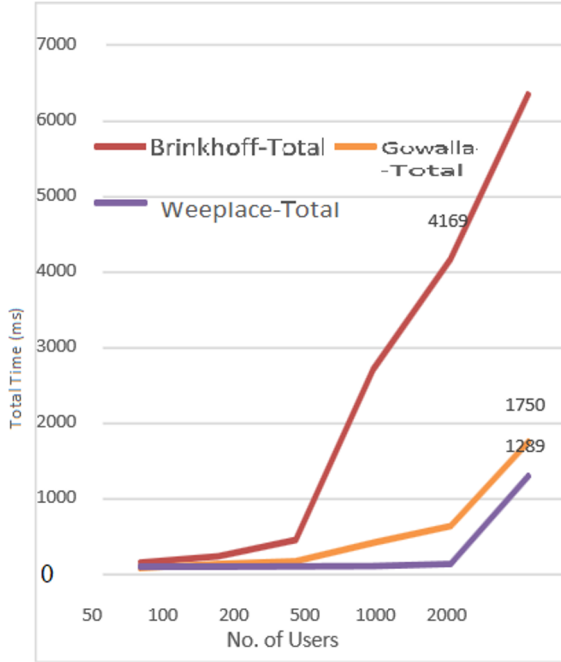
We employ a number of benchmark datasets, including those generated using the Brinckhoff network-based traffic generation simulator [103], the Gowalla datasets [112], and the Weeplace dataset [105].The Application for Testing

The application is tested for location-based services implemented in Java, as mentioned earlier. A number of modules, configurations, and interfaces are housed within this application. In order to evaluate the program, a few benchmark datasets are utilized. The number of user datasets that are interested in receiving location-based information is used for experimental reasons.

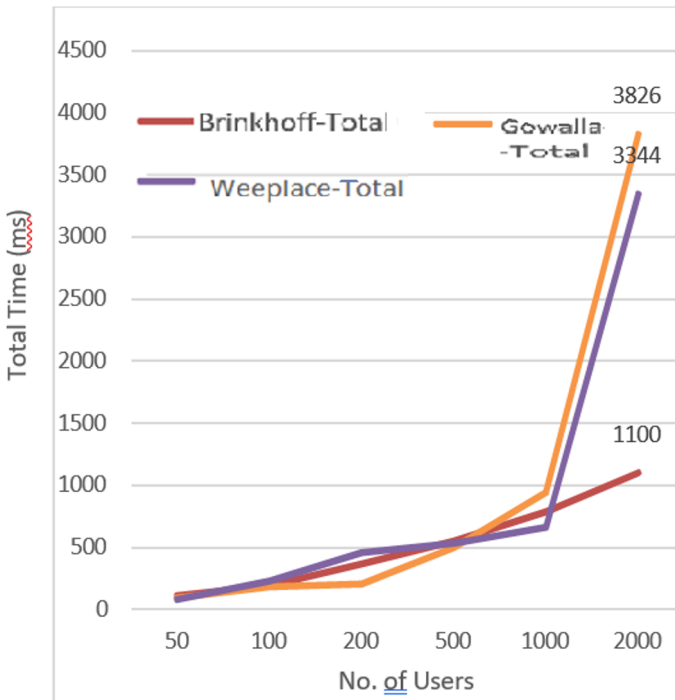
The total execution time of the suggested strategy must be known in order to conduct experimental evaluation, taking into account the time it takes to complete all phases.

**Table 1.** Result of various parameters of all three dataset

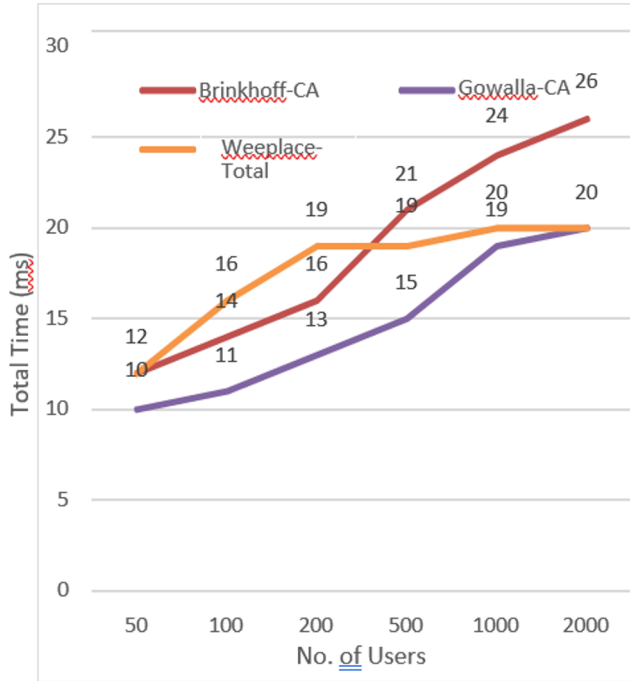
No of Users	Datasets	RR (ms)	SS&HE (ms)	DA (ms)	CA (ms)	Decryption Time (ms)	Total Time (ms)
50	Brinkhoff	112	144	1	12	10	279
100		192	229	1	14	10	436
200		367	444	1	16	10	828
500		551	2708	1	21	10	3281
1000		788	4169	1	24	10	4982
2000		1100	6352	2	26	11	7480
50		Gowalla	95	86	3	10	11
100	183		86	4	11	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	Wee Places		83	73	3	12	12
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



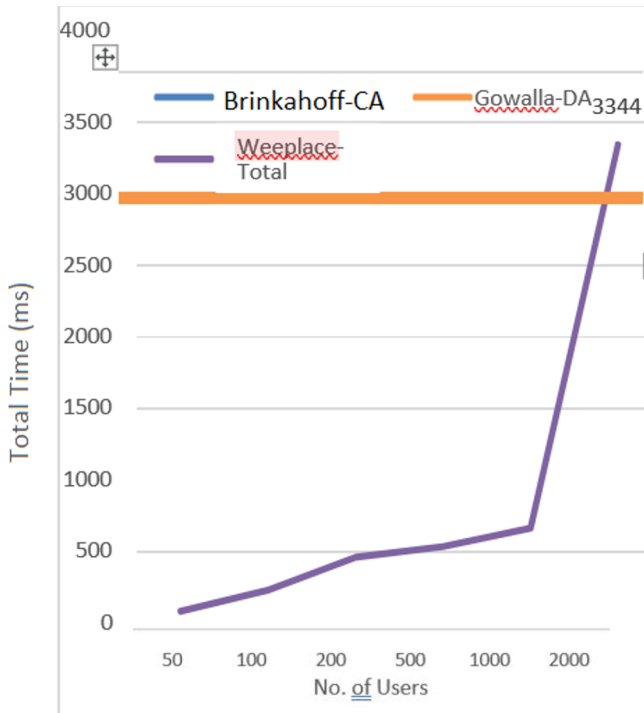
**Fig. 2.** Total Computational cost to create a random region with no. of encryption for all datasets.



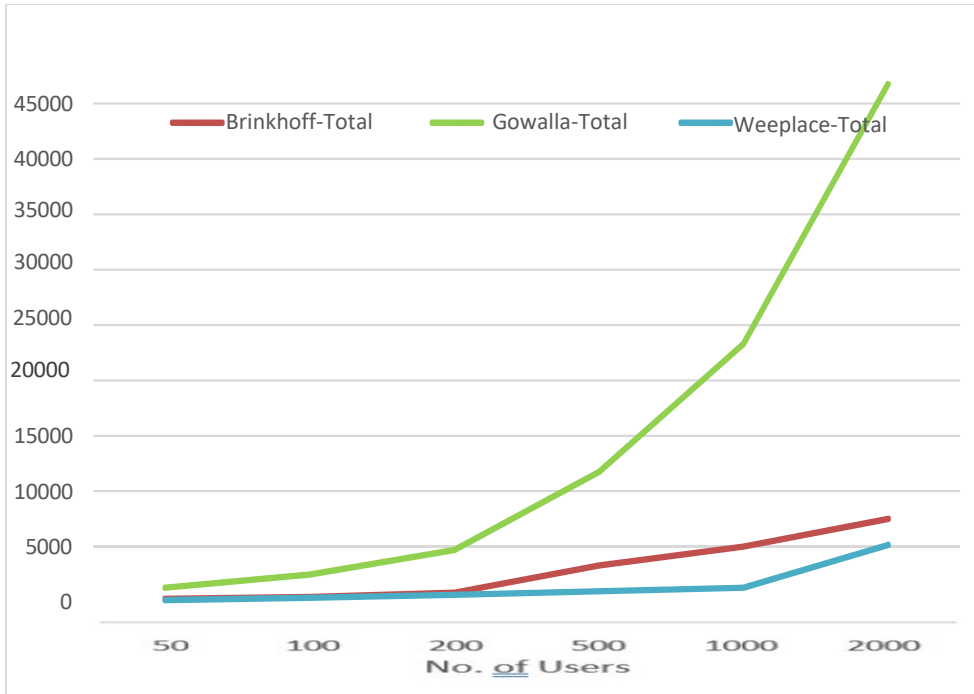
**Fig. 3.** Total Computational cost for random noise region with no. users for all datasets and homomorphic



**Fig. 4.** Perform a centralized approach using tree topology in each sub



**Fig. 5.** Total computational cost for decentralized random region all datasets. 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 reveals the overall time required to execute all the steps as specified by the algorithms. See in Fig. 6 how long it takes to compute the secured centroid on average across all datasets and user counts.

## 5 Conclusion

Service Provisioning through Location Many location-based services (LBS) applications, such as location-based social networking, location-based navigation, and location-based search, are booming in popularity and demand, and LBS holds great promise for these and other uses. Using a technique based on time-transfer packets (TTP) to protect the user's location. However, Trusted Third Party (TTP) links are not trustworthy since they could lead to harmful content. When it comes to cryptographic methods for protecting the location privacy of LBS users, a TTP-free collaborative approach is among the best options. All users collaborate in this method to complete tasks without involving any third parties (TTP). The main difficulty nowadays is providing consumers with privacy at a minimum cost, especially with the continuous expansion of LBS users. So, there's been a lot of work in the research community proposing and improving LBS user privacy in order to identify secure centroids. According to the study's results, no existing research offers user location privacy at a minimum cost while also improving scalability. Taking the aforementioned issue into account, we set out to conduct this research by presenting a fresh strategy for LBS that combines a hybrid method (combining centralized and decentralized components), secret sharing, clustering, and homomorphic encryption. The methods for locating secure centroids through secure data aggregation were proven through rigorous analysis, experimentation, and simulations. Using the features such as TTP free, parallel execution, reduced execution cost, support for scalability, lack of collusion, and enhanced

privacy of LBS users, the suggested methods are employed to locate secure centroid in cloaked regions through secure data aggregation in peer-to-peer collaborative mechanisms.

## Reference

1. Madhu, Bhukya, M. Venu Gopala Chari, Ramdas Vankdothu, Arun Kumar Silivery, and Veerender Aerranagula. "Intrusion detection models for IOT networks via deep learning approaches." *Measurement: Sensors* 25 (2023): 100641.
2. Madhu, Bhukya, and M. Venu Gopalachari. "Classification of the Severity of Attacks on Internet of Things Networks." In *Sentiment Analysis and Deep Learning: Proceedings of ICSADL 2022*, pp. 411-424. Singapore: Springer Nature Singapore, 2023.
3. Madhu, Bhukya, Sanjib Kumar Nayak, Veerender Aerranagula, E. Srinath, Mamidi Kiran Kumar, and Jitendra Kumar Gupta. "IoT Network Attack Severity Classification." In *E3S Web of Conferences*, vol. 430, p. 01152. EDP Sciences, 2023.
4. Madhu, Bhukya, Veerender Aerranagula, Riyaz Mahomad, V. Ravindernaik, K. Madhavi, and Gopal Krishna. "Techniques of Machine Learning for the Purpose of Predicting Diabetes Risk in PIMA Indians." In *E3S Web of Conferences*, vol. 430, p. 01151. EDP Sciences, 2023.
5. Silivery, Arun Kumar, Ram Mohan Rao Kovvur, Ramana Solleti, LK Suresh Kumar, and Bhukya Madhu. "A model for multi-attack classification to improve intrusion detection performance using deep learning approaches." *Measurement: Sensors* (2023): 100924.
6. Rakesh, S., Nagaratna P. Hegde, M. Venu Gopalachari, D. Jayaram, Bhukya Madhu, Mohd Abdul Hameed, Ramdas Vankdothu, and LK Suresh Kumar. "Moving object detection using modified GMM based background subtraction." *Measurement: Sensors* 30 (2023): 100898.
7. Madhu, Bhukya, M. Venu Gopala Chari, Ramdas Vankdothu, Arun Kumar Silivery, and Veerender Aerranagula. "Intrusion detection models for IOT networks via deep learning approaches." *Measurement: Sensors* 25 (2023): 100641.
8. Khan, Sarah, Quamrul Hassan, Kaushal Kumar, Saurav Dixit, Kshama Sharma, Vivek Kumar, Navdeep Dhaliwal, and Bhukya Madhu. "Modelling the Impact of Road Dust on Air Pollution: A Sustainable System Dynamics Approach." In *E3S Web of Conferences*, vol. 430, p. 01176. EDP Sciences, 2023.
9. Bhardwaj, Himanshi, Pooja Kapoor, Avnish Kumar, N. V. Ganapathi, and Bhukya Madhu. "Incorporating Sustainability: A Comprehensive Review of Factors Influencing Consumer Acceptance of Mobile Wallets." In *E3S Web of Conferences*, vol. 430, p. 01206. EDP Sciences, 2023.
10. Tumula S., Ramadevi Y., Padmalatha E., Kiran Kumar G., Venu Gopalachari M., Abualigah L., Chithaluru P., Kumar M., "An opportunistic energy-efficient dynamic self-configuration clustering algorithm in WSN-based IoT networks", (2024) *International Journal of Communication Systems*, 37 (1), art. no. e5633, DOI: 10.1002/dac.5633
11. Rajender N., Gopalachari M.V., "An efficient dimensionality reduction based on adaptive-GSM and transformer assisted classification for high dimensional data",

- (2024) International Journal of Information Technology (Singapore), 16 (1), pp. 403 - 416, DOI: 10.1007/s41870-023-01552-9
12. Gopalachari M.V., Kolla M., Mishra R.K., Tasneem Z., "Design and Implementation of Brain Tumor Segmentation and Detection Using a Novel Woelfel Filter and Morphological Segmentation", (2022) Complexity, 2022, art. no. 6985927, DOI: 10.1155/2022/6985927
  13. Kolla M., Mishra R.K., Zahoor Ul Huq S., Vijayalata Y., Gopalachari M.V., Siddiquee K., "CNN-Based Brain Tumor Detection Model Using Local Binary Pattern and Multilayered SVM Classifier", (2022), Computational Intelligence and Neuroscience, 2022, art. no. 9015778, DOI: 10.1155/2022/9015778
  14. Venu Gopalachari M., Gupta S., Rakesh S., Jayaram D., Venkateswara Rao P., "Aspect-based sentiment analysis on multi-domain reviews through word embedding", (2023) Journal of Intelligent Systems, 32 (1), DOI: 10.1515/jisys-2023-0001
  15. Mukkamula V.G., Nangunuri L, "Location aware social networks user profiling using big data analytics", (2017) International Journal of Intelligent Engineering and Systems, 10 (6), pp. 242 - 249, DOI:10.22266/ijies2017.1231.26
  16. Gopalachari M.V., Sammulal P., "A hybrid approach to handle cold start in a recommender by exploiting latent factors", (2016) International Journal of Applied Engineering Research, 11 (6), pp. 3905 – 3909
  17. Gopalachari M.V., "DBT recommender: Improved trustworthiness of ratings through de-biasing tendency of users", (2018) International Journal of Intelligent Engineering and Systems, 11 (2), pp. 85 - 92, DOI: 10.22266/IJIES2018.0430.10
  18. Vatambeti R., Divya N.S., Jalla H.R., Gopalachari M.V., Attack Detection Using a Lightweight Blockchain Based Elliptic Curve Digital Signature Algorithm in Cyber Systems, (2022) International Journal of Safety and Security Engineering, 12 (6), pp. 745 - 753, DOI:10.18280/ijssse.120611.
  19. Sammulal P., Venu Gopalachari M., "A personalized recommender system using conceptual dynamics", (2017) Advances in Intelligent Systems and Computing, 507, pp. 211 - 219, DOI: 10.1007/978-981-10-2471-9\_21
  20. Prathi J.K., Raparathi P.K., Gopalachari M.V., "Real-Time Aspect-Based Sentiment Analysis on Consumer Reviews", (2020) Advances in Intelligent Systems and Computing, 1079, pp. 801 - 810, DOI: 10.1007/978-981-15-1097-7\_67
  21. Venu Gopalachari M., Sammulal P., "Personalized collaborative filtering recommender system using domain knowledge", (2014) International Conference on Computing and Communication Technologies, ICCCT 2014, art. no. 7066693, DOI: 10.1109/ICCCT2.2014.7066693
  22. Venu Gopalachari M., Sammulal P., "Hybrid recommender system with conceptualization and temporal preferences", (2016) Advances in Intelligent Systems and Computing, 380, pp. 811 - 819, DOI: 10.1007/978-81-322-2523-2\_79
  23. Venu Gopalachari M., Sammulal P., "Personalized web page recommender system using integrated usage and content knowledge", (2015) Proceedings of 2014 IEEE International Conference on Advanced Communication, Control and Computing Technologies, ICACCCT 2014, art. no. 7019261, pp. 1066 - 1071, DOI:10.1109/ICACCCT.2014.7019261

24. Gopalachari M.V., Sammual P., Babu A.V., "Correlating scheduling and load balancing to achieve optimal performance from a cluster", (2009) 2009 IEEE International Advance Computing Conference, IACC 2009, art. no. 4809029, pp. 320 - 325, DOI: 10.1109/IADCC.2009.4809029
25. Kavati I., Kumar G.K., Gopalachari M.V., Babu E.S., Cheruku R., Reddy V.D., "Non-invertible Cancellable Template for Fingerprint Biometric", (2022) Lecture Notes in Networks and Systems, 420 LNNS, pp. 615 - 624, DOI: 10.1007/978-3-030-96305-7\_57
26. Pyaraka S.C.R., Lanka S.S., Konanki P., Venu Gopalachari M., Rakesh S., Jayaram D., "Review on 3D Model Generation Through Natural Language and Image Processing", (2023) Cognitive Science and Technology, Part F1466, pp. 311 - 317, DOI: 10.1007/978-981-99-2742-5\_33
27. Jayaram D., Rakesh S., Venu Gopalachari M., Gaddam S., Kranthi Kumar Reddy B., Pulluri P.S., "Student Monitoring System Using Deep Learning", (2023) Cognitive Science and Technology, Part F1466, pp. 467 - 474, DOI: 10.1007/978-981-99-2742-5\_48
28. Rakesh S., Venu Gopalachari M., Jayaram D., Gupta I., Agarwal K., Nishanth G., "A Review on Sign Language Recognition Techniques", (2023) Cognitive Science and Technology, Part F1466, pp. 301 - 309, DOI: 10.1007/978-981-99-2742-5\_32
29. Kiran Kumar G., Malathi Rani D., Venu Gopalachari M., Rakesh S., Ashraf S., "Melanoma Classification Using Convolutional Neural Network", (2023) AIP Conference Proceedings, 2754 (1), art. no. 070019, DOI: 10.1063/5.0162544
30. Rakesh S., Gopalachari M.V., Kumar G.K., Automatic music genre classification using deep learning, (2023) AIP Conference Proceedings, 2754 (1), art. no. 070012, DOI: 10.1063/5.0161104.