Virtual By-passing of Query Server for Privacy of Users for Continuous Location Based Services

P. Poornima, Mayur Vastari

***Abstract** – Location Based Services anticipate that customers should continually report their zone to a possibly untrusted server to get organizations reliant on their territory, which can open them to security risks. Tragically, existing security defending strategies for LBS have a couple of requirements, for instance, requiring a totally trusted in outcast, offering confined insurance confirmations and realizing high correspondence overhead. In this errand, A customer portrayed security organize structure called dynamic grid system (DGS) is proposed; the important sweeping structure that fulfills four central requirements for insurance shielding delineation and industrious LBS. The structure just requires a semi-trusted in outcast, at risk for doing clear planning undertakings viably. This semi-accepted pariah doesn't have any information about a customer's region. Secure delineation and steady zone assurance is guaranteed under the described enemy models. The correspondence cost for the customer doesn't depend upon the customer's optimal insurance level, it just depends upon the amount of huge central focuses in the area of the customer. Notwithstanding the way that the consideration is on range and k-nearest neighbor requests in this work, This structure can be easily connected with assistance other spatial inquiries without changing the estimations run by the semi-trusted in outcast and the database server, gave the essential interest an area of a spatial request can be engrossed into spatial regions. Experimental results show that the DGS is more productive than the best in class protection saving strategy for LBS.*

Keywords: Spatial Queries, Dynamic Grid System, Range Queries, Snapshot Queires.

I. INTRODUCTION

Location Based Services came about because of the combination of 3 advancements in a single gadget: versatile web access, situating and rich UIs. Until the late 1990's the accessible cell phones for the most part bolstered just voice and SMS and had not many UI capacities. Despite the fact that these advances could hypothetically as of now bolster exceptionally rough area based administrations (utilizing SMS and cell arrange based limitation), simply after the presentation of WAP and web access in cell phones there is updates on the principal by and large accessible area based services[1]. The 1999's Palm VII is viewed as the main LBS proficient cell phone in spite of the fact that the LBS applications it gave depended on postal district data to have the client situating. Additionally in 1999, WAP-empowered telephones begin to show up available giving web get to and more extravagant UIs than beforehand accessible.

The administration FriendZone is viewed as the principal LBS administration to be offered by a cell phone administrator in May 2001 after a primer preliminary that began in January 2001. The upgrades for UIs and the openness of mobile phones with significant standards contact screens made potential applications with increasingly excessive interfaces a portion of the time for all intents and purposes indistinguishable from PCs. From the start the zone was given by cell mastermind based limitation. With the availability of humble and little GNSS chipsets a consistently expanding number of mobiles are enabled.

At present, course progressions in client contraptions, for instance, PDAs are enabling a massive impact in region based organizations, with new advertisement openings reliant on the limit of customers to recognize their definite territory near with organizations, cordialities and others. The GNSS entrance in LBS contraptions of which 90% are mobile phones showed up at 20% in 2012. With the creating invasion of tablets and extended GNSS use in modernized cameras, the PDA offer will reduce all through the next decade, according to the appraisals gave by GNSS Market Report, Issue 3. Nevertheless, the general penetration is anticipated to augment as we continue depending on a creating number of compact applications for course, singular after, emergency calling, gaming, publicizing, social joint effort and general success. Likewise, the rising multi-star gathering GNSS recipients, as the GPS+Galileo mix will improve exactness and make new LBS openings. Timestamp and legitimacy of the leave.

Various other arranging systems and indoor arranging structures are open, especially for indoor use. GPS and GSM don't work very well inside, so various methods are used, including co-pilot reference point for CDMA frameworks, Bluetooth and Wi-Fi.

II. PROBLEM STATEMENT

The current situation with Location-Based Services is quite fearsome as the integrity of the security has been compromised several times due to the flaws within the existing system and high reliance on the Third-Party Organisations. These organisations acquire sensitive information which holds high value, Later there exists a threat of the Third Party organizations to be hacked against will and hence the a huge leak of personal data. This .paper intends to resolve that problem.

Revised Manuscript Received on June 25, 2020.

P. Poornima, Assistant Professor, Department of Computer Science and Engineering**,** Mahatma Gandhi Institute of Technology Hyderabad, India. E-mail: ppoornima_cse@mgit.ac.in

Mayur Vastari, Student, Department of Computer Science and Engineering**,** Mahatma Gandhi Institute of Technology Hyderabad, India. E-mail: mvastari_cse1605f8@mgit.ac.in

III. EXISTING AND PROPOSED SYSTEM

In this venture, a client characterized security network framework called dynamic lattice framework (DGS) to give a protection safeguarding preview and persistent LBS is proposed. The principle thought is to put a semi-confided in outsider, named Query Server (QS), between the client and the Service Provider (SP). QS just ought to be semi-confided considering the way that it won't accumulate/store or even methodology any customer territory information. Semi-trusted in this setting infers that while QS will endeavor to choose the region of a customer, it still precisely finishes the clear planning errands required in the show, i.e., it doesn't change or drop messages or make new messages. An untrusted QS would subjectively altered and droped messages just as infuse counterfeit messages, which is the reason the DGS relies upon a semi-confided in QS. In DGS, a Mobile User at first chooses a request locale, where the customer is pleasant to reveal how she is some spot inside this request zone. The request locale is isolated into proportional estimated grid cells reliant on the dynamic framework structure demonstrated by the customer. By then, the user scrambles a request that joins the information of the inquiry area and the dynamic system structure and encodes the character of each framework cell uniting the important chase zone of the spatial inquiry to convey a great deal of mixed identifiers.

IV. LITERATURE REVIEW

Table 1: Literature Review for User-Defined Privacy Grid

S.No.	Year	Name of Author	Title of Paper	Technique	Advantages	Disadvantages
[1]	Jul 2012	B. Bamba, Ling Liu, Peter Pesti, Ting Wang	Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid	Privacy Grid System	The experiment results based on a dataset of real network show the algorithm is effective and feasible.	Privacy leakage if attackers have knowledge about the grid structure
[2]	Jan 2015	Roman Schlegel, Chi-Yin Chow, Qiong Huang, Duncan S. Wong	User-Defined Privacy Grid System for Continuous Location-Based Services	Dynamic Grid System	DGS is more efficient than the state-of-the-art privacy-preserving technique for continuous LBS.	Complexity in implementation.
[3]	Nov 2017	Yuan Tian, Hai Liu, Zhenqiang Hu, Jing Hu	Enhanced Utility Approach for User-Centred Location Privacy Service.	Gaussian Distribution	Better for the User Location sharing precision	No Disadvantage

V. SYSTEM ARCHITECTURE AND FLOWCHART

The main background idea behind this paper is the transfer of encrypted cell identifiers only and not the location itself as shown in Fig 1. Among the modules involved, one of the most common and simplest is mobile use due to the existence of GPS. Intuitively, due to the overexposure, they tend to be hackable if the location resides with the middle-men, Hence the avoidance of location sharing. So, The grid system tends to hide the location all along and makes the location visible to the SP only after the main user's consent.

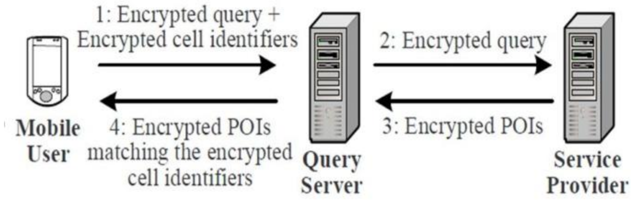


Fig. 1: Software Architecture of Proposed System.

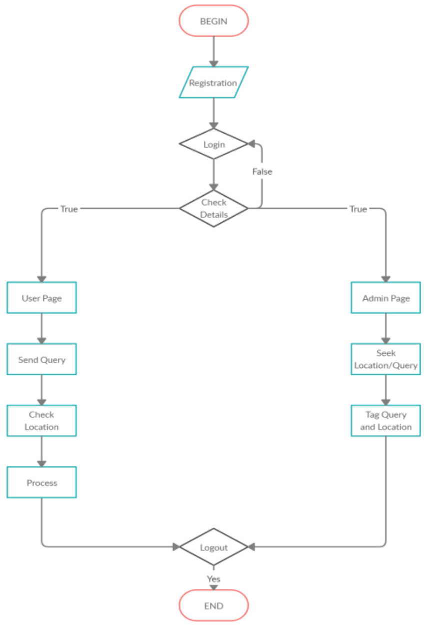


Fig. 2: Flowchart of the proposed System.

In the Fig 2, The flow chart depicts the working flow of the .paper for the two main actors, User and Admin, starting from the registration to showing the result for the user. The Diagram briefly shows the main features/responsibilities the actor has to perform while executing the paper. The User's main responsibility is to send a query along with the location in the form of hidden identifier keys whereas the admin is responsible for reciprocating the request made by the user, basically like a client-server mechanism.

VI. FEATURES

The Dynamic Grid System is completely user-defined, I.e The grid evolves/changes as per the users choice. For example The user can allocate the grid node to an area like
A9 - MGIT, Gandipet, Hyderabad
Z81- JNTUH, Kukatpally, Hyderabad
And accordingly the grid takes shape.
This way no two grids are the same and complete anonymity and privacy is achieved.This Grid System is the backbone of the whole project. The features of this paper are-Sign-Up: A user has to create an account as any of the 2 modules(Mobile User, QueryServer). Sign-In: The mobile user as well as the Query Server User has to login to access the services.Send Query: This feature allows the Mobile Users to send various queries.

Send Details: Can be accessed only by the Admin and the Query Server, It is a method to forward details to appropriate places without leaking the integrity of the privacy. Grid Result: Allows the Mobile User to get the confirmation about the location and displays the location over Google map.

1.MobileUser:-
Attributes:Send_Query,Grid_Location
Operations:Send_Query(),Grid_Location()
2.QueryServer:-
Attributes:Send_Details
Operations:Send_Details_ServiceProvider(),

VII. RESULTS

The Fig 3 , Shows the home page .

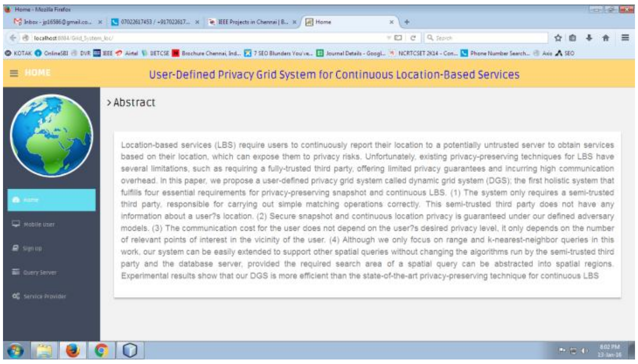


Fig. 3: Home Page.

The Fig 4, displays the Sign-In Page for the Mobile user, Seeking the User Name and the Password for Authentication of the User.

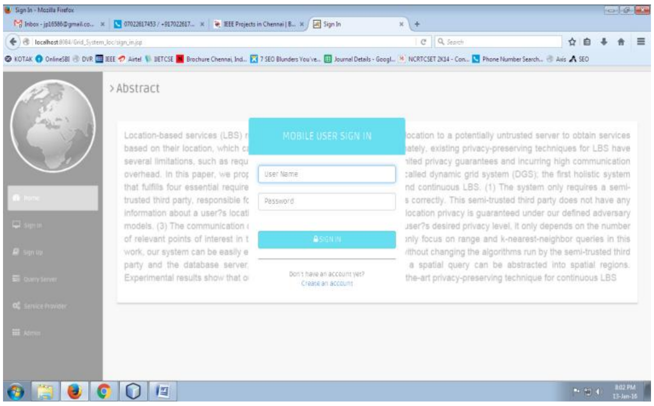


Fig. 4: Sign-In Page

Here, In Fig 5, it is seen that the location details in the form of an E-Key (Identifier), for maintaining the privacy, along with the User Name of the Mobile User is seen also there is an option of ‘Send Details’, Here the details are transferred from the Mobile User to the Service Provider. The Query Server acts as a Middle man in the whole User Location Transfer from user to Service Provider Operation.

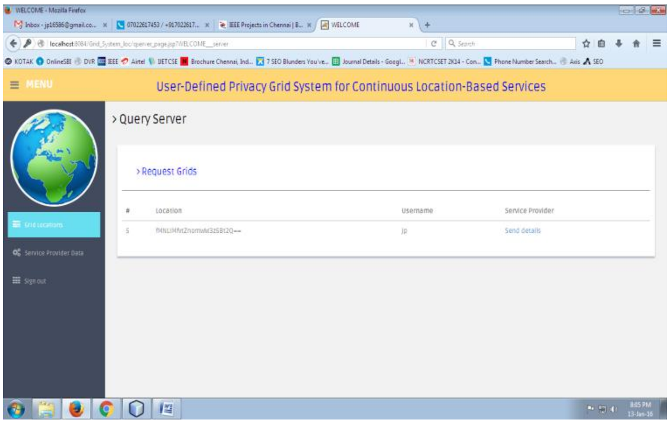


Fig.5: Query Server Request Page.

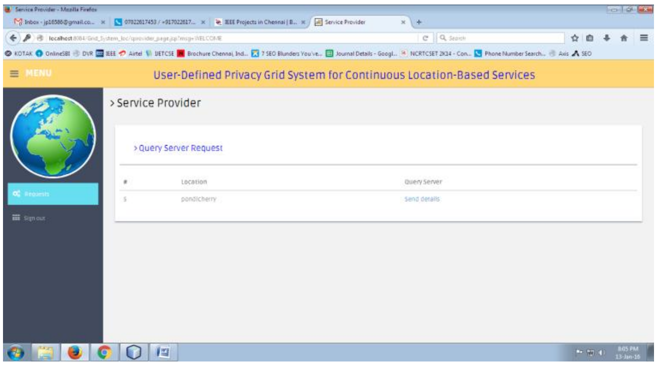
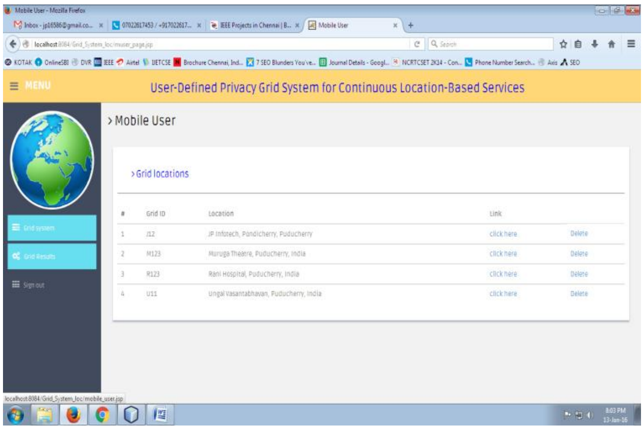


Fig 6: Service Provider Page.

In the above Fig 6, The Service Provider’s page is seen. The role of the Service provider is to tag the Query along with the location in reference to the grid, which is sent through the Query Server by the Mobile User. In order to preserve the privacy from the Partially Trusted Third-Party(Query Server), The Location Details are sent via a Unique Key Identifier know as the E-Location or E-Loc. This way the Location never comes out directly but with reference to Grid System.



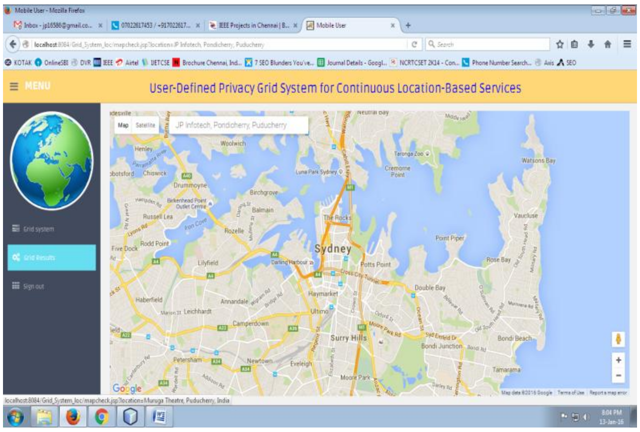


Fig 7: Results Page.

VIII. CONCLUSION

In this task, A powerful matrix framework (DGS) for giving security protecting nonstop LBS was proposed. The DGS incorporates the QS and the SP, and protection ensuring strategies to isolate the entire inquiry preparing task into two sections that are performed independently by QS and SP. DGS doesn't require any (TTP); rather, This approach requires just the a lot more vulnerable suspicion of no intrigue among QS and SP. The undertaking was additionally intended for productive conventions for DGS to help both consistent k-closest neighbor (NN) and range inquiries. To assess the presentation of DGS, it is contrasted with the cutting edge method requiring a TTP. DGS gives preferable protection ensures over the TTP plot, and the trial results show that DGS is significantly productive than the TTP }, as far as data cost is concerned. As far as calculation cost, DGS likewise consistently outflanks the TTP conspire for NN inquiries; it is tantamount or marginally more costly than the TTP plot for dynamic questions.

FUTURE SCOPE

This .paper can be further improvised by working on the security furthermore. Based on this concept the .paper can be implemented on Famous sites like Amazon, eBay, UrbanClap and more. Also, the .paper can further be improvised into a much faster working model with slight automation.

REFERENCES

1. B. Bamba, L. Liu, P. Pesti, and T.Wang, "Supporting anonymous location queries in mobile environments with PrivacyGrid," in *WWW*, 2008.
2. Roman Schlegel, Chi-Yin Chow, Qiong Huang, Duncan.S. Wong, "User Defined Privacy Grid System for Continuous Location Based Services," in *Jan*, 2015.
3. Yuan Tian, Hai Liu, Zhenqiang Hu, Jing Hu "Enhanced Utility Approach for User-Centred Location Privacy Service." in Nov,2017
4. M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in *ACM MobiSys*, 2003.
5. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," *IEEE TKDE*, vol. 19, no. 12, pp. 1719–1733, 2007.

AUTHORS PROFILE

Mrs P. Poornima, B.Tech(CSIT), M.Tech (CSE), has teaching experience of 15 years. Presently working as Asst Professor in Department of CSE, Mahatma Gandhi Institute of Technology, HYD. She has 6 research papers published in the International Journals of repute. Her research area consists of Image processing, Machine Learning, IoT, AI etc

Mr. Mayur Vastari, a Final year Student of Bachelors in Engineering in the field of Computer Science at Mahatma Gandhi Institute of Technology, Hyderabad. He has worked as an intern for several companies and has developed projects in the fields of IOT, Web Technologies, Java, Cloud Computing, etc. His areas of interests in research include Data Mining, Data Analytics, Web Technologies and IOT.