ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Privacy Preserving Location Based Services

S. Venkatachalam
MCA Student
CMR College of Engineering and Technology.

Ch.Dayakar Reddy, MCA, M.Tech, M.Phil, (Ph.D)
Professor and HoD of MCA,
CMR College of Engineeringand Technology.

Abstract:
Location-based services require users to continuously report their location to a potentially untrusted server to obtain services based on their location, which can expose them to privacy risks. The system only requires a semi-trusted third party, responsible for carrying out simple matching operations correctly. This semi-trusted third party does not have any information about a user's location. Although we only focus on range and k-nearest-neighbor queries in this work, our system can be easily extended to support other spatial queries without changing the algorithms

Index Terms: ***location privacy, Dynamic grid systems, k-anonymity, Security***

I.INTRODUCTION:

Location based services is valuable and users should be able to make use of them without having to give up their location privacy. A number of approaches have recently been proposed for preserving the user location privacy in Location based service. In general, these approaches can be classified into two main categories. Fully-trusted third party is the most popular privacy-preserving techniques require a trusted third party to be placed between the user and the service provider to hide the user's location information from the service provider.

The main task of the third party is keeping track of the exact location of all Users and blurring a querying user's location into a cloaked area thek-anonymity-based techniques only achieve low regional location privacy because cloaking a regional space to include k users in practice usually results in small cloaking areas. Private information retrieval or oblivious transfer. Although private information retrieval or oblivious transfer techniques do not require a third party, they incur a much higher communication overhead between the user and the service provider, requiring the transmission of much more information than the user actually needs. A user-defined privacy grid system called dynamic grid system to provide privacy-preserving snapshot and continuous LBS. The main idea is to place a semi trusted third party, termed query server, between the user and the service provider. Query server only needs to be semi-trusted because it will not collect/store or even have access to any user location information. There are also many location based services being used but all the techniques doesn't gives the privacy preserving for the user .In this project, the user is given the privacy to access and view the location to the another user with the encrpt and decrypt concept .

II.ARCHITECTURE:

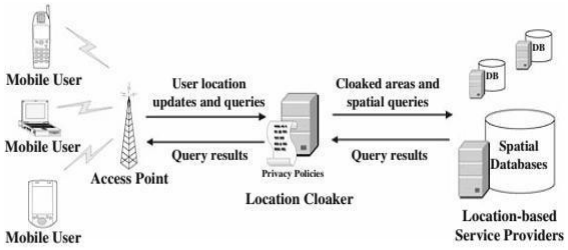

Fig 2.1 architecture diagram between multiple users

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The Above Diagram tells about how this project is executed between multiple users through the access point connected to the location cloaker which has the spatial database with which the service is being given to the users.

PROCESS FLOW DIAGRAM:

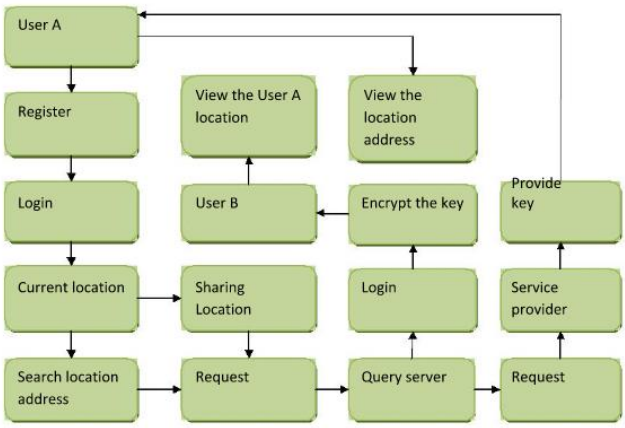

Fig 2.2 Process flow diagram between multiple users using service provider.

In the above diagram, user A register and logs in to the system then enters the current location and then gives the location address to the query server and the request is sent to the service provider he sends the key to the ACCESS the location to user A .The user A only has the full details about the encrypt function and will pass to User B for the Decryption process.

III.PROPOED SYSTEM:

We propose a user-defined privacy grid system called dynamic grid system (DGS) to provide privacy-preserving snapshot and continuous LBS. The main idea is to place a semi trusted third party, termed query server (QS), between the user and the service provider (SP). QS Only needs to be semi-trusted because it will not collect/store or even have access to any user location information. Semi-trusted in this context means that while QS will try to determine the location of a user, it still correctly carries out the simple matching operations required in the protocol, i.e., it does not modify or drop messages or create new messages. Finally, we described the Privacy Grid System framework which allows users to express their privacy requirements in terms of location hiding and POIs measures to control query processing overheads.

ADVANTAGES:

1. We provide more security to user location details. It is possible by a semi-trusted query server (QS) located between users and service providers and
2. We remove Trusted Third Party (TTP).

Low communication cost of Dynamic Grid System (DGS) for the user does not depend on the user-specified query area size. It only depends on the number of POIs in the grid cells overlapping with a query's required search area.

IV.EXISTING SYSTEM:

As a result of recent technological advances, mobile devices with significant computational abilities, gigabytes of storage capacity, and wireless communication capabilities have become increasingly popular. In addition, positioning techniques are embedded into more and more mobile devices. Based on these advances, new mobile applications allow users to issue location-dependent queries in a ubiquitous manner. With rapid advances in mobile communication technologies and continued price reduction of location tracking devices, location-based services (LBSs) are widely recognized as an important feature of the future computing environment. Though LBSs provide many new opportunities, the ability to locate mobile users also presents new threats − the intrusion of location privacy. Location privacy is defined as the ability to prevent unauthorized parties from learning one's current or past location. Location privacy threats refer to the risk that an adversary can obtain unauthorized access to raw location data derived or computed location information by locating a transmitting device, hijacking the location transmission channel and identifying the subject using the device. For example, location information can be used to spam users with unwanted advertisements or to learn about users' medical conditions, unpopular political or religious views.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Inferences can be drawn from visits to clinics, doctor's offices, entertainment clubs or political events. Public location information can lead to physical harm, such as stalking or domestic abuse.

DISADVANTAGES:

1. There is no security to user Location information.
2. Continuously expanding cloaked areas substantially increases in-efficiency of the query processing.
3. Privacy Leakage occurred by Third Party, means Third Party knows the exact location of every user.
4. Hacking can Also take place without Privacy.

V.MODULES:

User authentication:

Data owner has a collection of documents that he wants to outsource to the cloud server in encrypted form while still keeping the capability. In our scheme, the data owner firstly builds a secure searchable tree index from document collection, and then generates an encrypted document collection. The data owner outsources the encrypted collection and the secure index to the cloud server, and securely distributes the key information of trapdoor generation and document decryption to the authorized data users. In this module the User have to register first, then only he/she has to access the data base. After registration the user can login to the site. The authorization and authentication process facilitates the system to protect itself and besides it protects the whole mechanism from unauthorized usage. The Registration involves in getting the details of the users who wants to use this application.

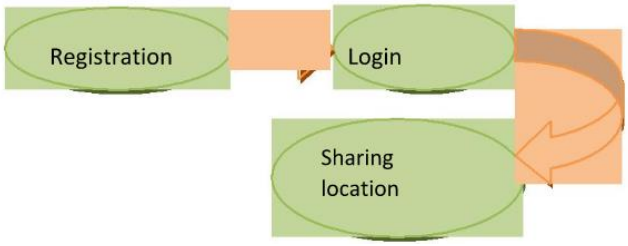

Fig5.1 User Authentication Query Processing:

This module allows admin verify the user requests and check the user request is contain in our database or not. If the database contains the user requests to calculate the range (Distance) value, and then send response to the appropriate values, suppose the request doesn't contain in the database send response is „Record Not Found" that query sent to the particular user.

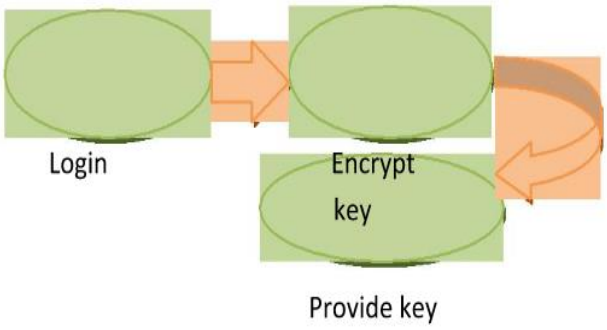

Fig 5.2 Query

Processing Mobile Users:

All users are mobile and travel on the underlying network and they also hold privacy policies which specify the privacy requirements of each user. The objective of this project is to provide the privacy to the user using friend list and to avoid the users outside the list.

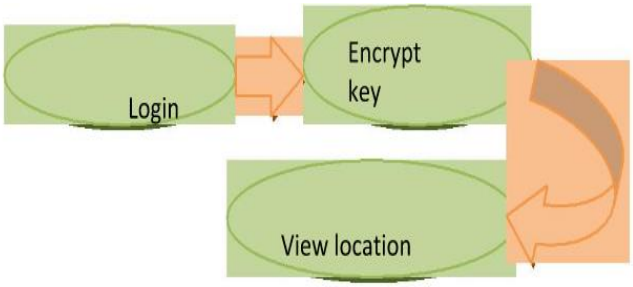

Fig 5.3 Mobile User

Location Cloaker:

The location Cloaker is an intermediate agent which can be trusted by mobile users. The location Cloaker receives continuous location updates from mobile users. In this we propose to explore historical locations that is also known as food prints. When a user request a location, his/her location is reported to the service provider. An another drawback of users location's area information can be overcome by location cloaker by foot print technique.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

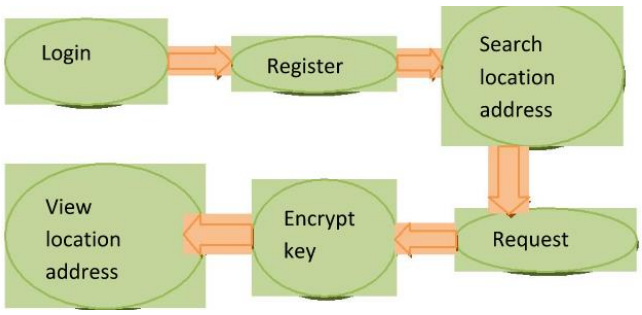

Fig5.4 Location cloaker

Location-Based Service Provider:

Location-based service providers play the role of spatial data maintainers and spatial query processors in our system. In order to handle privacy protected spatial queries, location-based service providers implement privacy protected query processors in their databases

VI.PERFORMANCEMEASURES:

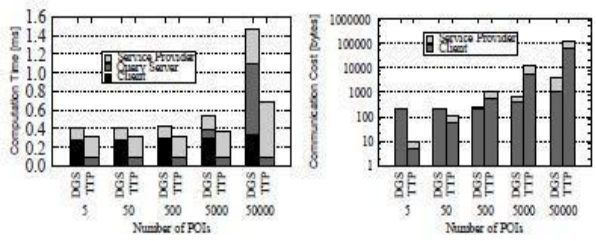

Fig 6.1 Number of POIs

The performance measure shows that the magnitude varies from 5-50,000.The result shows that DGS outperforms TTP. The Computation cost of DGS slightly greater than TTP.

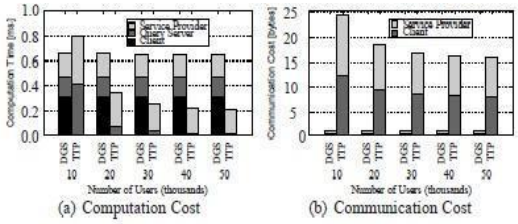

Fig6.2 No Of Mobile users

The result shows that DGS as Independent no of users while TTP heavily depends on the user identity.So the DGS as Desirable Privacy features For privacy preserving for location based services.

Dynamic grid system (dgs)

In this section, we will describe how our DGS supports privacy preserving continuous range and k-NN queries. This section is organized as follows: Section 3.1 describes the details of our DGS for processing continuous range queries and incrementally maintaining their answers, and Section 3.2 extends DGS to support k-NN queries.

Range Queries:

Our DGS has two main phases for privacy-preserving continuous range query processing. The first phase finds an initial answer for a range query and the second phase incrementally maintains the query answer based on the user's location update. Range Query Processing a continuous range query is defined as keeping track of the POIs within a user-specified distance Range of the user's current location (xu, yu) for a certain time period. In general, the privacy-preserving range query processing protocol has six main steps.

Step 1.Dynamic grid structure (by the user).The idea of this step is to construct a dynamic grid structure specified by the user. A querying user first specifies a query area, where the user is comfortable to reveal the fact that she is located somewhere within that query area. The query area is assumed to be a rectangular area, represented by the coordinates of its bottom-left vertex (xb, yb) and top-right vertex (xt, yt).

Step 2.Request generation (by the user).In this step, the querying user generates a request that includes (1) a query for a SP specified by the querying user and (2) a set of encrypted identifiers, Se, for aQS. The user first selects a random key K and derives three distinct keys:

(HK,EK,MK) ← KDF(K) (1) where KDF(•) is a key

derivation function ([24]). Then, the user sets query and Se.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Step 3. Request processing (by QS).When QS receives therequest from the user, it simply stores the set of encrypted identifiers Se and forwards the encrypted query to SP specified by the user.

Step 4. Query processing (by SP). SP decrypts the requestto retrieve the POI-type, the random key K selected by the user in the request generation step (Step 2), and the query area defined by m, (xb, yb), and (xt, yt). SP then selects a set of np POIs that match the required POI-type within the user specified query area from its database. For each selected POI j with a location (xj,yj)) ($1 \leq j \leq np$), SP computes the identity of the grid cell in the user specified dynamic grid structure covering j by (cj, rj) = _j xj−xb (xt−xb)/mk, j yj−yb (yt−yb)/mk_.

Step 5. Encrypted identifier matching (by QS).Upon receiving np triples, QS determines the set of matching POIs by comparing the encrypted identifiers Cj ($1 \leq j \leq np$) of the received POI with the set of encrypted identifiers Se previously received from the user. A match between a Cj and some Ci in the set Se indicates that the POI j is in one of the grid cells required by the user. Thus, QS forwards every matching POI hlj,σjito the user. If the query is a snapshot query, QS then deletes the received POIs and their encrypted identifiers. However, if the query is a continuous one, QS keeps the received POIs along with their encrypted identifiers until the user unregisters the query.

Step 6. Answer computation (by the user). Suppose that there are μ matched POIs received by the user. For each of these matched POIs, say hlj,σji, the user decrypts lj using EK and gets access to the exact location (xj, yj) of the POI. From (xj,yj) and lj, the user verifies σj by re-calculating the MAC value and compares it against σj . If they match, the user finds the answer that includes the POI whose location is within a distance of Range of the user's current position

(xu, yu).

K-Nearest-Neighbor Query Processing:

A continuous k-NN query is defined as keeping track of the k nearest POIs to a user's current location (xu, yu) for a certain time period, as presented in Section 2. In general, the privacy preserving k-NN query processing has six major steps to find an initial query answer.

Step 1. Dynamic grid structure (by the user).This step is the same as the dynamic grid structure step (Step 1) in the range query processing phase. It takes a user-specified query area with a left-bottom vertex (xb, yb) and a right-top vertex (xt, yt) and divides the query area into m × m equal-sized cells.

Step 2. Request generation (by the user).The required search area of the k-NN query is initially unknown to the user. The user first finds at least k POIs to compute the required search area as a circular area centered at the user's location with a radius of a distance from the user to the k-th nearest known POI. The user therefore first attempts to get the nearby POIs from a specific SP. In this step, the user requests the POIs in the cell containing the user and its neighboring cells from SP. Given the user' s current location (xu, yu) and a query area specified by the user in Step 1, she wants to get the POIs within a set of grid cells Sc that includes the cell containing herself, i.e., (cu, ru) = _j xu−xb (xt−xb)/mk , j yu−yb (yt−yb)/mk_, and its at most eight neighboring cells (cu −1, ru−1), (cu, ru−1), (cu+1, ru−1), (cu − 1, ru), (cu + 1, ru), (cu − 1, ru + 1), (cu, ru + 1), and (cu + 1, ru + 1). For each cell i in Sc, the user generates an encrypted identifier Ci using Equations 3 and 4, as in the request generation step (Step 2) in the range query processing phase. The user also creates a query to be sent to SP. Finally, the user sends a request, which includes the identity of SP, the query, and the set of encrypted identifiers (in random order), to QS.

Step 3. Request processing (by QS).This step is identical to Step 3 for range queries in the query processing phase.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Step 4. Query processing (by SP). This step is identical to Step 4 for range queries in the query processing phase Thanks to this query abstraction feature, our DGS can be easily extended to support other continuous spatial query types, e.g., reverse NN queries and density queries.

Step 5. Required search area (by the user and QS). This step is similar to the encrypted identifier matching step (Step 5) for range queries in the query processing phase, with the difference that this step may involve several rounds of interaction between the user and QS. QS Matches the encrypted identifiers of the encrypted POIs returned by SP with the encrypted identifiers in Se sent by the user in Step 2, and sends the matching encrypted POIs to the user.

Privacy Against Service Provider (SP):

We require that SP cannot learn the user's location any better than making a random guess. Formally, we consider the following game played between a challenger C and a (malicious) SP, denoted by A. The challenger prepares the system parameters, and gives them to A. A specifies a POI-type, the grid structure, a query area and two locations (x0, y0) and (x1, y1) in this area, and gives them to C. C chooses at random b ∈ {0, 1}, uses (xb, yb), the specified grid structure and POI-type to generate Msgb 2 with respect to the identity of A, i.e., the message that the malicious SP expects to receive. C then gives Msgb 2 to A. A outputs a bit b′ and wins the game if b′ = b.

Privacy Against Query Server (QS):

This requires that QS cannot tell from the user's request or SP's transcript about where the user is, provided that it does not collude with the intended SP. Formally, we consider the following game played between an adversary A (which is the dishonest QS) and a challenger C which acts the roles of the user and service providers. Given the system parameters, A begins to issue Private Key Query for polynomially many times: it submits the identity of a SP to C, and receives the corresponding private key. This models the case that QS colludes with a (non-intended) SP. A then specifies the POI-type, he identity of the intended SP (the private key of which has not been queried), the grid structure, a query area, and two user locations (x0, y0) and (x1, y1) in the query area, and gives them to C. C tosses a coin b ∈ {0, 1}, and uses (xb, yb) and the other information specified by A to generate Msgb 1 as the user's message to

QS, and the corresponding SP message Msgb 3. It sends both Msgb 1 and Msgb 3 to A. A continues to issue queries as above except that it cannot ask for the private key of the intended SP. Finally, A outputs a bit b′ as its guess of b, and wins the game if b′= b. These are the major concepts that are being followed in our privacy preserving techniques for the continuous location based services.

VII.CONCLUSION

In our paper we proposed a dynamic grid system for location based services. Our DGS have query processor, service provider and Cryptographic functions that divides the whole query processing into small no of divisions. DGS does not require fully trusted third party instead we have no collision between the QS and service provider. We also provide the efficient protocols for k-nearest neighbor.

VIII. FUTURE WORK

To evaluate the performance of DGS, we compare it to the state-of-the-art technique requiring a TTP. DGS provides better privacy guarantees than the TTP scheme, and the experimental results show that DGS is an order of magnitude more efficient than the TTP scheme, in terms of communication cost. In terms of computation cost, DGS also always outperforms the TTP scheme for NN queries; it is comparable or slightly more expensive than the TTP scheme for range queries.

VI. REFERENCES

[1]B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity.

[2]Architecture and algorithms, IEEE TMC, vol. 7, no. 1, pp.1–18, 2008.

[3]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.

[4]M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, "Efficient location Oblivious augmented maps: Location-based services with a payment Broker", in PET. 2007.

[5]R. Vishwanathan and Y. Huang, "A two-level protocol to answer private location-based queries", in ISI, 2009.

[6]A. Menezes, M. Qu, and S. Vanstone, "Some new key agreement protocols providing mutual implicit authentication," in SAC, 1995.

[7]A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "Providing k-anonymity in location based services," SIGKDD Explor.Newsl., vol.12, pp. 3–10, November 2010.

[8]D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO, 2001.

[9]R. Dingledine, N. Mathewson, and P. Syverson, "Tor: the second-generation onion router," in USENIX Security, 2004.

[10]G. Bissias, M. Liberatore, D. Jensen, and B. Levine, "Privacy vulnerabilities in encrypted HTTP streams," in PET, 2006.

Author Details

S.Venkatachalam, received her graduation degree in B. Sc – Computer science from St.Joseph's Autonomous College affiliated to Bharathidassan University for the year 2010-2013. Pursuing post graduate degree MCA from CMR College of Engineering and Technology affiliated to Jawaharlal Nehru Technological University, Hyderabad for the year 2013-2016.

CH. Dayakar Reddy, MCA, M. Tech, MPhil, (PhD) received his MCA from Osmania University and M. Tech from Jawaharlal Nehru Technological University, Hyderabad. MPhil from Periyar University and pursuing PhD in Nagarjuna University.