A SURVEY ON CONTINUOUS LOCATION BASED SERVICES USING USER-DEFINED PRIVACY GRID SYSTEM

SIRISHA KATLA*, Mr.SHAIK MOHAMMED SHAFIULLA**

PG SCHOLAR*,ASSISTANT PROFESSOR**

DEPARTMENT OF CSE, SCIENT INSTITUTE OF TECHNOLOGY, HYDERABAD

ABSTRACT: The number of mobile users who are using Location Based Services (LBS) are increasing day by day. To use Location Based Services, the users must report their exact location to the server. This may lead the user to risk his/her location privacy. The existing privacy preserving techniques for LBS has their own limitations. They use a Fully Trusted Third Party which doesn't guarantee any privacy and incur high communication overhead for each query. In this paper, we propose a user-defined privacy grid system called Dynamic Grid System (DGS). Dynamic Grid System satisfies four key needs for privacy-preserving snapshot and continuous LBS: (1) This is a semi-trusted third party and doesn't store any information related to location of the user. (2) Snapshot is secured and privacy of user location is guaranteed. (3) The value of communication depends only on the number of relevant Point of Interests (PoI). (4) We used range queries and k-nearest neighbour queries during this work. This system supports different spatial queries. We can show that DGS can give more location privacy and is more effective than the traditional privacy-preserving techniques.

I. INTRODUCTION In today's world, it is simple task for a person to know his/her location with the help of gadgets which contain GPS facility. If the user's vicinity is provided to Location-Based services (LBS), it's feasible to user to understand all vicinity based knowledge like location of friends or Nearest Restaurant. The significant use of cell gadgets create a path in which for the production of wireless networks that can be utilized to trade knowledge established on places. When the alternate of place understanding is finished amongst untrusted events, the privacy of the person might be in detrimental. Current protocol does not work on many extraordinary cellular gadgets and one other issue is that, Local Server (LS) must provide deceptive knowledge to consumer. In up to date years there has been a dramatic broaden within the quantity of mobile gadgets querying area servers for

expertise about POIs. Among many difficult obstacles to the broad deployment of such utility, privacy assurance is a predominant hassle. Location-based services (LBS) require customers to regularly file their vicinity to a probably untrusted server to acquire offerings headquartered on their location, which will put them in privacy dangers. Unfortunately, existing privacy keeping methods for LBS have a couple of obstacles, akin to requiring an utterlydepended on third party, providing confined privacy ensures and incurring excessive conversation overhead. Mobile protection checking out is becoming a pressing and essential study area because of the explosive increase of cellular app downloads and mobile customers. Now, location based function offerings in mobile apps no longer simplest enhance cell user experience, but additionally carry new challenges and disorders in application trying out and data protection. This paper specializes in location-based checking out disorders, assault prevention for mobile apps, and proposes a new monitoring and shopping model. This paper puts forward a user-defined privacy grid known as Dynamic Grid System (DGS) to provide privacy-preserving photograph and continuous LBS. The major concept is to position a semidepended on third party, termed Query Server (QS), between person and Service Provider (SP). QS wants to be semidepended on given that it will no longer collect/store or even have entry to any person vicinity expertise. Semi-depended in this context means that on that moment QS will try to investigate the place of a consumer, it still effectively carries out straight forward matching operations required within the protocol. Untrusted QS would randomly regulate and drop messages as good as inject fake messages, which is why our approach depends on semi trusted QS.

II. RELATED WORK

A. Supporting Anonymous Location Queries in Mobile Environments with Privacy Grid This paper introduces us to Privacy Grid − a framework which supports anonymous queries based on location in Service providers which provide location based services. This framework offers the following features: (1) It provides location P3P model i.e., location privacy protection preference profile model. In this model, mobile users can define their own location privacy requirements related to location hiding measures and location service quality measures. Examples of location hiding

measures are location k-anonymity and location l-diversity and examples of location service quality measures are maximum temporal and spatial resolution. (2) In some mobile environment, the privacy grid framework provides quick and reliable algorithms for location k-anonymity and location l-diversity. To achieve high anonymity success rate and reliability in time complexity and maintenance cost is the goal of this framework. A new method is developed by combining the advantages of top-down and bottom-up cloaking methods to reduce the anonymization time. (3) In this framework, location cloaking uses temporal cloaking which increases the chance of success for location anonymization. Privacy grid mechanisms are also discussed. Privacy requirements like location hiding and QOS measures can be expressed by the users in this framework. Three grid-based dynamic spatial cloaking algorithms are developed to provide location ldiversity and location k-anonymity. The experimental evaluation shows that this framework provides much higher anonymization success rate and are highly efficient in time complexity and cost.

B. Trajectory Privacy in Location Based Services and Data Publication Now-a-days, every mobile device has a access to GPS facility and internet connectivity. Due to this development of Location Based Services(LBS) resulted. We can search for nearby restaurants, hospitals and we can monitor the traffic using LBS. LBS can provide valuable services to the users but revealing the location of the user to untrustworthy Service Providers(SP) may pose a serious threat to user location privacy. Two modes of LBS are present. They are: (1) Snapshot LBS- the mobile user will check-in its current location to the SP once to get the required information. (2) Continuous LBS- the mobile user has to report its location in a periodic or on-demand manner to the SP to get its required continuous LBS. Continuous LBS is more challenging than snapshot LBS because the attackers may use temporal and spatial correlations to know the user's location with high certainity. The location samples used to know the user location is called the location trajectory. However, if location trajectories are published to public or third party for data analysis, it may cause serious privacy issues. Protection of privacy in continuous LBS and publication of location trajectory data has drawn the attention of research industry and community. In the current paper, we give an overview about state-of-the-art privacy preserving methods. In near future, more efficient and effective privacy preserving

technologies will be developed. Personalized LBS need more user semantics, an attacker may use this user semantics to know the user location. Hence, new privacy-preserving techniques must be developed to protect personalized LBS.

C. A Clustering Based Location Privacy Protection Scheme for Pervasive Computing In pervasive computational environments, the Location Based Services (LBS) are increasing day by day. The wide deployment of LBSs can affect the privacy related to mobile users location. Very important issue is to provide privacy methods for location privacy of mobile users from being attacked by attackers. in this paper we proposes a new technique for protecting location privacy. Location Kanonymity for a wide number of mobile users with their required anonymity levels by clustering is supported by this approach. To calculate Minimum Bounding Rectangle (MBR) the area in which users is put into clusters. MBR replaces the exact user location. Privacy analysis shows that this approach achieves high resilience to privacy threats of location and more privacy can be provided than expectations of users. This paper proposes a location privacy preserving technique for pervasive computing environment named Cluster Cloak. This approach protects location privacy with personalized K-anonymity. It also satisfies the privacy and QOS requirements of the mobile users. TTP adopted Cluster Cloak. When users move from one domain to another domain clusters can be adjusted. The theoretical and experimental analysis shows that this approach can provide more accurate QOS, more robustness, more privacy and lower complexity.

D. PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems Mobile users having GPS can use Location Based Services (LBS), also request query about points of interest in their range. Privacy and confidentiality are essential factors for the success of this type of applications. Encryption safeguards system from eavesdroppers but the queries may giveaway the location and identity of the user. Recently, centralized architectures have been put forward depending on K-anonymity. K-anonymity uses an buffer anonymizer among the mobile users and the LBS. However, all users must update their current locations continuously. If the anonymizer is compromised security threat occurs. Two issues are addressed in this paper : (i) current methods may not to give spatial anonymity of user locations and a novel technique is described to solve this

problem. (ii) PRIVE is proposed. It is a decentralized architecture to protect the anonymity of users by issuing LBS with spatial queries. PRIVE overcomes the disadvantages of centralized methods in anonymization and location updates. Moreover, the state of the system is distributed in between many of users, leaving PRIVE vulnerable to attacks. In deepth experimental studies show that PRIVE is applicable to real-life situations with so many mobile users. In the current paper, PRIVE is introduced which is a distributed system of anonymization of query in LBS. In PRIVE, mobile users issue location-based queries. They also organize themselves into a hierarchical overlay network and queries are anonymized in a fully decentralized fashion. hilbASR anonymization technique is supported by PRIVE . hilbASR guarantees anonymity under any user distribution. Experimental analysis show that this system is scalable, efficient, fault tolerant and achieves load balancing.

E. Providing K-anonymity in Location Based Services Anonymity among the relational databases has increased in the last decade. Different types of solution approaches have been used to solve this problem. K-anonymity has received a lot of attention and was thoroughly studied. New methods of data capturing user movement opens a path for offering better services such as Location Based Services (LBS). Concrete methods are required to safeguard the anonymity related to the mobile users while requesting LBSs. A survey has been conducted on new advancements of the giving of K-anonymity in LBS. Most of the methods depend on a reliable server component- that acts as mediator between the end user and the service provider- to protect the anonymity of the former user. Existing methods are divided into these categories: (a) historical K-anonymity (b) location K-anonymity (c) trajectory K-anonymity. We present the most prevalent methodologies from all categories and highlight their operations. This paper presents a survey on the state-of-the-art centralized K-anonymity approaches which offer privacy in LBSs. The aim of the presented methodologies is to preserve the location of the mobile users who request for LBSs in both static and continuous queries. A new and very important research regards K-anonymity methodologies which safeguard the user query along with the location of user.

F. Dynamic Grid System for Continuous Location Based Services Location-Based

Services(LBS) require the mobile users to provide an intimation of their location to a Service Provider to obtain services related to their proximity. This can lead them to risking their privacy. Existing privacypreserving methods for LBS contains certain limitations. It uses a genuine third party. Fully trusted third party gives a less privacy guarantee and it incurs high communication overhead for a query. This paper put forward a user-defined privacy grid system called as dynamic grid system(DGS). This is the first system which satisfies four necessary requirements for privacy-preserving snapshot and continuous LBS. (1) This system uses a semi-trusted third party which carries out matching operations between user and Service Provider. This semi-trusted third party don't have any information related to the user's location. (2) Secure snapshot and reliable location privacy is assured. (3) The communication price for particular user is depending on the relevant Point of Interest. (4) Range and k-nearest-neighbour queries are used, this system is used to support different spatial queries along with attribute based key encryption algorithm. This algorithm can be run by the semi-trusted third party and the database server. The results of proposed system show that Dynamic grid system is more effective than the currently available privacy- preserving method for continuous LBS. The DGS uses semi-trusted third party. Better privacy is assured in DGS than the TTP scheme. Experimental results depict that DGS has a order of magnitude in related to communication cost. This is more reliable than the TTP scheme. In case of computation cost, DGS is always better than the TTP scheme regarding NN queries; it is a bit more expensive than the TTP scheme used n range queries.

G. A Safe Exit Approach for Continuous Monitoring of Reverse K-Nearest Neighbours in Road Networks In road networks Reverse K-Nearest Neighbour (RKNN) queries have been studied in depth in recent years. There is still very few algorithms for traversing queries in a road network. This paper shows how to process moving queries. Query movement cannot be efficiently handled by existing algorithms. For example, the result of the query has to be recomputed whenever a query changes its location. To perfectly calculate the safe exit points for continuous RKNNs and also to avoid re computation of query results, we put forward a new technique. The result of the query remains same and the server need not receive a recomputation request. Due to

this server processing and the communication costs for the server and moving clients are reduced significantly. The experimental results conducted using real road network data shows that this proposed algorithm significantly reduces communication and computation costs. This paper shows the processing of continuous RKNN queries in road networks and a new algorithm is proposed which is called CMRNN that computes the safe exit points among road networks to move the RNN queries. The experimental conducted using real datasets show that our algorithm reduces computation costs and communication costs between server and client. In reallife scenarios when the server demands a high throughput and mobile devices have limited network bandwidth, CMRNN could be highly beneficial.

H. Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker The implementation of secured processing regarding location information in the location based services (LBS) can be done using cryptographic protocols. A protocol is proposed based on oblivious transfer and homomorphic encryption. Its properties are avoiding personal information on the services side, and a fair revenue distribution scheme. Other LBS answers are discussed related to this, which are used to anonymize information. We introduce a proxy party for this. the job of the proxy is to interact with multiple services and also to collect money from subscribing users. Based on the number of subscriptions to each service the proxy distributed the collected payment to the services. Neither the proxy nor the services know the exact relation between users and the services users subscribed to. The first privacy-preserving LBS framework is introduced based on cryptographic techniques, namely, oblivious transfer and homomorphic encryption. The privacy of the user is preserved by hiding location of the user from services and also by not revealing information on the user/service relationship. Additionally, a system for subscription management is presented including a fair yet anonymous payment scheme. Strong intuitions have been given on the different security properties of this scheme; however, it is a challenge to prove them in a formal context.

I. Private Queries in Location Based Services: Anonymizers are not Necessary Positioning capabilities are equipped into mobile devices which can request location-dependent queries to Location Based Services (LBS). The user location must not be revealed to protect the user privacy. A

trust worthy anonymizer is utilized in existing solutions among the users and the LBS. This approach has several disadvantages: (i) All users must trust the third party which anonymizes the location of the user. So it becomes a single point of attack. (ii)Some cooperating, trustworthy mobile users are required. (iii) Privacy can be assured only for one snapshot of user locations; users are not safeguarded against co-relation attacks. An ideal framework is requested based on PIR in support of private location dependent queries. Since privacy is obtained using cryptographic methods, a trusted third party is not required for this framework. This method achieves high privacy for user location snapshots when compared to existing work. This framework is used to implement exact algorithms for nearest-neighbour search. Query execution is optimized by using data mining techniques. These techniques identify computations which are not important. The results of experiments show that PIR uses cost efficient overhead and are usable in practice. This paper employs the Private Information Retrieval theory to guarantee privacy in location-dependent queries. This is the first experimental work to provide a practical PIR implementation with optimizations which achieve reasonable communication and CPU cost. This architecture is simpler, more secure and is the first one to protect against correlation attacks, when compared to previous work. Currently, to generate better optimized execution plans, in order to reduce further the CPU cost people are working on sophisticated heuristics. In future, there is a plan to investigate the extension of this framework to different types of queries like spatial joins. J. A Two-Level Protocol to Answer Private Locationbased Queries A significant privacy issue in Location Based Services(LBS) is to provide quality location based services by hiding user's identity and location. By using anonymous web browsing services, a user's identity can be easily hidden. However, a user's location can reveal a user's identity. For instance, a user at his home may want to ask queries such as "Find the nearest restaurant around me" through GPS enabled mobile phone but he may not be willing to reveal his location. Cloaking is a simple method to attain location privacy. Recently, to respond to private LBS queries PIR has been used. However, ensuring that the server must only reveal the data what is queried. This paper puts forward an efficient two-level answer depending on two cryptographic protocols: Oblivious Transfer and PIR. The answer for

query can be done by either two-level PIR or it can be a cluster of Oblivious Transfer and PIR. This method gives privacy to the user/client and a trusted party/anonymizer are not required when matched with previous methods, this approach ensures that server reveals only required amount of data and the data that is released is as fine-grained or precise as possible. This paper proposes a way to achieve mobile user privacy in location-based services. It also ensures the server disseminates as precise data as possible. Privacy properties are also defined in general and a proof sketch for our protocol is also provided. As a next step, a comparison is made between performance of our protocol with other schemes. For instance, PIR & K-anonymity with respect to computation and communication costs.

III.SYSTEM STUDY

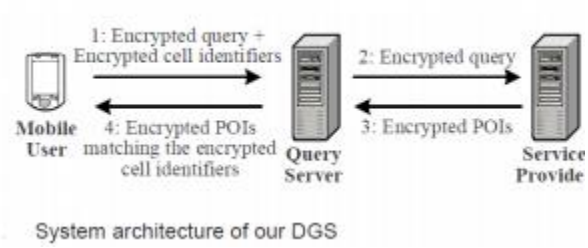
EXISTING SYSTEM: Spatial cloaking techniques have been widely used to preserve user location privacy in LBS Most of the existing spatial cloaking techniques rely on a fully-trusted third party (TTP), usually termed location anonymizer that is required between the user and the service provider. When a user subscribes to LBS, the location anonymizer will blur the user's exact location into a cloaked area such that the cloaked area includes at least k – 1 other user to satisfy kanonymity. In a system with such regional location privacy it is difficult for the user to specify personalized privacy requirements. The feeling based approach alleviates this issue by finding a cloaked area based on the number of its visitors that is at least as popular as the user's specified public region. Although some spatial clocking techniques can be applied to peer-to-peer environments, these techniques still rely on the kanonymity privacy requirement and can only achieve regional location privacy. Furthermore, these techniques require users to trust each other, as they have to reveal their locations to other peers and rely on other peers' locations to blur their locations, another distributed method was proposed that does not require users to trust each other, but it still uses multiple TTPs. Another family of algorithms uses incremental nearest neighbor queries, where a query starts at an "anchor" location which is different from the real location of a user and iteratively retrieves more points of interest until the query is satisfied. While it does not require a trusted third party, the approximate location of a user can still be learned; hence only regional location privacy is achieved.

DISADVANTAGES OF EXISTING SYSTEM: The TTP model has four major drawbacks. It is difficult to find a third party that can be fully trusted. All users need to continuously update their locations with the location anonymizer, even when they are not subscribed to any LBS, so that the location anonymizer has enough information to compute cloaked areas. Because the location anonymizer stores the exact location information of all users, compromising the location anonymizer exposes their locations. K-anonymity typically reveals the approximate location of a user and the location privacy depends on the user distribution.

PROPOSED SYSTEM: In this paper, 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. Untrusted QS would arbitrarily modify and drop messages as well as inject fake messages, which is why our system depends on a semi-trusted QS. The main idea of our DGS. In DGS, a querying user first determines a query area, where the user is comfortable to reveal the fact that she is somewhere within this query area. The query area is divided into equal-sized grid cells based on the dynamic grid structure specified by the user. Then, the user encrypts a query that includes the information of the query area and the dynamic grid structure, and encrypts the identity of each grid cell intersecting the required search area of the spatial query to produce a set of encrypted identifiers. Next, the user sends a request including (1) the encrypted query and (2) the encrypted identifiers to QS, which is a semi-trusted party located between the user and SP. QS stores the encrypted identifiers and forwards he encrypted query to SP specified by the user. SP decrypts the query and selects the POIs within the query area from its database. **ADVANTAGES OF PROPOSED SYSTEM:** For each selected POI, SP encrypts its information, using the dynamic grid structure specified by the user to find a grid cell covering the POI, and

encrypts the cell identity to produce the encrypted identifier for that POI. The encrypted POIs with their corresponding encrypted identifiers are returned to QS. QS stores the set of encrypted POIs and only returns to the user a subset of encrypted POIs whose corresponding identifiers match any one of the encrypted identifiers initially sent by the user. After the user receives the encrypted POIs, she decrypts them to get their exact locations and computes a query answer.

IV. SYSTEM ARCHITECTURE



System architecture of our DGS

V. CONCLUSION & FUTURE WORK

In this Paper we proposed a dynamic grid system (DGS) for providing privacy-preserving continuous LBS.DGS does not require any fullytrusted third party (TTP); instead, we require only the much weaker assumption of no collusion between QS and SP.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. For the future enhancement we will expand this system by giving the location snapshot to share to the friend. In any emergency cases we will provide guest users module in case user did not register themselves in to the system.

REFERENCES

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with PrivacyGrid," in WWW, 2008.

[2] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in SSTD, 2007.

[3] B. Gedik and L. Liu, "Protecting location privacy with personalized k- anonymity: Architecture and algorithms," IEEE TMC, vol. 7, no. 1, pp. 1–18, 2008.

[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

[6] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query pro- cessing for location services without compromising privacy," in VLDB, 2006.

[7] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," in ACM GIS, 2007.

[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Pri- vate queries in location based services: Anonymizers are not necessary," in ACM SIGMOD, 2008.

[9] M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, "Efficient oblivious augmented maps: Locationbased services with a payment broker," in PET, 2007.

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

[11] J. M. Kang, M. F. Mokbel, S. Shekhar, T. Xia, and D. Zhang, "Continuous evaluation of monochromatic and bichromatic reverse nearest neighbors," in IEEE ICDE, 2007.

[12] C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang, "Effective density queries of continuously moving objects," in IEEE ICDE, 2006

.