International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 03 | Mar -2020 ISSN: 2582-3930

User-Defined Privacy Grid System for Continuous Location-Based Services

[1]P. Vinoth Kumar,[2]K. Ramya,[3]N. Balasubramanian,[4]M. Mohamed Rafi

[1]Final Year MCA, Mohamed Sathak Engineering College, Kilakarai

[2]Assistant Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

[3]Associate Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

[4] Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

Abstract— Location-based services (LBS) require users to continuously description their location to a potentially untrusted server to obtain services based on their location, which can lead them to privacy risks. Unfortunately, present privacy-preserving techniques for Location Based Services have numerous restrictions, such as requiring a fully-trusted third party (FTTP), providing limited privacy guarantees and acquiring high communication overhead. A user-defined privacy grid system called dynamic grid system (DGS) the first general system that fulfills four essential requirements for privacy-preserving snapshot and continuous Location Based Services. The system only requires a semi-trusted third revelry, blamable for carrying out simple matching operations correctly. This semi-trusted third party does not have any data about a user's location. Safe snapshot and continuous location privacy are guaranteed under our defined adversary models. The communication cost for the user does not depend on the user's desired privacy level, it only depends on the number of significant points of interest in the vicinity of the user. Although we only focus on range and k-nearest-neighbor (KNN) queries in this work, our system can be simply extended to support other spatial queries without changing the algorithms run by the semi-trusted third party and the database server, provided the required search area of a spatial query can be abstracted into spatial regions. Experimental outcomes show that our Dynamic Grid System is more efficient than the state-of-the-art privacy-preserving technique for continuous LBS.

Keyword: Dynamic grid system, location privacy, location-based services, spatio -temporal query processing, cryptography, mobile computing.

I.INTRODUCTION

In the present world of mobility and ever- Internet connectivity, a huge number of people use LBS to obtain information related to their current locations from different types of service providers. This can be made as the search for nearest points of interests (POIs) (e.g., hotels, malls) location aware made by companies, traffic information suggested to the highway and providing direction to the user who is traveling and so on. The use of Location based services (LBS) can provide more details about a person to potentially untrustworthy service providers behind which people might obtain it. They can track the request made by the person it is possible to make a movement profile which can give data about a user's work space, health related record, political events (attending political events, conferences), etc. Nevertheless, Location based services (LBS) can be very valuable and users should be able to make use of the services given by them, without giving up their location privacy.

A number of methods have recently been suggested for preserving the location privacy of uses in Location based services (LBS) the techniques can be divided into two main categories, Fully-trusted third party (FTTP). The most popularly used privacy-preserving techniques require a trusted third party to be placed among the user and the service provider where to hide the user's location data from

it. Private data retrieval/oblivious transfer: Although private data retrieval or oblivious transfer techniques do not require a third party, they obtain greater communication overhead among the user and the service provider, requiring the transmission of many details than the user actually needs only a few privacy preserving techniques have been suggested for continuous Location based services.

Mobile Computing is a technology that allows transmission of data, voice and video through a computer or any other wireless enabled device without having to be connected to a fixed physical link. Mobile computing is the discipline for creating an information management platform.

The state of the user, static or mobile, does not affect the information management capability of the mobile platform. A user can continue to access and manipulate desired data while traveling on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the desired data and sufficient processing power are available on the spot, where as in reality they may be located far away. Otherwise Mobile computing is a common term used to discuss to a variety of devices that allow people to access data and information from where ever they are. An Location Based Services (LBS) requires five a basic components the services provider's software application, a mobile network to transmit data or information and request for service, a content provider to supply the end user.

2. RELATED WORK

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 anonymity. 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-topeer environments, these techniques still rely on the k-anonymity privacy requirement and can only achieve regional location privacy. Furthermore, these techniques require users to trust each other, as they have to reveal themlocations 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. There are many researchers concentrating on the how to obtain the privacy and accuracy in LBSs One of the researchers was Dewri, who has a long history in the field of privacy in location-based services. The aim of these papers is to revisit the location privacy problem with the objective of providing significantly more stringent privacy guarantees.

3. SYSTEM LEARNING

3.1 Propose Scheme:

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 Q.

3.2 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 issomewhere 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.

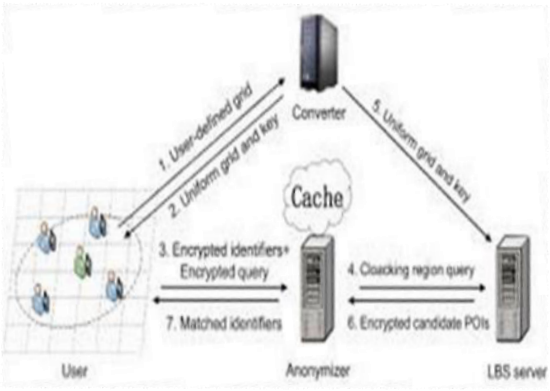

Fig.1.1 DGS with framework

3.3 Service providers (SP):

Our system supports any number of independent service providers. Each Service Provider is a spatial database management system that stores the location information of a particular type of static Point of Interest (POIs). Restaurants or hotels or the store location information of a particular company.

3.4 Mobile users:

Each mobile user is equipped with a Global Positioning System (GPS)-enabled device that determines the user's location in the form (Xu, Yu). The user can obtain snapshot or continuous Location Based Services from our system by issuing a spatial query to a particular Service Provider through Query Server.

3.5 Query servers (QS):

Query Server is a semi-trusted party placed among the mobile user and Service Provider. Similar to the most popular infrastructure in existing privacy-preserving techniques for Location Based Services, Query Server can be maintained by a telecom operator.

4. ENQUIRY WORKS

4.1 Enabling private continuous queries for revealed user locations:

Present location-based services provide specialized services to their customers based on the knowledge of their exact locations. With untrustworthy servers, location-based services may expose to numerous privacy threats ranging from worries over employers snooping on their worker's where about to fears of tracking by potential followers. While there exist numerous techniques to preserve location privacy in mobile environments, these methods are limited as they do not distinguish among location privacy (i.e., a user wants to hide her location) and query privacy (i.e., a user can reveal her location but not her query).This distinction is crucial in many applications where the locations of mobile users are publicly known. In this paper, the restriction of existing cloaking algorithms as we intend a new robust spatial cloaking technique for snapshot and continuous location-based queries that clearly distinguishes amongst location privacy and query privacy.

4.2 Protecting location privacy with personalized K Anonymity:

mobile networks and positioning technologies have created a strong market push for location-based applications. Examples include location-aware emergency response, location-based advertisement, and location-based entertainment. An important challenge in the wide deployment of location-based services (LBSs) is the privacy-aware management of location information,this paper defines a scalable structural design for protecting the location privacy from various privacy threats resulting from uncontrolled usage of Location Based Services. This structural design consists of the development of a personalized location anonymization model and a suite of location perturbation algorithms. A unique characteristic of our location privacy structural design is the use of a flexible privacy personalization framework to support location anonymity for a wide range of mobile users with context sensitive privacy requirements.

4.3 Anonyms tradition of location-based services through latitudinal and temporal covering:

Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. Anonymity can provide a high amount of privacy, save service users from dealing with service provider's privacy policies, and decreases the service provider's requirements for safeguarding -private information. However, guaranteeing anonymous usage of LBS requires that the precise location data transmitted by a client cannot be easily used to re-identify the subject. This paper presents a middleware structural design and algorithms that can be used by a centralized location agent service. The adaptive algorithms adjust the resolution of location information along spatial or temporal dimensions to meet specified anonymity constraints based on the entities who May be using location services within a given area. Using a model based on automotive traffic counts and

cartographic material, we estimate the realistically expected spatial resolution for different anonymity constraints.

4.5 Avoiding location-based identity interfering in anonymous spatial interrogations:

The increasing development of embedding positioning capabilities (for example, Global Positioning System (GPS)) in mobile devices facilitates the widespread use of location-based services. For such applications to succeed, privacy and confidentiality are essential. Existing privacy-enhancing techniques rely on encoding to safeguard communication channels, and on pseudonyms to protect user identities. Nevertheless, the query contents may disclose the physical location of the client. In this paper, we present a framework for preventing location-based identity inference of users who issue spatial queries to LBS. We propose transformations based on the well-established K-anonymity concept to compute exact answers for range and nearest neighbor search, without enlightening the query source. Our methods optimize the whole process of anonymizing the requests and processing the transformed spatial queries. Extensive experimental studies suggest that the proposed techniques are applicable to real-life scenarios with numerous mobile users.

4.6 Supporting unspecified location queries in mobile environment with privacy grid:

We develop dynamic bottom-up and top-down grid cloaking algorithm with the goal of achieving high anonymization success rate and efficiency in terms of both time complexity and maintenance cost. A hybrid approach that carefully combines the strengths of both bottom-up and top down cloaking approaches to further decrease the average anonymization time is also developed. Privacy Grid incorporates temporal cloaking into the location cloaking process to further increase the profit rate of location anonymization.

5.CONCLUSION

We have tried to implemented ―Roman Schlegel, Chi-Yin Chow, Qiong Huang and Duncan S. Wong‖,‖User defined Privacy Grid System For Continuous Location Based Services‖, IEEE TRANSACTIONS ON MOBILE COMPUTING, 2013 and according to the implementation the conclusion is ―A dynamic grid system (DGS) for providing privacy-preserving continuous Location Based Services (LBS). Dynamic Grid System (DGS) includes the query server (QS) and the service provider (SP), and cryptographic functions to split the complete query processing task into two parts that are performed separately by Query Server and Service Provider. Dynamic Grid System does not require any fully-trusted third party (FTTP); instead, we require only the much weaker assumption of no collusion among QS and SP. This separation also moves the data transfer load away from the user to the inexpensive and high-bandwidth link among QS and SP. We also designed efficient protocols for our DGS to support both continuous k-nearest-neighbor (KNN) and range queries. 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 Trusted Third-Party scheme, and the experimental outcomes 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 Nearest Neighbor queries it is comparable or slightly more expensive than the TTP scheme for range queries.

REFERENCES

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, ―Supporting anonymous location queries in mobile environments with Privacy Grid, ‖ 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 processing 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, ―Private 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: Location based services with a payment broker, ‖ in PET, 2007.

[10] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, ―Casper*: Query processing for location services without compromising privacy, ‖ ACM TODS, vol. 34, no. 4, 2009.

[11] T. Xu and Y. Cai, ―Feeling-based location privacy protection for location-basedservices, ‖ in ACM CCS, 2009.

[12] C.-Y. Chow, M. F. Mokbel, and X. Liu, ―A peer-to-peer spatial cloaking algorithm for anonymous location-based service,‖ in ACM GIS, 2006.