Volume 3, Issue 6, June-2016, pp. 289-294 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

User-Defined Privacy Grid System for Continuous Location Based Services

[1]Mr. G.SAI KUMAR, [2] Mr. G.LAKPATHI

[1] Pursuing M.Tech(CSE)from Jagruti Institute of Engineering and Technology
[2] Associate Professor, Department of Computer Science and Engineering,
Jagruti Institute of Engineering and Technology, Telangana State, India.

Abstract: In this paper we have demonstrated Location-Based Services (LBSs) which has surfaced as prominent applications in mobile networks. An important challenge in the wide deployment of location-based services (LBSs) is the privacy aware management of location information, providing safeguards for location privacy of mobile clients against vulnerabilities for abuse. This paper describes a scalable architecture for protecting the location privacy from various privacy threats resulting from uncontrolled usage of LBSs. This architecture includes the development of a personalized location anonymization model and a suite of location perturbation algorithms. In particular, our algorithm makes use of a variable-sized cloaking region that increases the location privacy of the user at the cost of additional computation, but maintains the same traffic cost. Our proposal does not require the use of a trusted third-party component, and ensures that we find a good compromise between user privacy and computational efficiency. we propose a user-defined privacy grid system called dynamic grid system (DGS); the first holistic system that fulfils four essential requirements for privacy-preserving snapshot and continuous LBS. Our experiments show that the personalized location k-anonymity model, together with our location perturbation engine, can achieve high resilience to location privacy threats without introducing any significant performance penalty. Experimental results show that our DGS is more efficient than the state-of-the-art privacy preserving technique for continuous LBS.

Key Words: SQL Server, ASP.net, Mobile Computing

1. INTRODUCTION

In today's world of mobility and ever-present Internet connectivity, an increasing number of people use location based services (LBS) to request information relevant to their current locations from a variety of service providers. This can be the search for nearby points of interest (POIs). The use of LBS, however, can reveal much more about a person to potentially untrustworthy service providers than many people would be will- ing to disclose. LBS can be very valuable and as such 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 LBS. In general, these approaches can be classified into two main categories. (1) Fully-trusted third party (TTP). The most popular privacy-preserving techniques require a TTP to be placed between the user and the service provider to hide the user's location information from the service provider (e.g., [1]–[8]). 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 are that includes k−1 other users to achieve k-anonymity. This TTP model has three drawbacks. (a) All users have to continuously report their exact location to the third party, even though they do not subscribe to any LBS. (b) As the third party knows the exact location of every user, it becomes an attractive target for attackers. (c) The k-anonymity-based techniques only achieve low regional location privacy because cloaking a region to include k users in practice usually results in small cloaking areas. (2) Private information retrieval (PIR) or oblivious transfer (OT). . In this project, 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 the encrypted query to SP specified by the user. SP decrypts the query and selects the POIs within the query area from its database. 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

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 users to satisfy k-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-to-peer 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 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.[5]. 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.

He has various publications relating to achieving the privacy in LBSs His last paper [1] proposed a user-controlled privacy experience "a user-centric location based service architecture", where the user determines the desired level of privacy based on his accuracy requirements. A provider "privacy-supportive LBS" provides supplemental information to the user for making "informed" privacy decisions. The system will inform the user of the accuracy (or lack thereof) based on the privacy specifications input into the system, depending on "a service-similarity profile" which the user gets. If the user is satisfied with the result set (even if it has errors or the privacy is under the required level), they can choose to proceed with the query. If they are not satisfied, they can change the privacy level into the balance of accuracy/privacy that is acceptable to them. The main purpose of previous papers is to understand (LBS) technology and identified the key components behind the service. Some papers present a concise survey of location based services, the technologies deployed to track the mobile user's location, the accuracy and reliability associate with such measurements, and the network infrastructure elements deployed by the wireless network operators to enable these kinds of services. Other papers define the user requirements in terms of mobile device features and LBS applications. In addition to the general idea of the LBS, the researchers discussed the impact on consumer, and utility computing offer attractive financial and technological advantages. As an example, Zhang and Mao studied the effects of three individual level factors; consumption values, privacy concerns, and subjective norms on consumers' intention to adopt location-based services on their mobile phones and to spread positive word-of-mouth (WOM) about LBS. Such knowledge helps business create effective communications to attract more potential adopters.

In light of the current findings, marketing communications need to heighten perceived consumption values about using LBS. All these scientific papers give the attracted people a general idea about LBSs, and how this service was important. Researchers have long been aware of the potential privacy risks associated with LBSs, because they know while the user used one of these application services to retrieve the accuracy information, this new functionality comes with significantly increased risks to personal privacy. They have proposed a number of promising schemes that can help users protect their privacy. Some of these papers present an overview of different protection goals and fundamental location privacy approaches, as well as a classification of different types of attacks according to the applied attacker knowledge. They clarified different protection goals and fundamental location privacy approaches, as well as a classification of different types of attacks according to the applied attacker knowledge. The aim of these papers is to revisit the location privacy problem with the objective of providing significantly more stringent privacy guarantees.

3. 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 k-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-to-peer 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 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.

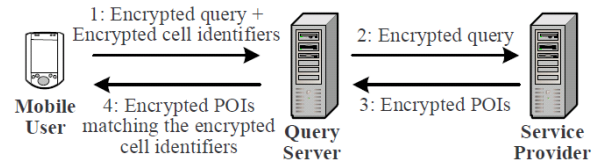
ADVANTAGES OF PROPOSED SYSTEM:

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.

4. SYSTEM ARCHITECTURE:



System architecture of our DGS

5. CONCLUSION & FUTURE WORK

In this Paper we proposed a dynamic grid system (DGS) for providing privacy-preserving continuous LBS.DGS does not require any fully-trusted 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 two-level 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.

ABOUT THE AUTHORS

Mrs.G.SAI KUMAR is pursuing M.Tech degree in, Computer Science and Engineering from Jagruti Institute of Engineering and Technology, Telangana State, India.

Mr.G.Lakpathi, presently working as Assistant Professor in, Department of computer science and engineering, Telangana State,India.

