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

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

Tattari Jayasri
M.Tech (CSE) Student,
Dept. of Computer Science,
Nimra College of Engineering & Technology,
A.P., India.

Guntapalli Minni
Assistant Professor,
Dept. of CSE,
Nimra College of Engineering & Technology,
A.P., India.

Sayeed Yasin
Associate Professor & HoD,
Dept. of CSE,
Nimra College of Engineering & Technology,
A.P., India.

Abstract

The services offers by LBS (Location based service) are characteristically based on a point of interest record. By recover the Points Of Interest (POIs) from the database server, the user can get reply to a variety of location based queries, which comprise but are not incomplete to determine the nearest ATM machine, gas station, hospital, or police station. Amongst numerous demanding blockades to the extensive operation of such submission, solitude declaration is a main question. The Location Server (LS), which proffer some LBS, expend its possessions to accumulate information about a variety of interesting POIs. Consequently, it is normal that the LS would not unveil any information devoid of amount. Therefore the LBS have to make certain that LS's data is not way in by any unofficial consumer. Unfortunately, existing privacy-preserving techniques for LBS have several limitations, such as requiring a fully-trusted third party, offering limited privacy guarantees and incurring high communication overhead. In this paper, we propose a user-defined privacy grid system called dynamic grid system (DGS); the first holistic system that fulfills four essential requirements for privacy-preserving snapshot and continuous LBS. We recommend a key augmentation upon preceding solutions by commence a two stage approach, where the first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to accomplish a secure solution for both parties. The solution we present is capable and realistic in numerous circumstances.

Keywords *— Location based query, private query, private information retrieval, oblivious transfer, Dynamic grid systems, location privacy.*

INTRODUCTION

Cloud computing provides shared processing environment for data storage and accessing also known as internet based computing. It is a model which provides configurable computing resources such as networks, servers, storage, applications and services. Cloud computing has a high computation power, lowest cost of services, higher performance, scalability, accessibility and availability for that reason it is highly demanded. Data outsourcing brings with it many advantages. But associated with it are the risks involved.

Though client cannot physically access the data from the cloud server directly, without client's are either not used by client from a long time. 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

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

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 and computes a query answer.

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. An 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.

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

LITERATURE SURVEY

1) Supporting anonymous location queries in mobile environments with PrivacyGrid

AUTHORS: B. Bamba, L. Liu, P. Pesti, and T.Wang

This paper presents PrivacyGrid - a framework for supporting anonymous location-based queries in mobile information delivery systems. The PrivacyGrid framework offers three unique capabilities. First, it provides a location privacy protection preference profile model, called location P3P, which allows mobile users to explicitly define their preferred location privacy requirements in terms of both location hiding measures (e.g., location k-anonymity and location l-diversity) and location service quality measures (e.g., maximum spatial resolution and maximum temporal resolution). Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment. We develop dynamic bottom-up and top-down grid cloaking algorithms 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 reduce the average anonymization time is also developed. Last but not the least, PrivacyGrid incorporates temporal cloaking into the location cloaking process to further increase the success rate of location anonymization. We also discuss PrivacyGrid mechanisms for supporting anonymous location queries. Experimental evaluation shows that the PrivacyGrid approach can provide close to optimal location k-anonymity as defined by per user location P3P without introducing significant performance penalties.

2) Enabling private continuous queries for revealed user locations

AUTHORS: C.-Y. Chow and M. F. Mokbel

Existing location-based services provide specialized services to their customers based on the knowledge of their exact locations. With untrustworthy servers, location-based services may lead to several privacy threats ranging from worries over employers snooping on their workers' whereabouts to fears of tracking by potential stalkers. While there exist several techniques to preserve location privacy in mobile environments, these techniques are limited as they do not distinguish between 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, we go beyond the limitation of existing cloaking algorithms aswe propose a newrobust spatial cloaking technique for snapshot and continuous location-based queries that clearly distinguishes between location privacy and query privacy. By this distinction, we achieve two main goals: (1) supporting private location-based services to those customerswith public locations, and (2) performing spatial cloaking on-demand basis only (i.e., when issuing queries) rather than exhaustively cloaking every single location update. Experimental results show that the robust spatial cloaking algorithm is scalable and efficient while providing anonymity for large numbers of continuous queries without hiding users' locations.

3) Protecting location privacy with personalized kanonymity: Architecture and algorithms

AUTHORS: B. Gedik and L. Liu

Continued advances in 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, 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. A unique characteristic of our location privacy architecture is the use of a flexible privacy personalization framework to support location k-anonymity for a wide range of mobile clients with

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

context-sensitive privacy requirements. This framework enables each mobile client to specify the minimum level of anonymity that it desires and the maximum temporal and spatial tolerances that it is willing to accept when requesting k-anonymity-preserving LBSs. We devise an efficient message perturbation engine to implement the proposed location privacy framework. The prototype that we develop is designed to be run by the anonymity server on a trusted platform and performs location anonymization on LBS request messages of mobile clients such as identity removal and spatio-temporal cloaking of the location information. We study the effectiveness of our location cloaking algorithms under various conditions by using realistic location data that is synthetically generated from real road maps and traffic volume data. 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.

4) Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking

AUTHORS: M. Gruteser and D. Grunwald

Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. Anonymity can provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service providers' requirements for safeguarding private information. However, guaranteeing anonymous usage of location-based services requires that the precise location information transmitted by a user cannot be easily used to re-identify the subject. This paper presents a middleware architecture and algorithms that can be used by a centralized location broker 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. The median resolution generated by our algorithms is 125 meters. Thus, anonymous location-based requests for urban areas would have the same accuracy currently needed for E-911 services; this would provide sufficient resolution for wayfinding, automated bus routing services and similar location-dependent services

5) Preventing location-based identity inference in anonymous spatial queries

AUTHORS: P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias

The increasing trend of embedding positioning capabilities (for example, 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 encryption to safeguard communication channels, and on pseudonyms to protect user identities. Nevertheless, the query contents may disclose the physical location of the user. In this paper, we present a framework for preventing location-based identity inference of users who issue spatial queries to location-based services. We propose transformations based on the well-established K-anonymity concept to compute exact answers for range and nearest neighbor search, without revealing the query source. Our methods optimize the entire 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.

REALATED WORK

LBSs one amongst the researchers was Dewri, World Health Organization includes a long history within the field of privacy in location-based services. He has numerous publications with reference to achieving the privacy in LBSs His last paper [1] projected a user-controlled privacy experience "a user-centric location based mostly service architecture", wherever the user determines the required level of privacy supported his accuracy necessities. A provider "privacy-supportive

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

LBS" provides supplemental information to the user for creating "informed" privacy decisions. The system can inform the user of the accuracy (or lack thereof) supported the privacy specifications input into the system, looking on "a service-similarity profile "which the user gets. If the user is happy with the result (even if it's errors or the privacy is beneath the desired level), they will opt to proceed with the question. If they are not happy, they will modification the privacy level into the balance of accuracy/privacy that's acceptable to them. The main purpose of previous papers is to grasp (LBS) technology and known the key parts behind the service.

Some papers gift a taciturn survey of location based services, the technologies deployed to trace the mobile user's location, the accuracy and reliableness associate with such measurements, and also the network parts deployed by the wireless network operators to modify these varieties of services. Different papers define the user necessities in terms of mobile device features and LBS applications. In addition to the overall plan of the LBS, the researchers discussed the impact on shopper, and utility computing offer enticing money and technological blessings. As an example, Zhang and Mao studied the results of 3individual level factors; consumption values, privacy, and subjective norms on consumers' intention to adopt location based services on their mobile phones and to spread positive spoken (WOM) concerning LBS. Such knowledge helps business produce effective communications to attract a lot of potential adopters. In lightweight of the present findings, promoting communications have to be compelled to height en perceived consumption values concerning exploitation LBS. All these scientific papers offer the attracted individuals a general plan concerning LBSs, and the way this service was important.

Researchers have long been responsive to the potential privacy risks related to LBSs, as a result of they know whereas the user used one amongst these application services to retrieve the accuracy data, this new practicality comes with considerably exaggerated risks to non-public privacy. they need projected variety of promising these papers gift an outline of various protection goals and elementary location privacy approaches, as well as a classification of various sorts of attacks in line wit the applied offender data.

CONCLUSION

In this paper, we proposed a dynamic grid system (DGS) for providing privacy-preserving continuous LBS. Our DGS includes the query server (QS) and the service provider (SP), and cryptographic functions to divide the whole query processing task into two parts that are performed separately by QS and SP. 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. This separation also moves the data transfer load away from the user to the inexpensive and high-bandwidth link between QS and SP. We also designed efficient protocols for our DGS to support both continuous k-nearest-neighbor (NN) 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 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.

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 kanonymity: Architecture and algorithms," IEEE TMC, vol. 7, no. 1, pp. 1–18, 2008.

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

[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] ——, "Exploring historical location data for anonymity preservation in location-based services," in IEEE INFOCOM, 2008.

[9] 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.

[10] 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.

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

[12] 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.

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

[14] S. Wang and X. S. Wang, "AnonTwist: Nearest neighbor querying with both location privacy and k-anonymity for mobile users," in MDM, 2009.

[15] W. B. Allshouse,W. B. Allshousea,M. K. Fitchb, K. H. Hamptonb, D. C. Gesinkc, I. A. Dohertyd, P. A. Leonebd, M. L. Serrea, andW. C. Millerb, "Geomasking sensitive health data and privacy protection: an evaluation using an E911 database," Geocarto International, vol. 25, pp. 443–452, October 2010.

Author Details

Ms. Tattarijayasri is a student of Nimra College of Engineering and Technology, Ibrahimpatnam, VIJAYAWADA. She is presently pursuing her M.Tech degree from JNTU,Kakinada.

G.Minni is presently working as Assistant professor in CSE department in Nimra college of Engineering and Technology, Jupudi, Nimra Nagar,VIJAYAWADA. She has obtained M.Tech degree from JNTU, Kakinada. She is pursuing Ph.D., in A.N.U, GUNTUR. She has published several research papers in various national and international Journals. She has more than Ten years of experience in teaching field, her area of interests are networks & Web Designing.
E-Mail :minni.guntapalli@gmail.com

Sayeed Yasin received his M.TECH in Computer Science & Engg from JNTU Hyderabad. He is pursuing Ph.D., in Rayalaseema University, Kurnool. He is currently working as an Associate Professor & Head in Nimra College of Science & Technology the Department of Computers Science and Engineering & Technology, Jupudi, Ibrahimpatnam,Vijayawada-521456. He has more than Eight years of experience in teaching field. His areas of interests are wireless networks & programming, & Mobile Computing.
E-Mail: sdyasin761@gmail.com