IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ENHANCING PRIVACY FOR USERS USING LOCATION BASED SERVICES

Manoj Kumar S*, Dr. B.G Prasad
[*] M.tech student, Dept of ISE BMS College of Engineering Bangalore- India
Professor(CSE) and Associate Dean(CS/IS),BMS College of Engineering,Bengaluru-560019

DOI: 10.5281/zenodo.54781

ABSTRACT

Location-based services (LBS) 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. 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 matrix framework (DMF); the first holistic system that fulfills four essential requirements for privacy-preserving snapshot and continuous LBS. (1) 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. (2) Secure snapshot and continuous location privacy is guaranteed under our defined adversary models. (3) The communication cost for the user does not depend on the user's desired privacy level, it only depends on the number of relevant points of interest in the vicinity of the user. (4) 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 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.

KEYWORDS: location privacy, location-based services,query processing, cryptography.

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 (SPs). This can be the search for nearby points of interest (POIs) (e.g., restaurants and hotels), location-aware advertising by companies, traffic information tailored to the highway and direction a user is traveling and so forth. The use of LBS, however, can reveal much more about a person to potentially untrustworthy service providers than many people would be willing to disclose. By tracking the requests of a person it is possible to build a movement profile which can reveal information about a user's work (office location), medical records (visit to specialist clinics), political views (attending political events), etc. Nevertheless, 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], [2], [3], [4], [5], [6], [7], [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 area 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). Although PIR or OT 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 (e.g., [9], [10], [11]).Only a few privacy-preserving techniques have been proposed for continuous LBS [2], [7]. These techniques rely on a TTP to continuously expand a cloaked area to include the initially assigned k users. These techniques not only inherit the drawbacks of the TTP model, but they also have other limitations. (1) Inefficiency. Continuously expanding cloaked areas substantially increases the query processing overhead. (2) Privacy leakage. Since the database server receives a set of consecutive cloaked areas of a user at different timestamps, the correlation among the cloaked areas would provide useful information for inferring the user's location. (3) Service termination. A user has to terminate the service when users initially assigned to her cloaked area leave the 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. 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 semitrusted QS[13].

RELATED WORK

MobiShare: Sharing context-dependent data & services from mobile sources

The rapid growth in wireless communications innovations and mobile computing have empowered personal portable devices that we use in everyday life to become information and services providers by supplementing or supplanting fixed-location hosts associated with wired systems.Such versatile mobile resources can be exceptionally essential for other moving clients, making noteworthy opportunities for many intriguing and novel applications. The MobiShare architecture provides the framework for seamless mobile access and mechanisms for publishing, discovering and accessing mobile data in a broad area, considering the association of both sources and requestors. Any remote communication technology could be used between a gadget and the framework. Moreover, the utilization of XML-related languages and conventions for portraying and trading metadata gives the framework a uniform and effortlessly versatile interface, permitting an assortment of gadgets to utilize it. The general methodology is information driven and benefit oriented, inferring that every gadget is dealt with as makers or requestors of information wrapped as data providers.

On the Anonymity of Home/Work Location Pairs

Numerous applications advantage from client area information, however area information raises protection concerns. Anonymization can secure privacy , but identities can sometimes be determined from supposedly obscure data. Here we ponder upon a new attack on the anonymity of location information. It is demonstrated that if the inexact locations of an individual's home and work place can both be reasoned from an area trace, then the median size of that person's anonymity set in the U.S. working populace is 1, 21 and 34,980, for areas known at the granularity of an census grid, census track and the county in that order . The area information of individuals who live and work in various districts can be re-recognized much all the more effectively. Our outcomes demonstrate that the danger of re-recognizable proof for area information is much more noteworthy when the individual's home and work areas can both be reasoned from the information. To safeguard secrecy direction for muddling area follows before they are uncovered.[14]

Evaluating the Privacy Risk of Location-Based Services

In present day mobile systems, clients progressively impart their area to third-parties consequently for location based services. Thusly, clients acquire services altered to their area. However, such communications leak location data about clients. Regardless of the fact that clients make utilization of pseudonyms, providers of area based services might have the capacity to recognize them and in this manner influence their security. Here they have examined the disintegration of privacy created by the utilization of area based services. To do so,they have experimented with genuine mobile traces and measure the elements of client privacy thereby measuring the security dangers instigated by the utilization of area based administrations.

A Survey of Computational Location Privacy

This is a literature review of computational location protection, which means calculation based security components that regard location information as geometric data. This definition incorporates protection safeguarding algorithms like anonymity and obfuscation and also security breaking algorithms that take advantage of the geometric nature of the information. The survey excludes non-computational strategies like physically investigating geotagged photographs, and it discards methods like encryption or access control that regard area information as general symbols. Here they have surveyed investigations of people groups' states of mind about location security, computational dangers on leaked location information, and computational countermeasures for mitigating these dangers.

Private Queries in Location Based Services

Cell phones furnished with positioning abilities (e.g., GPS) can ask area dependent inquiries to Location Based Services (LBS). To ensure privacy, the client area must not be revealed. Current methods use a trusted anonymizer between the clients and the LBS. This methodology has a few disadvantages: (i) All clients must trust the anonymizer, which is a specific point of assault. (ii) Huge number of obliging, dependable clients are required. (iii) Privacy is ensured just for a solitary depiction of client areas; clients are not secured against correlation assaults (e.g., history of client development).They have proposed a novel structure to bolster private location-dependent inquiries, in light of the hypothetical work on Private Information Retrieval (PIR).Their structure does not require a trusted outsider, since security is accomplished by means of cryptographic procedures. In contrast with existing work, their methodology accomplishes more area security for snapshots of client areas; additionally, it is the first to give provable protection ensures against correlation assaults. They use their system to execute approximate and accurate calculations for closest neighbor search. We advance question execution by utilizing information mining systems, which distinguish excess calculations. As opposed to basic conviction, the test results propose that PIR approaches acquire reasonable overhead and can be practically applied.[15]

SYSTEM ARCHITECTURE

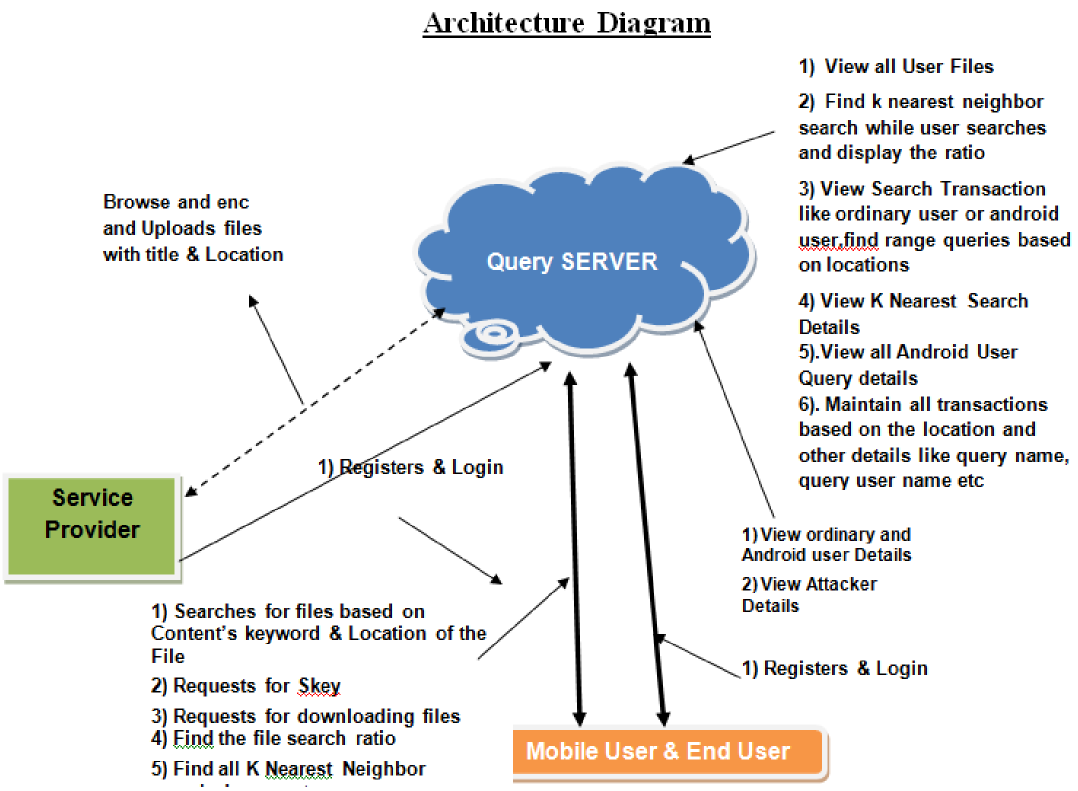
Architecture Diagram
1) View all User Files
2) Find k nearest neighbor search while user searches and display the ratio
3) View Search Transaction like ordinary user or android user,find range queries based on locations
4) View K Nearest Search Details
5).View all Android User Query details
6). Maintain all transactions based on the location and other details like query name, query user name etc
Browse and enc and Uploads files with title & Location
Query SERVER
1) Registers & Login
Service Provider
1) View ordinary and Android user Details
2) View Attacker Details
1) Searches for files based on Content's keyword & Location of the File
2) Requests for Skey
3) Requests for downloading files
4) Find the file search ratio
5) Find all K Nearest Neighbor
1) Registers & Login
Mobile User & End User

Fig:1 System Architecture

Fig. 1 depicts the system architecture of our dynamic matrix framework designed to provide privacy-preserving continuous LBS for mobile users. Our system consists of three main entities, service providers, query servers and mobile users.

Service providers. Our system supports any number of independent service providers. Each SP is a spatial database management system that stores the location information of a particular type of static POIs, e.g., restaurants or hotels, or the store location information of a particular company, e.g., Starbucks or McDonald's. The spatial database uses an existing spatial index (e.g., R-tree or grid structure) to index POIs and answer range queries (i.e., retrieve the POIs located in a certain area). As depicted in Fig. 1, SP does not communicate with mobile users directly, but it provides services for them indirectly through the query server.

Mobile users. Every wandering client's device is furnished with a GPS-empowered gadget that approximates the client's area. The client can get snapshot or persistent LBS from our framework by issuing a spatial inquiry to a specific SP through QS. Our framework helps the client select a inquiry region for the spatial inquiry, such that the client is willing to reveal his location to SP. At that point, a matrix structure is made and is inserted inside an encoded question that is sent to SP, it won't uncover any data about the inquiry region to QS itself. Also, the communication cost for the client in DGS does not rely on upon the inquiry zone size. This is one of the key components that outstands DGS from the current strategies in view of the fully trusted third party paradigm.

Query servers. QS is a semi-trusted party placed between the mobile user and SP. Similar to the most popular infrastructure in existing privacy-preserving techniques for LBS, QS can be maintained by a telecom operator [12].
The control/data flows of our DGS are as follows (Fig. 1):

1) The mobile user sends a request that includes (a) the identity of a user-specified SP, (b) an encrypted query (which includes information about the user-defined dynamic grid structure), and (c) a set of encrypted identifiers (which are calculated based on the userdefined dynamic grid structure) to QS.
2) QS stores the encrypted identifiers and forwards the encrypted query to the user-specified SP.
3) SP decrypts the query and finds a proper set of POIs from its database. It then encrypts the POIs and their corresponding identifiers based on the dynamic grid structure specified by the user and sends them to QS.
4) QS returns to the user every encrypted POI whose encrypted identifier matches one of the encrypted identifiers initially sent by the user. The user decrypts the received POIs to construct a candidate answer set, and then performs a simple filtering process to prune false positives to compute an exact query answer.

Comparison of DMF with TTP

Although DMF and TTP have architectural similarities, DMF provides better location privacy and privacy guarantees than TTP for the two reasons: (1) In a TTP system, the user is only K-anonymous, i.e., the user can be identified to be one of K users, but without being able to determine the exact user. In DGS, however, QS has no information at all to narrow down the anonymity set, while SP can only narrow the anonymity set down to the query area, but the query area can be chosen arbitrarily large by the user without negative performance impacts. Furthermore, TTP requires the cloaking area to expand as the user moves around, while in DMF the query area can stay fixed without an impact on the anonymity of the user. (2) The trusted third party in TTP needs to be fully trusted because it has access to all locations of all users in the system. In DMF, however, neither SP nor QS need to be fully trusted, as neither of them ever has access to the exact location of a user.

In DMF no entity has access to the exact location of users and the user's anonymity is not defined by a K value but by the query area, which can be chosen suitably large, so DMF provides better privacy guarantees than TTP. To achieve the same level of privacy with TTP compared to DMF, the K parameter in TTP would have to be chosen to correspond to the number of users present in the whole query area of DMF. However, the query area of DMF is typically chosen on a city-level, resulting in a large K value, e.g., tens of thousands of users. In TTP, however, K values are typically chosen in the lower hundreds, e.g., 200 [2]. This shows that DMF will by default provide much better privacy than TTP.

RESULTS

Table 1 shows the benchmark results for IBE encryption and AES decryption that refer to encrypting one request for SP and decrypting one POI received from QS, respectively. These results show that smartphones are easily capable of performing the cryptographic operations necessary in our protocol. While IBE is still a somewhat expensive operation requiring on the order of 50 ms, this is an infrequent request and hence not a bottleneck. Hashing/encrypting and AES decryption on the other hand are much more frequent operations in our protocol, but the operations are very efficient when done natively, so that a mobile device can easily decrypt up to several hundred thousand POIs per second, or even more if multiple cores are used (at which point bandwidth is more likely to become the bottleneck).

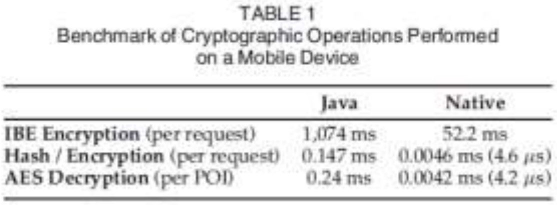

TABLE 1
Benchmark of Cryptographic Operations Performed on a Mobile Device

	Java	Native
IBE Encryption (per request)	1,074 ms	52.2 ms
Hash / Encryption (per request)	0.147 ms	0.0046 ms (4.6 μs)
AES Decryption (per POI)	0.24 ms	0.0042 ms (4.2 μs)

Table 1.Results

CONCLUSION

In this paper, we proposed a dynamic grid system for providing privacy-preserving continuous LBS. Our DMF includes the query server and the service provider, and cryptographic functions to divide the whole query processing task into two parts that are performed separately by QS and SP. DMF does not require any fully-trusted third party; 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 DMF to support both continuous k-nearest-neighbor and range queries. To evaluate the performance of DMF, we compare it to the state-of-the-art technique requiring a TTP. DMF provides better privacy guarantees than the TTP scheme, and the experimental results show that DMF is an order of magnitude more efficient than the TTP scheme, in terms of communication cost. In terms of computation cost, DMF 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 Proc. 17th Int. Conf. World Wide Web, 2008, pp. 237–246.

[2] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in Proc. 10th Int. Conf. Adv. Spatial Temporal Databases, 2007, pp. 258–273.

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

[4] M. Gruteser and D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking," in Proc. 1st Int. Conf. Mobile Syst., Appl. Services, 2003, pp. 31–42.

[5] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[6] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in Proc. 32nd Int. Conf. Very Large Data Bases, 2006, pp. 763–774.

[7] T. Xu and Y. Cai, "Location anonymity in continuous location based services," in Proc. 15th Annu. ACM Int. Symp. Adv. Geographic Inf. Syst., 2007, pp. 39:1–39:8.

[8] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location-based services," in Proc. IEEE INFOCOM, 2008, pp. 547–555.

[9] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in Proc. ACM SIGMOD Int. Conf. Manag. Data, 2008, pp. 121–132.

[10] M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, “Efficient oblivious augmented maps: Location-based services with a payment broker,” in Proc. 7th Int. Conf. Privacy Enhancing Technol., 2007, pp. 77–94.

[11] R. Vishwanathan and Y. Huang, “A two-level protocol to answer private location-based queries,” in Proc. IEEE Int. Conf. Intell. Security Informat., 2009, pp. 149–154.

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

[13] Schlegel, Roman, Chi-Yin Chow, Qiong Huang, and Duncan S. Wong. "User-Defined Privacy Grid System for Continuous Location-Based Services", IEEE Transactions on Mobile Computing, 2015.

[14] Philippe Golle. "On the Anonymity of Home/Work Location Pairs", Lecture Notes in Computer Science, 2009

[15] Kian-Lee Tan. "Private queries in location based services", Proceedings of the 2008 ACM SIGMOD international conference on Management of data - SIGMOD 08 SIGMOD 08, 2008.