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

Jyoti Pawar, G.P. Chakote

Abstract*: Location-based services (LBS) require users to continually report their location to a potentially unreliable server to obtain services based on location, which may expose them to confidentiality risks. Unfortunately, existing privacy techniques have several limitations, such as the requirement of a fully reliable third party offering limited privacy and high communication overhead. In this paper, we propose a user-defined privacy grid system called a dynamic grid system (DGS); The first holistic system that meets four essential requirements for the preservation of instant and continuous privacy LBS. (1) The system requires only a trusted third party responsible for the proper execution of the matching operations. This semi-reliable third party has no information about a user's location. (2) Secure confidentiality and continued site confidentiality are warranted in our defined opponent models. (3) The cost of communication for the user does not depend on the level of confidentiality desired by the user, it depends only on the number of relevant points of interest near the user. (4) Although we only focus on range and k-neighbor-neighbor queries in this work, our system can be extended to support spatial queries without modifying the algorithms executed by the semi-reliable third party and The database server, the search area required for a spatial query can be extracted into spatial regions. The experimental results show that our DGS is more efficient than the state-of-the-art privacy technology for continuous LBS.

***Index Terms*: Location Based Service (LBS), Dynamic Grid System (DGS), Confidentiality, Privacy Technologys.**

I. INTRODUCTION

In this modern world, it is very easy for a person to know its location with the help of devices having a GPS installation. When the location of the user is provided to location-based services (LBS), it is possible for the user to know all location-dependent information such as the location of the friends or nearest Restaurant, Or traffic conditions. The usage of mobile phones in our day to day lives paves the way for the possibility of wireless communication networks that can be used to exchange information across locations. When the exchange of location information is between unreliable parties, the user's privacy could be harmful. The existing protocol does not work on many different mobile devices and another problem is that the location server (LS) must provide deceptive data to the user. In recent years, the number of mobile devices polled on location servers has increased dramatically to obtain information on POIs. Among the many barriers that prevent the deployment of such an application, privacy is a major issue. Site-based services (LBS) require users to continually report their location to a potentially unreliable server to obtain services based on location, which may expose them to confidentiality risks. Unfortunately, the protection of existing privacy LBS techniques have several limitations, such as the requirement of a fully reliable third party, offering limited confidentiality and resulting high communication costs. Mobile security testing is becoming an urgent and important research topic due to the explosive increase in mobile app downloads and mobile users. Now functional services based on location in mobile applications not only enhance the mobile user experience but also bring new challenges and problems in software testing and data security. This paper focuses on localization problems, the prevention of Mobile applications, and offers a new model and method of tracking and research to meet these needs. Site-based services (LBS) require users to continually report their location to a potentially unreliable server to obtain services based on location, which may expose them to confidentiality risks. Unfortunately, existing privacy techniques for location-based services (LBS) have several limitations, such as the requirement of a fully reliable third party, offering limited confidentiality guarantees and a high communication load . Increased number of mobile intruders.

Privacy is a serious security threat that can be highly detrimental to businesses and consumers in the mobile environment. The location attack can be performed either by mobile networks or by database. By retrieving the Points of Interest (POI) from the database server, the user can obtain responses to various location-based queries, which include, but are not limited to, discovery of the ATM, Gas station, hospital or nearest police station.

There are more and more mobile phone users around the world. Thus, location technologies can currently be used by wireless telecommunications operators to provide a good prediction of the location of the user. Today, the number of users is based on services based on provide location information. Much research has been done on the preservation of privacy. But no one gave absolute guarantee of the data of the user and the request. Basically, when the user has used a specific location service or registered for that, LBS can provide a number of other services such as delivery coupons or other marketing information for the customer that is in a geographical area specific. Nowadays, there are number of users taking advantage of location services and the graph is increasing..

II. RELATED WORK

The first solution to the problem has been proposed by Beresford [6], in which the user's privacy is maintained by constantly changing the name of the user or pseudonym into a certain mixing area. It can be shown that, due to the nature of the data exchanged between the user and the server, the frequent change of the user name provides little protection to the user's privacy. A more recent study of the mix-zone approach has

Revised Version Manuscript Received on January 30, 2017.

Jyoti Ganeshrao Pawar, M.Tech, Department of Computer Science & Engineering, Matsyodari Shikshan Sansthas College of Engineering and Technology, Aurangabad (Maharashtra)-431203. India.

Prof. G.P. Chakote, Head of Department Computer Science & Engineering, Matsyodari Shikshan Sansthas College of Engineering and Technology, Aurangabad (Maharashtra)-431203. India.

been applied to road networks [18]. They studied the number of users required to satisfy the deactivation property when there are repeated requests over an interval. This requires careful control of the number of users in the mixing area, which is difficult to achieve in practice [13].

Old problems introduced in a new method that presents a preliminary investigation on the confidentiality issues involved in the use of location services. The geo-localized history of user queries can act as a quasi-identifier and can be used to access sensitive information on specific individuals [1]. A technique complementary to the approach of the mixed zone is based on the anonymity k [3], [2], [5]. The concept of kanonymity was introduced as a method to preserve privacy when releasing sensitive records [13]. This is done by generalization and suppression algorithms to ensure that a record can not be distinguished from (k - 1) other records. Solutions for LBS use a trusted anonymization to ensure the anonymity of location data, such as location data. As more and more user information becomes available with the rapid growth of Internet applications, for example, social networks, attackers have the ability to build personal user profiles. This raises new challenges and Reconsideration of existing confidentiality measures, such as k anonymity. A new metric to measure the confidentiality of users' requests taking into account user profiles [2]. However, knowledge of places is often perceived as personal information. Although a number of privacy models and algorithms have taken shape in recent years, it is almost universal to specify the requirement of confidentiality without understanding its implications for quality of service. [14] . Becoming omnipresent. However, traditional search engines do not function properly for a significant fraction of location-based queries, which are non-factual (ie, subjective, relative, or multidimensional). As an alternative, we are studying the feasibility of responding to queries based on localization by the Twitter feeding crowd. Specifically, they have developed the efficiency of using location-based services (such as Foursquare) to find the right people to respond to a given location query. The results give an idea of the feasibility of this approach and highlight some research challenges in the social search engines [10].

A significant privacy problem in location-based services (LBS) is to hide the identity and location of a user while providing quality location-based services. The identity of a user can be easily hidden through anonymous web browsing services. However, the location of a user can reveal the identity of a user. In addition, they argue that ensuring the server does not reveal more data than what is being queried is important at the same time. They propose an efficient two-level solution based on two cryptographic protocols: PIR and unconscious transfer. Our solution is general purpose and can use either a two level PIR [2] or it can use a combination of PIR and unconscious transfer. Their approach provides confidentiality for the user / client, does not use a trusted party or anonymizer, is protecting privacy and, compared to previous approaches, ensures that the server reveals the minimum data required and that the data is broadcast by the server is as fine or as accurate as possible [9]. Another method to avoid the use of a trusted anonymization is to use "fictitious locations" [7], [11]. The basic and plain idea is to obscure and garble the location of the user by sending a lot of random other locations to the server, so that the server cannot distinguish the actual location from the false locations.

Also studied for privacy in LBS are methods that work on encrypted or transformed data. For example, Khoshgozaran and Shahabi proposed a system that uses Hilbert curves to map places in a different space and then solves NN queries in transformed space [38]. A similar approach but using encryption has been proposed by Wong et al. In [3]. Their work focuses on outsourcing an encrypted database to a service provider and allows users to perform k-NN requests on the encrypted database. Their attention, however, is more about protecting the database instead of the privacy of the users. Similar work has been done in [40]. Some privacy techniques have attempted to use the TTP model for continuous LBS [2], [7], [1]. The idea of [2] is to keep the expansion of an initial camouflage zone to include at least the same users k, [7] is to predict a user's fingerprints and blur each fingerprint in a k-anonymised zone , And [41] is to use a mixing area to make the users located therein at the same time indistinguishable. The TTP model has been extended to protect the privacy of a group of anonymized users by generalizing their spatial request regions to make their queries indistinguishable [4] and ensuring that the number of their requested service values is at least m to obtain M-invariance [4]. Temporary encryption and encryption techniques are used for aggregated traffic data collection [4], but they cannot provide continuous LBS for privacy protection.

III. PROPOSED SYSTEM

The proposed architecture avoided the trusted third-party server. Thus, it is useful to overcome the limitations of current LBS privacy techniques, such as the requirement of a fully reliable third party, offering limited confidentiality and high communication costs. The, safe-tracker will update each tracking location of current users within a limited range. A continuous range request is defined as follows the trace of the POIs within a range of distance specified by the user of the user's current location (xu, yu) for a certain period of time. Location details are also encrypted (latitude and longitude of location details and digits) using homomorphic encryption.

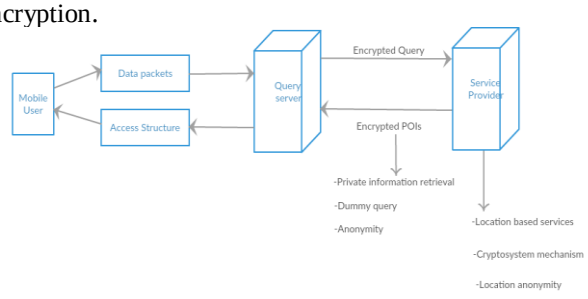

Figure 1 Proposed Architecture

In DGS, a query user first determines a query box, where the user is comfortable revealing the fact that it is somewhere in that query box. The query area is divided into grid cells of equal size based on the dynamic grid structure specified by the user.

The user then encrypts a request that includes the request area information and the dynamic grid structure and encrypts the identity of each grid cell intersecting the required search area of the spatial request to produce a set of identifiers Encrypted.

Then, the user sends a request comprising (1) the encrypted request and (2) the encrypted identifiers to QS, which is a semi-reliable part located between the user and SP. QS stores the encrypted IDs and transmits the encrypted request to the SP specified by the user. SP decrypts the query and selects the POIs in the query box from its database.

For every POI that is selected, SP encrypts the information using a dynamic grid structure as defined by the user to find a grid cell covering the POI and encrypts the identity of the cell to produce the encrypted identifier for that POI. Encrypted POIs with their corresponding encrypted IDs are returned to QS. QS stores all the encrypted POIs and returns to the user only a subset of encrypted POIs whose corresponding identifiers correspond to one of the encrypted identifiers originally sent by the user. Once the user receives the encrypted POIs, it decrypts them to get their exact location and calculates a query response.

IV. HOMOMORPHIC ENCRYPTION

The aspect of security and confidentiality must intervene to protect the data of each company. Secure storage and processing of data requires the use of a modern aspect of cryptography that has processing criteria such as the time required to respond to any request sent by the client and the size of the encrypted data that will be stored on The Cloud server. The proposed system suggests encrypting the data before sending it to the cloud provider, but to perform the calculations, the data must be decrypted whenever we need to work on it. Until now, it was impossible to encrypt the data and trust a third party to keep them safe and able to perform remote calculations on them. Therefore, to allow the Cloud provider to perform operations on encrypted data without decrypting them, cryptosystems based on homomorphic encryption must be used.

Homomorphic encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decipher the result of an operation, it is the same thing as if we had done the calculation on the raw data, that is, in plain text.

An encryption is homomorphic, if, from E(a) and E(b) it is possible to compute E(f(a,b)), where f can be: +, ×, ⊕ and without using the private key. Homomorphic encryptions are distinguished according to the operations that allows to assess on raw data, the additive Homomorphic encryption allows only additions of the raw data and is known is the Pailler cryptosystem and Goldwasser- Micalli cryptosystems, and the multiplicative Homomorphic encryption allows only products on raw data is the RSA and El Gamal cryptosystems.

A. *Additive Homomorphic Encryption*

A Homomorphic encryption is additive, if,

$$E(x \oplus y) = E(x) \otimes E(y)$$

$$E\left(\sum_{i=1} m_i\right) = \prod_{i=1} E(m_i)$$

Suppose we have two ciphers C_1 and C_2 such that,

$C_1 = g^{m1} . r_1^n \mod n^2$

$C_2 = g^{m2} . r_2^n \mod n^2$

$C_1 . C_2 = g^{m1} . r_1^n . g^{m2} . r_2^n \mod n^2 = g^{m1+m2} . (r_1 r_2)^n \mod n^2$

So, Pailler cryptosystem realizes the property of additive Homomorphic encryption. An application of an additive Homomorphic encryption is electronic voting: Each vote is encrypted but only the "sum" is decrypted.

B. *Multiplicative Homomorphic Encryption*

A Homomorphic encryption is multiplicative, if,

$$Enc(x \otimes y) = Enc(x) \otimes Enc(y)$$

$$E\left(\prod_{i=1} m_i\right) = \prod_{i=1} E(m_i)$$

Suppose we have two ciphers C_1 and C_2 such that,

$C_1 = m_1^e \mod n$

$C_2 = m_2^e \mod n$

$C_1 . C_2 = m_1^e \, m_2^e \mod n = (m_1 m_2)^e \mod n$

The client sends the pair (C_1,) to the Cloud server, the server will perform the calculations requested by the client and sends the encrypted result (C_1 *) to the client.

V. K-NEAREST-NEIGHBOR QUERIES

Similar to continuous range requests, confidentiality query processing for continuous k-NN requests has two main phases. The first phase finds an initial (or instant) response, while the second phase maintains the correct response when the user moves using incremental updates. However, unlike interval queries, the search area required for a k-NN query is unknown to a user until the user finds at least k POIs to calculate a required search area, That is to say a circular zone centered at the location of the user with a radius of the user at the nearest k-th POI. Thus, the k-NN query processing protocol that preserves confidentiality is slightly different.

If at least k encrypted POIs are returned to the user, they can be decrypted to calculate a search area required for the k-NN query in the form of a circle centered at the user's location with a radius of The distance between the user and the nearest K-th POI. On the other hand, if less than k POIs are returned, the user starts the next iteration by asking the QS grid cells a jump further away from the user's position, ie the cells Adjacent to the grid cells that have already been requested by the user.

This incremental search process is repeated (i.e. by requiring more cells to move progressively outward from the user's position) until the user has obtained at Minus k POI of QS. When the user determines the required search area, there are two possibilities:

1) The user has already requested all cells that cross the required search area. In this case, the user proceeds to the next step.

2) The required search area cuts off some cells that have not yet been requested from QS. The POIs (at least) found so far may in this case not be an exact answer and the user requests these QS cells that intersect the requested search area but have not yet been requested. After receiving all encrypted POIs in the newly requested QS cells, the user proceeds to the next step.

VI. CONCLUSION

In this paper, we proposed a dynamic grid system (DGS) to ensure confidentiality by maintaining continuous LBS. Our DGS includes the query server (QS) and service provider (SP), as well as cryptographic functions to split the query processing task into two parts that are executed separately by QS and SP. DGS does not require any trusted third party (TTP); On the contrary, we only ask for the much lower hypothesis of absence of collusion between QS and SP. This separation also moves the data transfer load from the user to the inexpensive, high bandwidth link between QS and SP. We also designed effective protocols so that our DGS can support continuous k-neighbor-neighbor (NN) and distance requests. To evaluate the performance of the DGS, we compare it to the most recent technique requiring a TTP. DGS offers better protection of privacy than the TTP system, and

The results show that the DGS is an order of magnitude more efficient than the TTP system, in terms of communication costs. In terms of computational cost, DGS also always outperforms the TTP scheme for NN requests; It is comparable or slightly more expensive than the TTP schema for range requests.

ACKNOWLEDGMENT

I would like to thank Principal. Dr. S.K. Biradar, MSSCET for the support & guidance throughout the project.

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.
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.
16. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "Providing kanonymity in location based services," SIGKDD Explor. Newsl., vol. 12, pp. 3–10, November 2010.
17. D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO, 2001.
18. Menezes, M. Qu, and S. Vanstone, "Some new key agreement protocols providing mutual implicit authentication," in SAC, 1995.
19. S. Yau and H. An, "Anonymous service usage and payment in servicebased systems," in IEEE HPCC, 2011, pp. 714–720.
20. M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, "Where's that phone?: Geolocating ip addresses on 3G networks," in ACM SIGCOMM IMC, 2009.
21. R. Dingledine, N. Mathewson, and P. Syverson, "Tor: the secondgeneration onion router," in USENIX Security, 2004.
22. G. Bissias, M. Liberatore, D. Jensen, and B. Levine, "Privacy vulnerabilities in encrypted HTTP streams," in PET, 2006.
23. P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in Pervasive Computing, 2009.
24. IEEE, P1363-2000: Standard Specifications for Public-Key Cryptography, 2000.
25. B. Lewko and B. Waters, "Efficient pseudorandom functions from the decisional linear assumption and weaker variants," in ACM CCS, 2009.

AUTHOER PROFILE

Jyoti Ganeshrao Pawar, currently pursuing M.Tech in Matsyodari Shikshan Sansthas College of Engineering and Technology, Aurangabad, Maharashtra. Area of research is Data Mining.

Gajanan Pilajirao Chakote (M.Tech, SIT) is HOD of Computer Science, Matsyodari Shikshan Sansthas College of Engineering and Technology, Aurangabad, Maharashtra.