ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 12 , December 2015

Protecting and Preserving Private Content of Location Based Services-A Review

Shweta Amrutkar, Prof.M.M.Naoghare

P.G. Student, Department of Computer Engineering SVIT, Chincholi, Maharashtra, India

Assistant Professor, Department of Computer Engineering SVIT, Chincholi, Maharashtra, India

ABSTRACT: The system secures the user's location data i.e. data from GPS devices and other devices indicate the user's current location. The system treats the location data and other data related to user as confidential data and will provide the security to the confidential data when it is in network or when location server. Location Based Services (LBS) uses multiple devices like mobile phones and tables to finding the various places and control features using the location data obtained using Global Positioning System (GPS) and. So, at the time when the user is using LBS from the location server, security to the location data will be provided. In previous paper, the security is provided by using Symmetric key encryption algorithm which uses symmetric key for both the ends. The problem in symmetric algorithm is that key remains same for both ends. The proposed system will use Asymmetric key encryption for encrypting the user's location data and it then can be used to query the location server after decrypting the location data at location server. Asymmetric key algorithm uses deferent keys for both ends i.e. private and public key. Also the response from the location server can be encrypted using Asymmetric key (public key) and can be read by user who requested for LBS after decrypting it with asymmetric key (private key). Hence, the system will provide security at user end and location server end.

KEYWORDS: Location based services, Asymmetric key, Point of interest (POI), oblivious transfer.

I. INTRODUCTION

A location based service (LBS) is an information, entertainment and utility service generally accessible by mobile devices such as, mobile phones, GPS devices, pocket PCs, and operating through a mobile network. LBS can over many services to the users based on the geographical position of their mobile device. The services provided by LBS are typically based on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to - discovering the nearest ATM machine, gas station, hospital, or police station. In recent years there has been a dramatic increase in the number of mobile devices querying location servers for information about POIs. Among many challenging barriers to the wide deployment of such application, privacy assurance is a major issue. For instance, users may feel reluctant to disclose their locations to the LBS, because it may be possible for a location server to learn who is making a certain query by linking these locations with a residential phone book database, since users are likely to perform many queries from home. The Location Server (LS), which over's some LBS, spends its resources to compile information about various interesting POIs. Hence, it is expected that the LS would not disclose any information without fees. [1] Therefore the LBS have to ensure that LSs data is not accessed by any unauthorized user. During the process of transmission the users should not be allowed to discover any information for which they have not paid. It is thus crucial that solutions be devised that address the privacy of the users issuing queries, but also prevent users from accessing content to which they do not have authorization. The first solution to the problem was proposed by Beresford, in which the privacy of the user is maintained by constantly changing the users name or pseudonym within some mix-zone. It can be shown that, due to the nature of the data being exchanged between the user and the server, the frequent changing of the users name provides little protection for the user's privacy. A more recent investigation of the mix-zone approach has been applied to road networks. They investigated the required number of users to satisfy the unlink ability property when there are repeated queries over an interval. This requires careful control of how many users are contained within the mix-zone, which is difficult to achieve in practice. A complementary technique to the mix-zone approach is based on k-anonymity. The concept of k-anonymity was introduced as a method for preserving privacy when releasing sensitive records. This is achieved by generalization and suppression algorithms to ensure that a record could not be distinguished from (k-1) other records. The solutions for LBS use a trusted anon miser to provide anonymity for the

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 12 , December 2015

location data, such that the location data of a user cannot be distinguished from (k-1) other users. An enhanced trusted anon miser approach has also been proposed, which allows the users to set their level of privacy based on the value of k. This means that, given the overhead of the anon miser, a small value of k could be used to increase the efficiency. Conversely, a large value of k could be chosen to improve the privacy, if the users felt that their position data could be used maliciously. Choosing a value for k, however, seems unnatural. There have been efforts to make the process less artificial by adding the concept of feeling-based privacy. Instead of specifying a k, they propose that the user species a cloaking region that they feel will protect their privacy, and the system sets the number of cells for the region based on the popularity of the area. The popularity is computed by using historical footprint database that the server collected.[3]

II. LITERATURE STUDY

"Protecting Privacy Against Location-based Personal Identification" Claudio Bettini, X. Sean Wang, and Sushil Jajodia proposed the privacy issues involved in accessing location based services, i.e., services that, based on the user current position, can provide location aware information. Typical examples are map and navigation services, services that provide information on close-by public resources (e.g., gas stations, pharmacies, ATM machines,)as there are currently over 1.5 billion mobile phone users worldwide and the numbers are still growing very fast[13]

"Measuring Query Privacy in Location-Based Services" Xihui Chen and Jun Pang propose new metrics to measure users query privacy taking into account user proles. Furthermore, we design spatial generalization algorithms to compute regions satisfying user's privacy requirements expressed in these metrics. [2]

"The PROBE Framework for the Personalized Cloaking of Private Locations" Maria Luisa Damiani, Elisa Bertino , Claudio Silvestri showed a system of a common strategy, referred to as obfuscation (or cloaking), to protect location privacy is based on forwarding the location based service provider a coarse user location instead of the actual user location, as there was The widespread adoption of location-based services raises increasing concerns for the protection of personal location information.[5]

"A Formal Model of Obfuscation and Negotiation for Location Privacy" Matt Duckham and Lars Kulik argues that we argue that obfuscation is an important technique for protecting an individual's location privacy within a pervasive computing environment. Negotiation is used to ensure that a location-based service provider receives only the information it needs [3] to know in order to provide a service of satisfactory quality [14]

"Location Privacy in Mobile Systems A Personalized An on imitation Model" BugraGedik, Ling Liu describes a personalized k-anonymity model for protecting location privacy against various privacy threats through location information sharing. Their model has two unique features. First, they provide a unied privacy personalization framework to support location k-anonymity for a wide range of users with context-sensitive personalized privacy requirements.

Second, they devised an efficient message perturbation engine which runs by the location protection broker on a trusted server and performs location an ony mization on mobile users LBS (Location Based Server)request messages, such as identity removal and spatiotemporal cloaking of location information. They developed a suite of scalable and yet efficient spatio-temporal cloaking algorithms, called Clique Cloak algorithms, to provide high quality personalized location k-anonymity, aiming at avoiding or reducing known location privacy threats before forwarding requests to LBS providers. [12]

"Approximate and exact hybrid algorithms for private nearest-neighbour queries with database protection" Gabriel Ghinita1, Panos Kalnis, Murat Kantarcioglu, and Elisa Bertino proposed a hybrid, two-step approach to private location-based queries, which provides protection for both the users and the database. In the first step, user locations are generalized to coar segrained cloaking regions s which provides strong privacy. Second a PIR protocol is applied with respect to the obtained query cloaking regions. To protect excessive disclosure of points of interest locations Experimental results show that the hybrid approach is scalable in practice, and clearly outperforms the pure- private information retrieval approach in terms of computational and communication overhead.[6]

"Private Queries in Location Based Services: Anonymizers are not Necessary" Gabriel Ghinita, PanosKalnis, Ali Khoshgozaran, Cyrus Shahabi, Kian-Lee Tan e proposed a novel framework to support private location dependent queries, based on the theoretical work on Private Information Retrieval (PIR). Their framework does not require a trusted third party, since privacy is achieved via cryptographic techniques. Compared to existing work, their approach achieves stronger privacy for snapshots of user locations; moreover, it is the first to provide provable privacy guarantees against correlation attacks. [10]

"Protecting Location Privacy through Path Confusion" Baik Hoh and Macro Grusteser proposed a path perturbation algorithm which can maximize users' location privacy given a quality of service constraint. This work concentrates on a class of applications that continuously collect location samples from a large group of users, where just removing user

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 12 , December 2015

identiers from all samples is insufcient because an adversary could use trajectory information to track paths and follow users' footsteps home. [15]

"Preventing Location-Based Identity Inference in Anonymous Spatial Queries" Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis, and Dimitris Papa dispersants a framework for preventing location based identity inference of users who issue spatial queries to Location Based Services. They propose transformations based on the well-established K-anonymity concept to compute exact answers for range and nearest neighbour search, without revealing the query source. Their methods optimize the entire process of anonymizing the requests and processing the transformed spatial queries. [11]

"A Hybrid Technique for Private Location-Based Queries with Database Protection" Gabriel Ghinita, PanosKalnis, Murat Kantarcioglu, and Elisa Bertino proposed a hybrid, two-step approach to private location-based queries, which provides protection for both the users and the database. In the rst step, user locations are generalized to coarse-grained cloaking regions (CR) which provide strong privacy. Next, a PIR protocol is applied with respect to the obtained query CR. To protect excessive disclosure of point of interest (POI) locations, we devise a cryptographic protocol that privately evaluates whether a point is enclosed inside a rectangular region. We also introduce an algorithm to efficiently support PIR on dynamic POI sub-sets. Our method discloses O(1) POI, orders of magnitude fewer than CR based techniques.[8]

"Time Warp: How Time Aects Privacy in LBSs". Roberto Di Pietro, Bruno Crispo , and Mauro contribution of this work is to highlight the importance of the time when providing privacy in LBSs. Further, we show how applying our considerations user privacy can be violated in the related model, but also in a relaxed one. We support our claim with both analysis and a practical counter-example. [7]

III. SYSTEMS IMPLEMENTATIONS

A. Existing System

In the previous system LBS (Location Based Service) have become one of the useful services in the. LBS used the location data as an input to provide its services to the users. But, due to the sharing of location data over the network, the location data needs to be securing from other parties and also from location server which itself is responsible for providing the LBS services. Here only security is provided at one end and there is no security implemented for both ends.

B.Proposed System

In the proposed system, it can be implemented by providing the security to the location data. In the existing systems, the security is provided by using Symmetric key encryption algorithm which uses symmetric key for both the ends. The problem in symmetric algorithm is that key remains same for both ends. The proposed system will use Asymmetric key encryption for encrypting the user's location data and it then can be used to query the location server after decrypting the location data at location server. Asymmetric key algorithm uses different keys for both ends i.e. private and public key. Also the response from the location server can be encrypted using Asymmetric key (public key) and can be read by user who requested for LBS after decrypting it with asymmetric key (private key). Hence, the system will provide security at user end and location server end. Proxy server is also a key feature of the proposed architecture. As any user doesn't send request to the Location Based Server. It goes through proxy server so any intruder spying on the LBS can't read the location of the User.

C. Future Implementation

After encrypting the location data, user is then allowed to send the encrypted data towards the location server through proxy server, When location server receives the encrypted location data, it decrypts the location data using its private key and searches for the user queried like finding the Point Of Interest (POI).Location server then creates the response and encrypts the response using public key provided by user/owner .Encrypted response is then forwarded to the respective user through network (Internet).At the user end, encrypted the data is then decrypt by users/owners private key. If user sends same request repetitively, there will be no need to send data to LBS. Proxy server will do the job of LBS and directly reply to User. So it will be time saving and safer.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 12 , December 2015

D. Modules

User/owner retrieves his/her location data (Longitude, Latitude) from the devices like mobile, tablet, pocket pc which contains inbuilt GPS device. User then encrypts the location data.

• **Public key:** provided by location server is used for encrypting the location data, user is then allowed to send the encrypted data towards the location server.

• **Point of Interest (POI):** When location server receives the encrypted location data, it decrypts the location data using its private key and searches for the user queried like finding the Point of Interest (POI). The ultimate goal of our protocol is to obtain a set (block) of POI records from the LS, which are close to the users position, without compromising the privacy of the user or the data stored at the server.

• **Private Information Retrieval Phase:** Our transfer phase can be repeatedly used to retrieve points of interest from the location database. With these functions described, we can build security. The user can initiate a private information retrieval protocol with the location server to acquire the encrypted POI data.

• **Oblivious Transfer Phase:** The purpose of this protocol is for the user to obtain one and only one record from the cell in the public grid .We achieves this by constructing a 2-dimensional oblivious transfer. Location server then creates the response and encrypts the response using public key provided by user/owner. Encrypted response is then forwarded to the respective user through network (Internet).At the user end, encrypted the data is then decrypt by users/owners private key. Hence, using the asymmetric encryption algorithm at both ends (server and client), data is transferred securely through network.

• **Client's Security:** The information that is most valuable to the user is his/her location. This location is mapped to a cell. In both phases of our protocol, the oblivious transfer based protocol and the private information retrieval based protocol, the server must not be able to distinguish two queries of the client from each other.

• **Server's Security:** The server's security requires that the client can retrieve one record only in each query to the server, and the server must not disclose other records to the client in the response. Our protocol achieves the server's security in the oblivious transfer phase

E. Techniques:

Diffe-Hellman Key Exchange establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network. It is a public key distribution system, a concept developed by Merkle, and hence should be called 'Diffe-Hellman Merkle key exchange. The parties agree on the algorithm parameters p and g. The parties generate their private keys, named a, b, and c.

• A computes ga and sends it to B.
• B computes (ga)b = gab and sends it to C.
• C computes (gab)c = gabcand uses it as her secret.
• B computes gb and sends it to C.
• C computes (gb)c = gbc and sends it to A.
• A computes (gbc)a = gbca = gabc and uses it as her secret.
• C computes gc and sends it to A.
• A computes (gc)a = gca and sends it to B.
• B computes (gca)b = gcab = gabc and uses it as his secret.

An eavesdropper has been able to see ga, gb, gc, gab, gac, and gbc, but cannot use any combination of these to efficiently reproduce gabc. To extend this mechanism to larger groups, two basic principles must be followed:

• Starting with an "empty" key consisting only of g, the secret is made by raising the current value to every participant's private exponent once, in any order (the first such exponentiation yields the participants own public key).

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 12 , December 2015

F. System Architecture

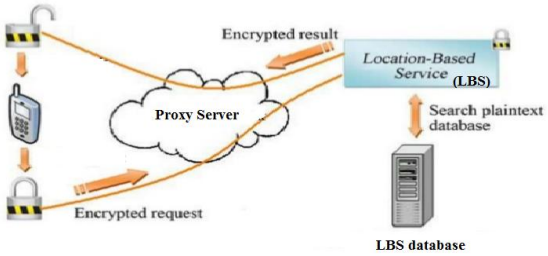

Figure 3.1: Location transfer at both the ends-Client and Server side

Figure 3.1 shows the Location transfer at both the ends-Client and Server side. User/owner retrieves his/her location data (Longitude, Latitude) from the devices like mobile, tablet, pocket pc which contains inbuilt GPS devices. User then encrypts the location data with the public key provided by location server. After encrypting the location data, user is then allowed to send the encrypted data towards the location server. When location server receives the encrypted location data, it decrypts the location data using its private key and searches for the user queried like finding the Point of Interest (POI).Location server then creates the response and encrypts the response using public key provided by user/owner. Encrypted response is then forwarded to the respective user through network (Internet).At the user end, encrypted the data is then decrypt by users/owners private key. Hence, using the asymmetric encryption algorithm at both ends (server and client), data is transferred securely through network.

IV. CONCLUSION

Traditional way to use the location aware system is not secure and it can be very harmful to the user's privacy. To overcome this, the new frame works in which need not to change the architecture of the LBS server. By using better encryption algorithm, it hides the user septic data from the server by using the proxy server along with encryption security. Future work will involve testing the protocol on many different mobile devices. The mobile result we provide may be different than other mobile devices and software environments. There is need to reduce the overhead of the primarily test used in the private information retrieval based protocol.

REFERENCES

[1] Russell Paulet, Md. GolamKaosar, Xun Yi, and Elisa Bertino, "Privacy Preserving and Content-Protecting Location Based Queries" in IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 5, MAY 2014,pp.1200-1210
[2] X. Chen and J. Pang, "Measuring query privacy in location-based services," in Proc. 2nd ACM CODASPY, San Antonio, TX, USA, 2012, pp. 49-60.
[3] R. Paulet, M. GolamKaosar, X. Yi, and E. Bertino, "Privacy preserving and contentprotecting location based queries,"in Proc. ICDE, Washington, DC, USA, 2012, pp. 44-53.
[4] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in Proc. ICDE, Hannover, Germany, 2011, pp. 494505.
[5] M. Damiani, E. Bertino, and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations," Trans. Data Privacy, vol. 3, no. 2, pp. 123148, 2010.
[6] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 128, 2010.
[7] "Time Warp: How Time Aects Privacy in LBSs" Luciana Marconi, Roberto Di Pietro, Bruno Crispo , and Mauro Conti ,LNCS 6476, pp. 325339, 2010.
[8] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in Proc. Adv. Spatial Temporal Databases, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98116, LNCS 5644.
[9] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services," in Proc. 16th ACM CCS, Chicago, IL, USA, 2009, pp. 348357.
[10] 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, Van 22
[11] 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. 17191733, Dec. 2007.
[12] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proc. ICDCS, Columbus, OH, USA, 2005, pp. 620629.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 12 , December 2015

[13] Bettini, X. Wang, and S. Jajodia, "Protecting privacy against location-based personal identication," in Proc. 2nd VDLB Int. Conf. SDM, W. Jonker and M. Petkovic, Eds., Trondheim, Norway, 2005, pp. 185199, LNCS 3674.
[14] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243251, LNCS 3468.
[15] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in Proc. 1st Int. Conf. Secure Comm, 2005, pp. 194205.