A survey on preserving user data privacy on location based services

HARISHA D K[1] UMASHANKER M L[2]

***Abstract.*-Due to the large increasing use of Location Based Services (LBS), which require personal data of the user to provide the continuous service, protecting the privacy of these data has become a challenge. An approach to preserving a privacy is through anonymity, by hiding the identity and user location data of the mobile device from the service provider(third party) or from any unauthorized party who has access at the user's request .Considering the challenge mentioned, in this paper gives a classification according to the Architecture, approaches and techniques used in previous works, and presents a survey of solutions to provide anonymity in LBS including the open issues or possible improvements to current solutions. All of this, in order to provide guidelines for choosing the best solution approach to a specific scenery in which anonymity is required.**

Keywords: Dynamic grid system, cloaking areas, location based services, Encryption ,privacy.

I. INTRODUCTION

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 interest places(e.g., restaurants and hotels, hospitals), 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

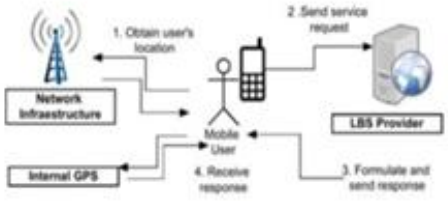

Fig1: Location Based Services General Architecture with entities that participating

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[1].A number of approaches have recently been proposed for preserving the user location privacy in LBS.

Manuscript received March, 2016.

Harisha D K *,Department Of Computer Science, Visvesvaraya Technological University, Bengaluru, India,*

Umashankar M L*, Department Of Computer Science, Visvesvaraya Technological University, Bengaluru, India ,*

The mobile device location information consists of latitude and longitude coordinates determined by a geo-location(GPS) technique that can be implemented directly on the mobile device or with the active participation of the network infrastructure. In general, a LBS architecture works as follows:

1.The mobile user having internal hardware to get the location data from the network

2.This collected data (latitude and longitude)is passed or send to LBS service provider for computation

3.The service provider receive a request from user and processing the request and send a response to the user corresponding to the request

4.In the other side of the user mobile having internal GPS to locate the exact location.

The proposed solutions in the literature aim to provide the service as well as privacy to the user at the same time. These solutions can be either classified by the entities that participate in the solution or the technique they use. The rest of the paper is organized as follows: Section 2 presents a proposed classification for the solutions that provide privacy in LBS. Section 3 and 4 summarize some of the solutions to anonymity that have been presented in other articles, classifies the presented solutions by two approaches: cryptographic and not- cryptographic and then points out in each of them which architectural approach they implement. Section 5 gives a conclusion on the survey and possible future work.

II. CLASSIFICATION OF SOLUTIONS

The solutions that provide anonymity can be classified either by the architecture (entities that participate to provide the solution) or by the techniques and methods they use.

2.1 Architectures To Provide Anonymity

The architectural solutions can be grouped into three categories [2] based on whether a third party is involved or not *independent architecture* The mobile device by itself computes its location; it hides its identity and location using its own capability and then sends the request to the LBS provider. This is the simplest architecture but in this architecture the performance of the process become decreasing because the mobile device itself compute and hide the location details its take more time to send the request to

In the below architecture mobile user as to hide the location details and send the request to the service provider service provider return back to mobile user with the results.to hide the user location data user has to use some cryptographic algorithm to encrypt the details of the user location.

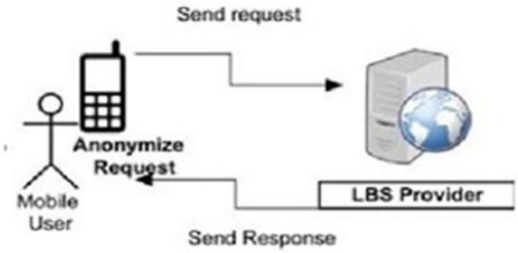

Fig2:Independent architecture

Centralized trust third party. It adds a trusted server that is responsible of performing the anonymzing technique, sending the request to the LBS provider and returning the result to the user. This approach is more robust in terms of privacy but the trusted server can become a potential bottleneck in the communication

TTP to be placed between the user and the service provider to hide the user's location information from the service provider [3], [4], [5], [6], [7], [8], [9]. 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. This TTP model has 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.

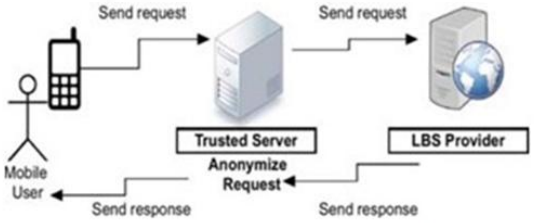

Fig 2.1: Centralized trusted third party

In the above centralized trusted third party user has to report their location to the server to obtain the LBS services if the TTP saves all the information of the user attacker can easily can get the details of the user

III. Proposed solutions using non-cryptographic approach

3.1 Fake Location Information

This set of solutions generally uses the independent architecture approach and the basic idea is to hide the user's real location among different fake locations generated at the client (some dummy queries.

The basic dummy technique [10] consists of a user sending its true position data along with several false position data(location) dummies to a service provider, who creates a reply message to all received position data. The user simply extracts the necessary information from the reply message. dummy generation algorithms are proposed.

The privacy-aware dummy-based technique (PAD) [10] seeks to improve the fact that in [11] they do not take into account the distances between dummies locations, thus they are not capable of controlling the area of the privacy region.

The problem with these solutions is that most of the algorithms require a lot of processing power from the mobile device to produce the fake locations. If the number of dummies generated is very high, the latency in the network can increase to processing all queries and produce a answer for the all queries include original and dummy queries this take an much processing power and time also this decrease in performance of the system

3.2 Spatial Cloaking

This technique is the most commonly used for protecting user location data from the third party attackers where in this technique extracted user location is blurred before submitting into service provider server for processing

The solution proposed in this area is further classified by the architectural approach

3.3 Semi Trusted Third Party (Dynamic Grid System)

To overcome the problem of in the above architecture propose a new architecture called dynamic grid system (DGS) [14] 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.

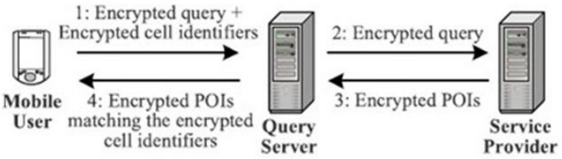

Fig 3: Architectural Diagram of DGS

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..

3.4 Obfuscation Techniques

This kind of solutions assumes the identification of users and introduces perturbations or inaccuracies into collected

locations to decrease their accuracy. In [15] the authors present three spatial obfuscation techniques to represent the user location as a circular region and using artificial perturbations of location information collected by sensing technology. The possible user locations are uniformly distributed within that region. The algorithm Matlock presented in [16], uses matrix obfuscation, transforming the space and temporal dimensions of the location information with a small number of arithmetic operations achieving in this way low computational resources used. In [17] path obfuscation techniques using hash chains and chains are presented. This solution is best suited for applications, which do not need to know the exact location of the user, but instead need to compute some metrics based on the information received (fitness apps, insurance apps). The user can choose to share the seed to de-obfuscate the path only to trusted users. In [21] the authors propose using a TTP to combine ambient conditions to obfuscate the location information. The TTP uses four mechanisms to achieve this goal: First it uses r-anonymity to generate r-1 trajectories similar to the real user, then it uses the k-1 metric to produce an area containing k users, in order to avoid areas with high density, it uses the s-segment paradigm to produce a cloaked region with real world conditions and finally it uses the time obfuscation approach to confuse the LBS randomizing the query issuing time.

IV. Proposed Solutions using Cryptographic Approach

This approach contains an establishing a secure channel for communication between service provider and user's ,to achieve a user data privacy on communication path need to establish a secure communication channel between two end points

4.1 Private Information Retrieval (PIR) OR Oblivious Transfer (OT).

In paper [19] the authors find the problem of protecting location privacy of the mobile user to an Oblivious transfer problem, where the issuer of the request receives only its corresponding reply and the service provider remains oblivious of the location of the user. Further on, they design some solutions based on different kinds of Oblivious Transfer (OT) namely Adaptive OT (implementing blind signatures), Dynamic OT and Proxy OT. They propose the solutions but do not provide any further analysis on the correctness or feasibility of their proposals. Based on [19], the authors in [20] propose an improved protocol by using two oblivious transfers where no third party is required to enable user's privacy. They assume the existence of a total server, which is responsible of a group of LBS providers. The user has to perform a double OT implemented with blind signatures in order to get the key required response to the query. This solution is thought for LBS that require payment.

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**.**

4.2 MQV(Key Arrangement Protocol)

MQV, is a signature-less AKE(Authentication key exchange) protocol. Key exchange, together with other basic primitives like encryption and signature, constitutes a building block of modern cryptography. Key exchange algorithms enable two parties communicating on an insecure channel to agree on a common secret value. Diffie-Hellman algorithm [21]

Several applications might benefit from an AKE protocol able to cope with a computing device. Mobile phones include smart cards which store the user authentication data; the handsets themselves are the computing devices. PCs equipped with a crypto token have a lot more computing power than the token itself, but may be plagued by spyware or viruses. New designs can also be devised. For example, using an AKE protocol secure in our model, one could build authenticated end-to-end encrypted communications in mobile phone networks: the handsets act as the authentication devices and the service provider as the computing devices. Session keys are negotiated between two handsets when a communication is initiated. With such a setup, the network operator knows session keys and can therefore decipher calls as required by the law, but is still unable to fake the users authentication.

In [22], all variants of HMQV including the 3-pass variant HMQV-C are proved

secure in the CK model, assuming intermediate scalar values are stored in protected memory, that is, out of reach of Session State queries. This is not very satisfactory as these values are inherently ephemeral. The protocol we propose is designed to overcome this drawback. Our security proof result can therefore be seen as an extension of what is proved in

4.3 Identity Based Encryption (IBE)

For an effective key management system these are all requirements 2] Authenticate users and decrypt data 3] Manage keys with partners 4] Deliver keys to trusted infrastructure components 5] Recover keys

Adi Shamir, one of the pioneers of public key cryptography, proposed a new type of public key algorithm in 1984. While public key systems have the inherent problem of distributing public keys and tying those public keys to a specific receiver. The scheme has chosen cipher text security in the random oracle model assuming a variant of the computational Diffie-Hellman problem. This system is based on bilinear maps between groups.

In this paper we propose a fully functional identity-based encryption scheme. The performance of our system is comparable to the performance of ElGamal encryption. The security of our system is based on a natural analogue of the computational Diffie-Hellman assumption. this assumption showed that the new system has chosen cipher text security in the random oracle model. Using standard techniques from threshold cryptography [23, 24] the PKG in our scheme can be distributed so that the master-key is never available in a single location.

IBE system can be built from any bilinear map G1_G1 ! We use the Weil pairing on elliptic curves as an example of such a map. Until recently the Weil pairing has mostly been used for attacking elliptic curve systems [25,26]. Joux [27] recently showed that the Weil pairing can be used

for good" by using it for a protocol for three party one round Diffie-Hellman key exchange. Sakai et al. [28] used the pairing for key exchange and Verheul [29] used it to construct an ElGamal encryption scheme where each public key has two corresponding private keys. In addition to our identity-based encryption scheme, we show how to construct an ElGamal encryption scheme with \built-in" key escrow, i.e., where one global escrow key can decrypt cipher texts encrypted under any public key

IBE system we define chosen cipher text security for identity based encryption. Our model gives the adversary more power than the standard model for chosen cipher text security [26, 29]. First, we allow the attacker to attack an arbitrary public key ID of her choice. Second, while mounting a chosen cipher text attack on ID we allow the attacker to obtain from the PKG the private key for any public key of her choice, other than the private key for ID. This models an attacker who obtains a number of private keys corresponding to some identities of her choice and then tries to attack some other public key ID of her choice. Even with the help of such queries the attacker should have negligible advantage in defeating the semantic security of the system

V. Conclusion

It is necessary to propose new models that address new threats and attack models, which seek to break user's privacy in Location Based Services. These new models need to overcome the disadvantages of existing ones. Novel solutions approaches could combine different proposed solutions, to compensate the disadvantages of certain models with the advantages of others.

The job of updating or proposing a new survey will remain as an open task, as the development of new solutions to protect user's privacy in Location Based Services remains active; moreover it is necessary to classify the solutions by the privacy degree they offer, the attack model(s) from which they are resilient and the type of LBS to which they can be applied.

REFERENCES

[1] Schiller, J. Voisard, A.: Location-Based Services. Morgan Kaufmann Publishers (2004)

[2] Mohaisen, A., Hong, D., Nyang, D.: Privacy in Location based services: Primitives toward the solution. NCM (2008)

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

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

[9]. Kido, H., Yanagisawa, Y., Satoh, T. An Anonymous Communication Technique using Dummies for Location-based Services. In: IEEE International Conference on Pervasive Services ICPS (2005) 88–97

[10]. Lu, H., Jensen, C.S., Yiu, M.L.: PAD: Privacy-Area Aware. Dummy-Based Location Privacy in Mobile Services MobiDE (2008) 16–23

[11]. Bamba, B., Liu, L., Pesti, P., Wang, T.: Supporting anonymous location queries in mobile environments with privacy grid. In: Proceedings of the International World Wide Web Conference, WWW (2008)

[12]. Gedik, B.,Liu, L.: Protecting location privacy with personalized k-anonymity: Architecture and algorithms. In: IEEE Transactions on Mobile Computing, TMC (2008) 1–18

[13]. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the International Conference on Mobile Systems,Applications, and Services, MobiSys (2003)

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

[15]. Ardagna, C. A., Cremonini, M., Damiani, E., De Capitani di Vimercati S., Samarati, P.: Location privacy protection through obfuscation based techniques. Data and Applications Security XXI, Volume 4602 (2007)

[16]. Wightman, P.M.; Jimeno, M.A; Jabba, D.; Labrador, M.: Matlock: A location obfuscation technique for accuracy-restricted applications. 2012 IEEE Wireless Communications and Networking Conference (WCNC) (2012)

[17]. Di Pietro, R., Mandati, R., Verde, N.V.: Track me if you can: Transparent obfuscation for Location based Services. 2013 IEEE 14th International Symposium and Workshops on World of Wireless, Mobile and Multimedia Networks (WoWMoM) (2013)

[18]. Hwang R., Hsueh , Y., Chung, H. A Novel Time-Obfuscated Algorithm for Trajectory Privacy Protection. IEEE Transactions on Services Computing (2014)

[19]. Kohlweis, M., Gedrojc, B.: Privacy friendly location based service protocols using efficient oblivious transfer. In: Workshop uber Kryptographie (2006) 1-4

[20]. Kohlweiss, M., Faust, S., Fritsch, L.: Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker. In: Proceedings of 7th Workshop on Privacy Enhancing Technologies, LNCS 4776 (2007) 77-94

[21] H. Krawczyk. HMQV: A High-Performance Di_e-Hellman Protocol. In Victor Shoup, editor, Proceedings of CRYPTO 2005, volume 3621 of LNCS, pages 546{566. Springer-Verlag, August 2005.

[22] P. Gemmell, \An introduction to threshold cryptography", in CryptoBytes, a technical newsletter of RSA Laboratories, Vol. 2, No. 7, 1997.

[23] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, \Secure Distributed Key Generation for
Discrete-Log Based Cryptosystems", Advances in Cryptology { Eurocrypt '99, Lecture Notes in Computer Science, Vol. 1592, Springer-Verlag, pp. 295{310, 1999.
[24] G. Frey, M. M□uller, H. R□uck, \The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems", IEEE Tran. on Info. Th., Vol. 45, pp. 1717{1718, 1999
[25] A. Menezes, T. Okamoto, S. Vanstone, \Reducing elliptic curve logarithms to logarithms in a _nite _eld", IEEE Tran. on Info. Th., Vol. 39, pp. 1639{1646, 1993.
[26] A. Joux, \A one round protocol for tripartite Di_e-Hellman", Proc. Fourth Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, Vol. 1838, Springer-Verlag, pp. 385{ 394, 2000.
[27] R. Sakai, K. Ohgishi, and M. Kasahara, \Cryptosystems based on pairings," In Proceedings of Symposium on Cryptography and Information Security, Japan, 2000.
[28] E. Verheul, \Evidence that XTR is more secure than supersingular elliptic curve cryptosystems", in Advances in Cryptology { Eurocrypt 2001, Lecture Notes in Computer Science, Vol. 2045, Springer-Verlag, pp. 195{210, 2001.
[29] M. Bellare, A. Desai, D. Pointcheval, P. Rogaway, \Relations among notions of security for public-key encryption schemes", in Advances in Cryptology { Crypto '98, Lecture Notes in Computer Science, Vol. 1462, Springer-Verlag, pp. 26{45, 1998.

