A Dynamic Privacy Aware Access Control Model for Location Based Services

Leila Karimi, Balaji Palanisamy, James Joshi
School of Information Sciences
University of Pittsburgh
Pittsburgh, PA, USA
{leila.karimi, bpalan, jjoshi}@pitt.edu

***Abstract*— The proliferation of Location Based Services (LBSs) and Geo Social Networks (GSNs) significantly increase the exposure risks of location information leading to leakage of sensitive information. Location privacy preserving methods are designed to provide a specified level of privacy based on some pre-defined privacy guarantees such as k-anonymity and ε-differential privacy. In certain situations, we note that users would need different privacy protection levels based on their relationships and trust associated with the users of the exposed location data. For instance, users of a location-based social network may need a lower privacy protection level during their interactions with their close friends and a higher privacy protection level when they interact with public users. In this paper, we propose a privacy aware access control model that provides different location privacy protection levels for users based on their needs. The proposed model also provides an efficient mechanism for grant and revoke of authorizations.**

I. INTRODUCTION

The recent prevalent use of mobile devices and the availability of high-resolution spatio-temporal data sensing devices have popularized the use of Location-Based Services (LBSs) and Location-based Geosocial Networks (GSNs). These location-based systems (e.g. Foursquare, Yelp, Google Latitude, and Facebook Places) provide services based on the location of their users. In a Location-Based Social Network (LBSN), users publish their location information through check-ins, share them with their friends and other users of the system. In addition, users can explore places around their current location and take advantage of the feedback and reviews provided by their friends and other users of the system. These introduce new security and privacy challenges in a LBS. For example, knowing user's check-ins at a specific hospital, an adversary may be able to infer the users disease or other sensitive health information about the user.

In a LBS, there are different kinds of privacy issues such as *Location Privacy*, *Absence Privacy*, *Co-Location Privacy* etc., that may cause serious privacy risks for the users [1]. Puttaswamy et al. in [2] report several incidents of location privacy leakage that have resulted in serious consequences for the users of location-based services. Besides users' online information that may invade their privacy, location-based service providers may publish their datasets for academic or industrial purposes which can lead to the disclosure of user's sensitive information. Naively anonymizing Geosocial Network datasets will not preserve users' privacy as they are subject to the risk of re-identification. Attackers may take advantage of their background knowledge (e.g. Top m locations of a user [3], location trajectory of a user, and location-based information of friends of a user) for re-identifying users in a GSN dataset. Differential privacy provides a more rigorous guarantee by bounding the adversary's ability to infer the sensitive information from the exposed differentially private information.

Although there have been several studies that tried to solve the location privacy problem, existing solutions have been designed to provide one specific level of location privacy protection to all users of the system without considering different levels of relationships and trusts that may exist between the users. For example, in an online social network, a user may have various categories of other users connected on the social network such as Close Friends, Friends, Family, Public, etc., with each of them having different levels of access to the user's information. A straight-forward privacy preserving mechanism may provide only a specific location privacy level without considering the access control imposed to the users in these lists. However, in such scenarios, users may prefer to reveal their exact location to Close Friends, an approximate location with small noise to other friends, and an approximate location with a larger amount of noise to Public users.

In this paper, we present a location privacy aware access control model that provides different levels of location privacy protection based on access control privileges of the users. We consider policy updates which may result in grant/revoke of authorizations and we present an analysis of the security properties and performance of the proposed model.

II. PRIVACY AWARE ACCESS CONTROL MODEL

In this section, We first briefly introduce the notion of differential privacy and then present our privacy aware access control model.

Differential Privacy [5] is a notion from the domain of statistical databases that preserves an individual's privacy when publishing aggregate information. Differential privacy bounds the adversary's ability to infer a single user's data in a dataset. This can be achieved by adding a controlled amount of noise to the query result. Differential privacy is formally defined as follows:

978-1-5090-4607-2/16 $31.00 © 2016 IEEE
DOI 10.1109/CIC.2016.82

Definition 1: A randomized function M gives ε-differential privacy if for all data sets D_1 and D_2 differing on a single user, and all $S \subseteq Range(M)$,

$$Pr[M(D_1) \in S] < exp(\varepsilon) \times Pr[M(D_2) \in S]$$

Differential privacy can be also extended to support location privacy. For example, Andrs et al. in [17] introduce the notion of geo-indistinguishability and presents a mechanism for achieving it by adding a controlled amount of noise to the users' location.

We next present our proposed privacy aware access control model that is inspired by [4] and is founded on Chinese Remainder Theorem (CRT) [7] for managing access to a piece of information which is intended to be shared among authorized users. In our model, the list of authorized users is specified by the access control list (ACL) of the owner of the information. We assume that a user's exact location l is represented by a rectangular region which is shown by a 4-tuple $l =< x,y,w,h >$, in which x and y are latitude and longitude of the top left corner of the region, and w and h are width and height of the region. A differentially private location privacy preserving mechanism may publish an approximate location of the user, $l' =< x',y',w',h' >$ by adding some amount of noise to the exact location, here the noise can be shown by $\varepsilon =< |x-x'|,|y-y'|,|w-w'|,|h-h'| >$. Based on different parameter settings in privacy preserving model, different approximate locations of the user's exact location can be published.

We assume a GSN in which each user has three access control list: Closed Friends, Friends, and Public Users. The user may prefer to publish his exact location to his Close Friends, but he may prefer to publish his approximate location (l') with a small amount of noise (i.e. ε) to his Friends, and he may want to publish another approximate location (l'') with larger amount of noise (e.g ε') to Public Users. A simple solution in this scenario is shown below:

The user publishes his approximate location l'' to all the users of the system and he will send ε and ε' to all of his Friends and his Closed Friends, respectively. In this way, his Friends can calculate his approximate location which contains small amount of noise (i.e. $l' = l'' - \varepsilon$) and his Closed Friends can calculate his exact location (i.e. $l = l'' - \varepsilon'$). We note that this is not an efficient solution and it may force high communication overload to the users of the system. Instead, by using CRT in the following way, the amount of communication overhead can be reduced using the following protocol:

Assume that one of the access control list of the user U is his Close Friends which is shown by: ${ACL^U}_{ClsFrnd} = \{u_1,u_2,\ldots,u_r\}$. We also assume that each user u_i of the system has been assigned a public and private key pairs (puk_i, prk_i), and a moduli n_i. Then, user U can solve the system of simultaneous congruences in (1), and publish the solution x_ε besides publishing his approximate location l":

$$\begin{cases} x_\varepsilon \equiv E_{puk_1}(\varepsilon) \ \ mod \ \ n_1 \\ x_\varepsilon \equiv E_{puk_2}(\varepsilon) \ \ mod \ \ n_2 \\ \quad \ldots \\ x_\varepsilon \equiv E_{puk_r}(\varepsilon) \ \ mod \ \ n_r \end{cases} \tag{1}$$

If any of the U's Close Friends (e.g. $u_i \in {ACL^U}_{ClsFrnd}$) needs to access ε, he/she can calculate it as follows:

$$E_{puk_i}(\varepsilon) \equiv x_\varepsilon \ \ mod \ \ n_i \tag{2}$$

$$\varepsilon = D_{prk_i}(E_{puk_i}(\varepsilon)) \tag{3}$$

As an illustrative example, let us consider that Alice (A) has two Close Friends: Bob (B) and Carol (C) and two more Friends: Dave (D) and Edward (E). The exact location of Alice is $l_A =< x,y,w,h >$ and the differentially private privacy preserving method has generated two approximates of her location ${l_A}' =< x',y',w',h' >$ and ${l_A}'' =< x'',y'',w'',h'' >$. $\varepsilon_A = l_A - {l'}_A$ and ${\varepsilon'}_A = l_A - {l''}_A$ are two noises related to these approximations where $\varepsilon_A < {\varepsilon'}_A$. Alice wants Public Users to have access to ${l''}_A$, her Friends to have access to ${l'}_A$ and her Close Friends to have access to l_A. She will publish ${l''}_A$ as an approximation of her location which is accessible by all users of the LBS. In addition, she needs to calculate and publish shared information $x_{{\varepsilon'}_A}$ and $x_{{\varepsilon''}_A}$ using CRT systems of simultaneous congruences shown in (4) and (5). Here ${\varepsilon''}_A = {l'}_A - {l''}_A = {\varepsilon'}_A - \varepsilon_A$.

$$\begin{cases} x_{{\varepsilon'}_A} \equiv E_{puk_B}({\varepsilon'}_A) \ \ mod \ \ n_B \\ x_{{\varepsilon'}_A} \equiv E_{puk_C}({\varepsilon'}_A) \ \ mod \ \ n_C \end{cases} \tag{4}$$

$$\begin{cases} x_{{\varepsilon''}_A} \equiv E_{puk_B}({\varepsilon''}_A) \ \ mod \ \ n_B \\ x_{{\varepsilon''}_A} \equiv E_{puk_C}({\varepsilon''}_A) \ \ mod \ \ n_C \\ x_{{\varepsilon''}_A} \equiv E_{puk_D}({\varepsilon''}_A) \ \ mod \ \ n_D \\ x_{{\varepsilon''}_A} \equiv E_{puk_E}({\varepsilon''}_A) \ \ mod \ \ n_E \end{cases} \tag{5}$$

If Bob wants to get the exact location of Alice, he has access to both ${l''}_A$ and $x_{{\varepsilon'}_A}$. He needs to calculate ${\varepsilon'}_A$ using equations in (6) and (7) and then he can get the exact location of Alice by calculating $l_A = {\varepsilon'}_A + {l''}_A$.

$$E_{puk_B}({\varepsilon'}_A) \equiv x_{{\varepsilon'}_A} \ \ mod \ \ n_B \tag{6}$$

$${\varepsilon'}_A = D_{prk_B}(E_{puk_B}({\varepsilon'}_A)) \tag{7}$$

In the same way, Dave can access ${l'}_A$ by solving equations (8) through (10):

$$E_{puk_D}({\varepsilon''}_A) \equiv x_{{\varepsilon''}_A} \ \ mod \ \ n_D \tag{8}$$

$${\varepsilon''}_A = D_{prk_D}(E_{puk_D}({\varepsilon''}_A)) \tag{9}$$

$${l'}_A = {\varepsilon''}_A + {l''}_A \tag{10}$$

On the other hand, Dave cannot access the exact location of Alice (l_A) as he has access to neither prk_B nor prk_c.

A. Policy Updates

In any information system, updating access control policies is a probable practice. These updates may be done through *Grant* and *Revoke* operations. In a GSN, it is common that users modify their relationships with other users. They may add a user to their Friend list (*Grant*) or on the other hand, they may remove a user from the list (*Revoke*). In both situations, the users access control list has been changed. The straightforward solution is to recalculate the shared information using CRT according to new access control list. However, when policy updates occur frequently in a LBS, these calculations may impose high overhead to the users of the system. Kong et al. in [4] suggest an efficient approach for updating policies. We discuss the method through an example.

In our previous example, if Alice (A) wants to add Frank (F) to her Close Friends, he can have access to her exact location and as a result, he should be able to calculate ε'_A having access to both l''_A and $x_{\varepsilon'_A}$. For this purpose, Alice needs to calculate and publish $x'_{\varepsilon'_A}$ which is the solution of the CRT systems of simultaneous congruences in (11).

$$\begin{cases} x'_{\varepsilon'_A} \equiv x_{\varepsilon'_A} \mod n_B n_C \\ x'_{\varepsilon'_A} \equiv E_{puk_F}(\varepsilon'_A) \mod n_F \end{cases} \tag{11}$$

On the other hand, if Alice wants to remove Edward (E) from her Friend list, he should not be able to calculate ε''_A anymore. For this purpose, Alice has to calculate the new shared information $x'_{\varepsilon''_A}$ as follows:

$$x'_{\varepsilon''_A} = x_{\varepsilon''_A} \mod n_B n_C n_D \tag{12}$$

We refer the interested readers to [4] for details on the security analysis of Grant and Revoke operations. Using this technique, users of a LBS system can easily modify their lists and hence update their access control policies.

III. Performance and Security Analysis

Based on Menezes et al [8], Garners Algorithm is an efficient algorithm for computing Chinese Remainder Theorem which has the time complexity of $O(kl^2)$ assuming that in Equation (1) each modulus n_i has l bits and the CRT solution x_ε has lk bits.

As we discussed in the previous section the grant operation needs a solution to a CRT with two equations to be calculated. Hence the complexity of grant operation is of $O(l^2)$. The revoke operation can be done with one modular operation which has the complexity of $O(kl^2)$.

Size of the CRT solution has a direct relationship with the number of equations (k) and the size of the modulus (l) in the system of simultaneous congruences in (1). As $0 \leq x \leq n = n_1 n_2 \ldots n_k$, the CRT solution is at most lk bits. As a result, in the proposed model, communication overhead which is due to transferring shared information ($x_{\varepsilon'_A}$ or $x_{\varepsilon''_A}$) is impacted by the size of access control list of the user and the size of each modulus. As in the CRT, $0 \leq a_i < n_i$ and size of each modulus should be greater than each ciphertext. If we choose a RSA cryptosystem in which the ciphertext has 1024 bits size, then the CRT moduli should also be of 1024 bits size and so the communication overhead will be $1024r$, here r is the size of access control list of the user.

The proposed model preserves the confidentiality of authorization policies of the users of the system, as knowing the shared information and moduli does not reveal any information about the access control list of the user. However, as the moduli in equation (1) are not private, the model may suffer from known plain text attacks, so it is important to employ an encryption algorithm which can protect against this kind of attacks.

IV. Related Work

Different approaches have been proposed to provide privacy preserving mechanisms for Location Based Services and Location-based geo-social Networks. Obfuscation or cloaking methods try to hide the exact location of the user through spatial cloaking algorithms [9]–[12]. The techniques based on k-anonymity and l-diversity build cloaking region by providing k-anonymity and l-diversity guarantees [13]–[16].

Differential Privacy is another approach for obfuscating users' location by adding a carefully calibrated noise [17], [18]. Some studies try to employ encryption techniques to provide location privacy [19]–[21]. Use of secret sharing [22] and TTP (Trusted Third Party) [23] are other mechanisms for preserving the privacy of users in a LBS.

Some studies try to provide security for users of a LBS through access control models and mechanisms. Common approaches are based on extending RBAC model [24]–[26]. Zue et. al. propose a cryptographic access control framework for a fine-grained spatio-temporal access control for Location Based Systems [27]. Tarameshloo's access control model is based on primitive spatial relations between users' locations in the system [28]. These techniques do not consider altering privacy parameters according to access control policies. Few works in the past consider dynamic privacy for relational databases, in which according to role's permissions (that are specified through queries), privacy parameters are set [29], [30], however, they are not applicable to the location privacy problem in the context of location based services as permissions are not defined by queries in these systems.

V. CONCLUSIONS

Despite the popularity of location based services and location-based geo-social networks, privacy issues in these systems remains an open challenge. In this work, we proposed a privacy preserving access control model which provides various location privacy protection levels based on different access privileges of users in a LBS. In addition, the model efficiently allows the users of the system to grant authorization to new users and revoke authorization from the existing ones.

ACKNOWLEDGMENT

This work was performed under a partial support by the National Science Foundation under the grant DGE-1438809.

REFERENCES

[1] C. R. Vicente, D. Freni, C. Bettini, & C. S. Jensen, Location-related privacy in geo-social networks, IEEE Internet Computing, vol. 15, no. 3, pp. 20-27, 2011.

[2] K. P. N. Puttaswamy and B. Y. Zhao, Preserving Privacy in Location-Based Mobile Social Applications, in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, 2010, pp. 16.

[3] A. Masoumzadeh and J. Joshi, "Top Location Anonymization for Geosocial Network Datasets," Transactions on Data Privacy, vol. 6, no. 1, pp. 107-126, 2013.

[4] Y. Kong, J. Seberry, J. R. Getta, and P. Yu, A Cryptographic Solution for General Access Control, in International Conference on Information Security, 2005, pp. 461-473.

[5] C. Dwork, Differential Privacy, in Proc. of ICALP, volume 4052 of LNCS, Springer, 2006, pp. 112.

[6] H. Zang and J. C. Bolot, Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study, in Proceedings of the 17th annual international conference on Mobile computing and networking, 2011, pp. 145-156.

[7] S. Y. Yan, Number Theory for Computing, 2nd Edition, Springer-Verlag, 2002.

[8] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography, CRC Press, 1996.

[9] M. L. Damiani, E. Bertino, and C. Silvestri, Protecting Location Privacy Through Semantics-Aware Obfuscation Techniques, in IFIP International Conference on Trust Management, 2008, pp. 231245.

[10] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, Preserving User Location Privacy in Mobile Data Management Infrastructures, in International Workshop on Privacy Enhancing Technologies, 2006, pp. 393412.

[11] C.-Y. Chow and M. F. Mokbel, Enabling Private Continuous Queries for Revealed User Locations, in International Symposium on Spatial and Temporal Databases, 2007, pp. 258275.

[12] M. Gruteser and D. Grunwald, Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking, in Proceedings of the 1st international conference on Mobile systems, applications and services, 2003, pp. 3142.

[13] B. Gedik and L. Liu, Location Privacy in Mobile Systems: A Personalized Anonymization Model, in 25th IEEE International Conference on Distributed Computing Systems (ICDCS05), 2005, pp. 620629.

[14] B. Gedik and L. Liu, Protecting Location Privacy with Personalized k-anonymity: Architecture and Algorithms, IEEE Trans. Mob. Comput., vol. 7, no. 1, pp. 118, 2008.

[15] F. Liu, K. A. Hua, and Y. Cai, Query l-diversity in Location-based Services, in 2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, 2009, pp. 436442.

[16] M. Xue, P. Kalnis, and H. K. Pung, Location Diversity: Enhanced Privacy Protection in Location Based Services, in International Symposium on Location-and Context-Awareness, 2009, pp. 7087.

[17] M. E. Andrs, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, Geo-indistinguishability: Differential Privacy for Location-Based Systems, in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 901914.

[18] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, Location Privacy via geo-indistinguishability, ACM SIGLOG News, vol. 2, no. 3, pp. 4669, 2015.

[19] M. Ashouri-Talouki, A. Baraani-Dastjerdi, and A. A. Seluk, GLP: A Cryptographic Approach for Group Location Privacy, Computer Communications, vol. 35, no. 12, pp. 15271533, 2012.

[20] Y. Sun, T. F. La Porta, and P. Kermani, A Flexible Privacy-enhanced Location-based Services System Framework and Practice, IEEE Trans. Mob. Comput., vol. 8, no. 3, pp. 304321, 2009.

[21] J. ednka and P. Gasti, Privacy-Preserving Distance Computation and Proximity Testing on Earth, Done Right, in Proceedings of the 9th ACM symposium on Information, computer and communications security, 2014, pp. 99110.

[22] M. Wernke, F. Drr, and K. Rothermel, PShare: Position Sharing for Location Privacy Based on Multi-Secret Sharing, in Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on, 2012, pp. 153161.

[23] D. Freni, C. Ruiz Vicente, S. Mascetti, C. Bettini, and C. S. Jensen, Preserving Location and Absence Privacy in Geo-Social Networks, in Proceedings of the 19th ACM international conference on Information and knowledge management, 2010, pp. 309318.

[24] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, GEO-RBAC: A Spatially Aware RBAC, in Proceedings of the tenth ACM symposium on Access control models and technologies, 2005, pp. 2937.

[25] F. Hansen and V. Oleshchuk, Spatial Role-Based Access Control Model for Wireless Networks, in In Proceedings of the 58th IEEE Vehicular Technology Conference (VTC03). Vol. 3. IEEE Computer Society, 2003.

[26] I. Ray, M. Kumar, and L. Yu, LRBAC: A Location-Aware Role-Based Access Control Model, in International Conference on Information Systems Security, 2006, pp. 147161.

[27] Y. Zhu, D. Ma, D. Huang, and C. Hu, Enabling Secure Location-Based Services in Mobile Cloud Computing, in Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing, 2013, pp. 2732.

[28] E. Tarameshloo and P. W. L. Fong, Access Control Models for Geo-social Computing Systems, in Proceedings of the 19th ACM symposium on Access control models and technologies, 2014, pp. 115126.

[29] Z. Pervaiz, W. G. Aref, A. Ghafoor, and N. Prabhu, Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data, IEEE Trans. Knowl. Data Eng., vol. 26, no. 4, pp. 795807, 2014.

[30] Z. Pervaiz, A. Ghafoor, and W. G. Aref, Precision-Bounded Access Control Using Sliding-Window Query Views for Privacy-Preserving Data Streams, IEEE Trans. Knowl. Data Eng., vol. 27, no. 7, pp. 19922004, 2015.