ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1115-1119), Month: April - June 2015, Available at: www.researchpublish.com

Privacy Preserving Location Based Messaging Service

[1]Sangeetha U, [2]Sanjay Kamar C K

[1]M. Tech Final Year Student, [2]Asst. Professor, [1]Computer Network Engineering, [2] PG Studies In CE & A NIE Mysuru, INDIA

Abstract: **Location-Based Service (LBS) is becoming popular with the growth of smartphones and social network services (SNS), and its context-rich functionalities attract enormous users. LBS providers use users' location information to provide them convenience and useful functions. The LBS could break through personal privacy because the location itself contains lot of information about the user. Hence, preserving location privacy is still a challenging issue. This paper proposes non-trivial challenge by designing a suite of Privacy-preserving Location based messaging services. This allows different levels of location requests on encrypted location information for different users, and it is efficient enough to be applied in mobile platforms.**

Keywords: **Location Based Services (LBS), Google maps, Social network services (SNS).**

I. INTRODUCTION

Location Based Service (LBS) has become one of the most popular mobile applications due to the wide use of smart phones. The smart phones, equipped with GPS modules, have powerful computation ability to process holders' location information, and this brought the flood of LBS applications in the Smartphone ecosystem. A good example is the Smartphone camera: if one takes a photo with a Smartphone camera, the location where the photo is taken is embedded in the picture automatically, which helps one's remembrance. Furthermore, the explosive growth of social network services (SNS) also assisted its growth by constructing connections between location information and social network. When a picture taken by a Smartphone (location embedded) is uploaded to the Face book album, the system automatically shows the location of the picture on the map, and this is shared with the owner's friends in the Facebook (unless the privacy setting specifies otherwise). Many similar applications exploit both LBS and SNS. For example, when Alice and Bob both use check-in application in Face book (which leaves a location record in one's webpage) in a nice restaurant, it is inferable that they are having a date and that they could be in a relationship. This inference might be an unintended information leakage from Alice's and Bob's perspective. Therefore, a privacy-preserving protocol is needed to prevent significant privacy breach resulted from the combination of LBS and SNS.

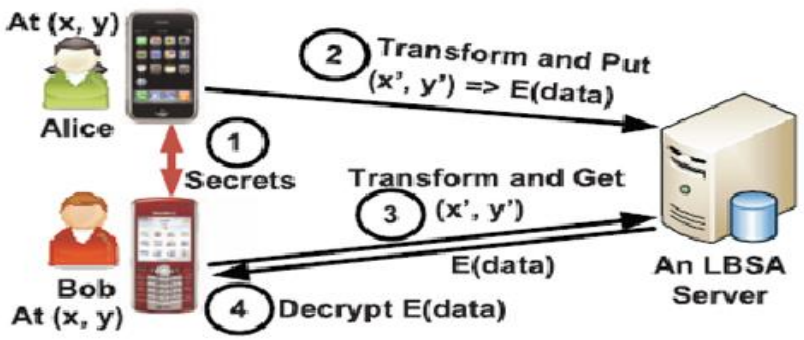

Fig. 1 Example location based service

Many applications are there who uses LBS and SNS and they provide a way to access a location published by someone using some grouped based access control mechanism. There are some social photo sharing website like Flickr and some SNS website like Facebook and Google++ that also provide location sharing or retrieving based facilities to the user.

A. EXISTING SYSTEM:

These applications propose a number of interesting things to enjoy to the user, but one big problem here is the location information of someone that contains the much information about that person to violate their privacy i.e., information leakage. For example suppose Alice and Bob (couples) are in a nice restaurant and as per them it is not good to disclose the relationship between them to others. But at the same time they both started using the check-in application in Facebook social network that post location information to the webpage. And for Bob and Alice, this information leakage may not be acceptable. On the other perspective suppose Alice wants to share the good moment to their friends and telling them the correct location. On the same time, suppose Alice wants to tell some of her friends about her date but she don't want to disclose her exact location to them, here some settings are needed to put these kind of condition to accomplish the Alice need.

Disadvantages of existing systems:

There are some pitfalls in the existing system,

- The location information can be accessed only limited list of users.
- Choice like user can have binary choices either enable or disable the discloser of the location information.
- Privacy leakage because of the server storing the information.

User disclosed all of his location information but steal on server the information may be opened. For solving this problem the concept of encrypted location is required

B. PROPOSED SYSTEM:

The proposed system uses Privacy-preserving Location Query Protocol (PLQP) that is fine-grained and which make possible to query location information with fulfilling the complete satisfaction of user and without leakage of any unintended information from the user. Some main contribution to this research are;

- In the place of selecting some user from a huge amount of contact list or selecting a group that is having some drawback.
- The protocol will allow to set the range of the location
- Once user is added as a friend in the list of any user he can get the location of that user anytime, just by sending a message.

Advantages of proposed system:

Location information will be encrypted so that one can query the location but the full control to location will be in under of publishers of location. Even the server will not able to understand the encrypted location information.

II. LITERATURE SURVEY

A. Profile Anonymization Model for Location Based Services:

In this paper[2],] Heechang Shin tells about a novel unified index structure, called the (PTPR- tree), which organizes both the locations of mobile users as well as their profiles using a single index, and as a result, offers significant performance gain during anonymization as well as query processing.] Heechang Shin presents and it address the problem of privacy preservation via anonymization. Prior research in this area attempts to ensure k-anonymity by generalizing the location. However, a person may still be identified based on his/her profile if the profiles of all k people are not the same. We extend the notion of k-anonymity by proposing a profile based k-anonymization model that guarantees anonymity even when profiles of mobile users are known to untrusted entities. The main advantage of this method is adding attachment to tell about the location profile and main drawback of this paper is difficult to maintain the large set of records in limited server.

B. Preserving Anonymity of Recurrent Location-Based Queries:

In this paper[4], C. B. D. Riboni, L. Pareschi and S. Jajodia provides a formal model of the privacy threat, and it proposes an incremental defense technique based on a combination of anonymity and obfuscation.] C. B. D. Riboni, L. Pareschi and S. Jajodia shows the effectiveness of this technique by means of an extensive experimental evaluation. The anonymization of location based queries through the generalization of spatio-temporal information has been proposed as a privacy preserving technique. According to C. B. D. Riboni, L. Pareschi and S. Jajodia, they shows that the presence of multiple concurrent requests, the repetition of similar requests by the same issuers, and the distribution of different service parameters in the requests can significantly affect the level of privacy obtained by current anonymity-based techniques. The advantage of this method is highly suitable for preserving Secrecy about the user‟s location and drawback is confusion occurs while the user is large and the resource is large.

C. Mix Zones: User Privacy in Location-Aware Services:

In that paper [1], Alastair R. Beresford and Frank Stajano refine a method, called the mix zone, developed to enhance user privacy in location-based services. it improves the mathematical model, examine and minimize computational complexity and develop a method of providing feedback to users. The main advantage of this method is adding privacy to user searches and drawback is number of user is restricted at certain level. So it hard to find results for large number of users.

D. Exploring Historical Location Data for Anonymity Preservation in Location-Based Services:

In this paper [3], .Xu and Y.Cai F. Liu, K. A. Hua, and Y. Cai, presents a new approach for if-anonymity protection in Location-Based Services (LBSs). Specifically, it depersonalizes location information by ensuring that each location reported for LBSs is a cloaking area that contains K different footprints-historical locations of different mobile nodes. Therefore, the exact identity and location of the service requestor remain anonymous from LBS service providers. Existing techniques, on the other hand, compute the cloaking area using current locations of K neighboring hosts of the service requestor. Because of this difference, our approach significantly reduces the cloaking area, which in turn decreases query processing and communication overhead for returning query results to the requesting host. The advantage of this method is searches are made simple because find the records from previously derived history and other drawback is difficult to find the exact data in temporary memory medium.

E. Nearest Neighbour Search with Strong Location Privacy:

According to this paper [5],] S. Papadopoulos, S.Bakiras and D.Papadias focus on k nearest neighbor (kNN) queries and define the notion of strong location privacy, which renders a query indistinguishable from any location in the data space. it argues that previous work fails to support this property for arbitrary kNN search. Towards this end,] S. Papadopoulos, S.Bakiras and D.Papadias introduce methods that offer strong location privacy, by integrating private information retrieval (PIR) functionality. The main advantage of this method is providing option to ask location to the nearest neighbor and disadvantage is lack of Privacy.

III. SYSTEM DESIGN

A. SYSTEM MODEL:

We denote every person engaged in the protocol as a user U_i (we do not differentiate smartphone users and PC users), the user who publishes his location as a publisher Pi and the user who queries the location information of other user as a querier Q_i. Note that a user can be a querier and a publisher at the same time. When he queries on others, he acts as a querier and when he is queried, he acts as a publisher. That is, $U_i = P_i = Q_i$ for the same $_i$. Also, mobile applications or SNS applications which support LBS are denoted as service providers SP. Q and P retrieves keys from SP, which are used for access control. For simplicity, we consider only one SP here. We assume an independent semi-honest model for users and service providers. That is, they all behave independently and will try to extract useful information from the ciphertexts, but they will follow the protocol in general and will not collude with each other. We further assume that every user communicate with each other via an anonymized network or other anonymized protocol such that the privacy is not compromised by the underlying network protocol. We assume the origin of a packet is successfully hidden, which is out of this paper's scope (otherwise any attacker can achieve the location based on the origin of the packet).

B. LOCATION ASSUMPTION:

For simplicity, we assume the ground surface is a plane, and every user's location is mapped to an Euclidean space with integer coordinates (with meter as unit). That is, everyone's location can be expressed as a tuple of coordinates representing a point in a grid partition of the space. This does not affect the generality since there exists a bijection

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1115-1119), Month: April - June 2015, Available at: www.researchpublish.com

between spherical locations and Euclidean locations. By approximating the coordinates in the Euclidean space to the nearest grid point, we can show that it results in errors of the Euclidean distance between two locations at most √2 meters when the space is partitioned using grid of side-length 1 meter.

The Euclidean distance between two users with locations $\mathbf{x}_1 = (x_{11}, x_{12}, x_{13})$ and

$\mathbf{x}_2 = (x_{21}, x_{22}, x_{23})$ is dist(U1, U2) = $|\mathbf{x}_1 - \mathbf{x}_2| = \sqrt{\sum_{i=1}^{3}(x_{1i} - x_{2i})^2}$ ....(1)

Given a real location on the surface of the earth, we need to compute the surface distance, denoted as SD (U_i, U_j), between these two points. By assuming that the earth is a sphere with radius R meters, it is easy to show that

SD (U_i, U_j) = 2 arcsin(dist(U_i, U_j)/2R) ・ R……(2)

Then the surface distance can be quickly computed from the Euclidean distance. To check if the surface distance satisfies certain conditions, we can convert it to check if the Euclidean distance satisfying corresponding conditions. For example, dist (U_1, U_2) ≤ D is equivalent as SD (U_i, U_j) ≤ 2Rarcsin (D/2R). For simplicity and convenience of presentation, in this paper, we will focus on the Euclidean distance instead of the surface distance. Notice that although we consider only Euclidean space here, our protocol works for any system where distance is a polynomial of location points **x**'s, where **x** is a vector.

C. PRELIMINARY DESIGN:

In this paper we need that a publisher can specify some access control process for every potential location queriers. All access trees will give access to a different level of the knowledge about the location information, which then achieved by using FE in the protocol. And, strictly speaking, encryption in the protocol is not formal FE since we support constant functions of data, so we refer it as a semi-functional of encryption. In order to allow set of all possible queries by every users, we firstly present 5 distances of computation and comparison related algorithms which will be then used to provide the four levels of the functions over a location data in semi-functional PLBMS..

1) Privacy Distance Computation: Let x = (x1, x2, x3) and y = (y1, y2, y3) be publisher P's and a querier Q's 3-dimensional of location respectively. We uses Algorithms 1 to let Q securely get compute dist(P,Q) without knowing the P's coordinates or disclosing their own one. Algorithm 1 Privacy Preserving Distance Computation 1: Q generates pair of encryption and decryption key's of Paillier's cryptosystem:EK = (n, g), DK = (_, i). We assume n is length of 1024-bit. EQ denotes that encryption done by Q using his encryption keys 2: Q generates the following cipher texts and sends them to P at x. EQ(1), EQ(X3 i=1 y2 i), {EQ(yi) | i = 1, 2, 3}, 3: P,after receiving the cipher texts, executes the following homomorphic operations: ({EQ(yi).2xi} = {EQ(.2xiyi)}, for i = 1, 2, 3 EQ(1) P3 i=1 x2 i = EQ(P i=1 x2 i) 4: P computes and sends the following to the querier Q: EQ(X3 i=1 x2 I) · EQ(X3 i=1 y2 i) · Y3 i=1 (EQ(.2xiyi)) = EQ(X3 i=1 (xi . yi)2) = EQ(|x . y|2) 5: Q uses the private key DK to decrypt the EQ(|x . y|2) to get distance. Note that location y is kept secret to P during whole protocol, since he does not to know private key; on the other hand, location x is also kept secret since Q achieves E(|x . y|2). However, location x is inferred if the Q runs same protocol at the different places for all four times in the Euclidean of space (three times in the Euclidean plane). This will be all discussed in complete detail in TheoremVI.1. 2) Privacy Distance Comparison: Let x = (x1, x2, x3) and y = (y1, y2, y3) be publisher of the P's and querier Q's 3-dimensional location of respectively. We can use Algorithm 2 to let Q learn whether dist(P,Q) is the less than, a equal to or greater than the threshold value _, which can be determined by publisher P. The reason _ and _□ Œ are chosen always from Z2972 and Z21022 is because comparison is not correct because the modular operations. This is further discussed in Section of VIF. On the contrary, if Q wants to be determine the threshold value _, he can only send another ciphertext E(_2) at the Step 2. And then, P compute E(_2)_ □ E E(1)_□ Œ = E(__2 + _□ Œ) at Steps 4 and proceed same as Algorithm 2. Algorithms 2 Privacy Distance Comparisons 1: Q generate encryption and decryption key pair of all Paillier□ fs cryptosystem: EK = (n, g),DK = (_, *f*Ê).2: Q generates following ciphertexts and then sends them to a user named P with the location x. EQ(1), EQ(X3 i=1 y2 i), {EQ(.2yi) | i = 1, 2, 3} 3: P, after receiving the ciphertexts, randomly then picks two integers _ □ ¸ Z2972 , _□ Œ □ ¸ Z21022 and then executes the following homo morphic operations: ýýýýýýý ýýýýýý {EQ(.2yi)_xi = EQ(.2_xiyi) | i = 1, 2, 3} EQ(P3 i=1 y2 i)_ = EQ(_(y2 1 + y2 2 + y2 3)) EQ(1)_ P3 i=1 x2 i = EQ(_ P3 i=1 x2 i)) EQ(1)_□ Œ = EQ(_□ Œ) EQ(_ P3 i=1 x2 i) □ E EQ(_□ Œ) = EQ(_ 3 i=1 x2 i + _□ Œ) 4: P computes followings and sends them back to other users at y. EQ(_ X3 i=1 x2i + _□ Œ) □ E EQ(_ X3 i=1 y2 i

) Y3 i=1 (EQ(.2_xiyi)) = EQ((_ X3 i=1 (xi . yi)2) + _ • Œ) = EQ(_|x . y|2 + _□ Œ) EQ(1)__2 +_□ Œ = EQ(__ 2 + _□ Œ) 5: Q uses the private keys DK(_, *f*Ê) to decrypt ciphertexts and get _|x . y|2 + _□ Œ and __2 + _□ Œ. If, without the modular operation, both of them are less than the given modulo n, know we have: _|x . y|2 + _□ Œ < __2 + _□ Œ □ Ì |x . y| < _

IV. CONCLUSION

In this paper, a smooth Privacy-preserving Location based messaging service, which successfully solves the privacy issues in existing LBS applications and provides various location based queries. The Privacy-preserving Location based messaging service uses novel distance computation and comparison protocol to implement semi-functional encryption, which supports multi-leveled access control, and used CP-ABE as supporting encryption scheme to make access control be more even. Also, during processing, unless accessed by the location publisher, the location information is kept secret to anyone else.

V. FUTURE WORK

Location information, however, if on one side is critical for providing customized services, on the other hand, if misused, can lead to privacy breaches. A attacker may infer sensitive information about the individual, such as healthcare or financial information so location privacy is requiered. Future researches can be carried in positioning techniques, small devices, GIS-based services and cache managements.

The LBS application can help user to find hospitals, school, gas filling station or any other facility of interest indicated by user within certain range. Just like a GPS device its location will also be updated as soon as user changes his/her position.

REFERENCES

[1] Alastair R. Beresford and Frank Stajano " Mix Zones: User Privacy in Location- aware Services " Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on March 2004.

[2] Heechang Shin, Vaidya J. Atluri.V "A Profile Anonymization Model for Privacy in a Personalized Location Based Service Environment "Mobile Data Management, 2008. MDM '08. 9th International Conference on April 2008.

[3] T.Xu and Y.Cai F. Liu, K. A. Hua, and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-based Services," in Proceedings of the 10th International Conference on Mobile Data Management: Systems, Services and Middleware, 2008.

[4] C. B. D. Riboni, L. Pareschi and S. Jajodia, "Preserving Anonymity of Recurrent Location-Based Queries," in Proceedings of the 16th International Symposium on Temporal Representation and Reasoning,2009.

[5] S. Papadopoulos, S.Bakiras and D.Papadias ""Nearest Neighbor Search with Strong Location Privacy" Proceedings of the VLDB Endowment, Vol. 3, No. 1 Copyright 2010 VLDB Endowment 2010.

[6] B.Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacy Grid," in Proceedings of the 17th International World Wide Web Conference, 2008.

[7] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," Ubicomp 2007: Ubiquitous Computing, pp.2007.

[8] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against location based personal identification," Secure Data Management, pp. 2005.

[9] M. Mokbel, C. Chow, and W. Aref, "The new Casper: query processing for location services without compromising privacy," in Proceedings of the 32nd international conference on Very large data bases, VLDB Endowment, 2006, pp.