Get Me on the Map If You Can: Secure Locale Scepticism Activity

Ashwini Shinde¹, Venkata Reddy G², Janapati Venkata Krishna³

¹Pursuing M.Tech (CSE), Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India
²Working as Assistant Professor (CSE Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India
³Working as Associate Professor & HOD (CSE Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India

Abstract- There are two things to consider about this application that is Location-Based Service (LBS) and social network services (SNS). Now a day almost every social network service provider giving the facilities to the user so that user can share or produce their location to the specified persons. Many location based services (LBS) takes the user current location to provide the users handful and convenient functionality to their daily life. For all this the LBS will access the location of the user and the current location of anyone contains so many information regarding to them, so it can be said that user personal privacy will be affected. So, preserving user location privacy while using the facility of location information is still a challenging issue. To get rid from this issue a suite of novel fine-grained privacy-preserving location query protocol (PLQP) is designed. Newly introduced protocol will check different level of conditions and also provide encrypted location information for the authorized user.

EXISTING SYSTEM

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. While sharing the location Flickr allows its client to select some user from a huge contact list or selecting a group that is having some common user like friends, colleagues, etc whereas Facebook and Google++ in addition allows its users to make some custom group to specify the groups for location accessibility. Many applications capitalize on both LBS and SNS. 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

There are some pitfalls in the existing system like; 1) users are allowed to specify only explicit list of users who can access the location information. 2) the existing system have a access control policy that only follows the binary rules of choice like user can either enable or disable the discloser of the location information. One more problem with the existing system is the 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.

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; 1) In the place of selecting some user from a huge amount of contact list or selecting a group that is having some drawback, our application directly allows to put some condition by the user to decide location sharing. 2) The protocol will allow to set the range of the location i.e., user will decide that what will be the accuracy of the application. Means user only decide that at what extends the location is to be shared. 3) 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.

ADVANTAGE

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

RELATED WORK

There are some works achieving the privacy-preserving location for query, which are all based on k anonymity model. K-anonymity model has been always used for protect data privacy. Basic ideas are to remove features like each item should not recognize among other k items. However, techniques that achieve k-anonymity of the data cannot be always used in our case because of following four reasons: 1) The technique protects privacy of the data will stored in server side. In proposed PLQP, we are not storing any data. 2) Here in LBS, the data of location is rapidly updated, and this kind of behavior introduces a huge raised to keep in data k-anonymity. 3) As analyzed by Zang et al. getting k-Anonymous in the location data importantly violate utility of Even for the small k, so it’s never suitable for location information query Protocol. 4) the k is system-wide parameters which Determine about the level of privacy for all data within the system, but the goal is to always leave decision for privacy level to the each users. Kido et al. proposed scheme that appends so many false locations to a true location. LBS only respond all reports, and client collects related response to the true location. They examine some dummy-related technique after that predict the way to make plausible based dummy locations and to reduce the unwanted communication cost. Their technique always protects users’ related location information privacy against all the LBS providers. The technique is also interested in a specified user’s location for privacy against other defined users. In this mixed zone of model that proposed by Beresford et al. users are all given a different pseudonyms for all time they come to the mixed zone, after that users’ ways are hidden like that. Some works are related to the model, and they guarantee privacy only when user mass is high and their behaviors technique is uncertain. Most of them will need trusted servers. Here also some works concern to the CR (cloaking region). In this work, the LBS get a cloaking region all instead of the actual users’ related locations. Gedit et al. proposed that is related to space cloaking and temporal cloaking. Each and every query show a temporal interval, but queries in the same interval, which sources are in vicinity for the first query’s starting, all merged into a single query. Other than, query will be rejected saying it has no more anonymity.

SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

We denote all persons relates in protocol as user Ui (we are not going to differentiate the user of smart phone and PC), a user who is publishing the location like a publisher Pi and user who queries location of the other user as a querier Qi. Note a user can be a querier and a publisher same time. When they queries on to the others, they acts as querier and when he queried, and acts as publisher. That is, the Ui = Pi = Qi for the same i.

B. Location Assumption

For simplicity, we let the ground surface is plane, and all user location is a mapped as a Euclidean space 3 including integers coordinates (meter as unit). Means everyone’s location infer will be expressed like tuple of a coordinates that representing point in grid partition for space. This will not affect generality because there are bisection in spherical and Euclidean locations. After approximating coordinates of Euclidean space to nearest grid point, we will able to show that it results in errors of Euclidean distance within two locations at √2 meters when space will partitioned by grid of side-length as 1 meter. Euclidean distance between two user having locations x1 = (x11, x12, x13) and x2 = (x21, x22, x23) is dist(U1, U2) = |x1 − x2| = s P3 i=1 (x1i − x2i)2

PRELIMINARY DESIGN

In PLQP, 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 PLQP. 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 = (_, µ). 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 y1 i ), {EQ(yi) | i = 1, 2, 3}, 3: P, after receiving the cipher texts, executes the following homomorphic operations: ( {EQ(yi)−2xi} = {EQ(−2yi)i}), 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 1) · EQ(X3 i=1 y1 i ) · Y3 i=1(EQ(−2yi)i) = 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 Theorem VI.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 _ are chosen always from Z2972 and Z21022 is because comparison is not correct because the modular operations. This is further discussed in Section of VI-F. 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 computes E(2)_ · E(1)_ = E(2 + _) at Steps 4 and proceed same as Algorithm 2. Algorithms 2 Privacy Distance Comparisons 1: Q generate encryption and decryption key pair all Paillier’s cryptosystem: EK = (n, g), DK = (_, µ).

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 , _ ∈ Z21022 and then executes the following homomorphic operations:

{EQ(−2yi)xi = EQ(−2xiyi) ∈ i = 1, 2, 3} {EQ(P3 i=1 x2 i) = EQ(−2x2 2 x2 3)} EQ(1)_ , P3 = E(1)_{x2 i = EQ(−2x i2 i)} EQ(1)_{x2 i = EQ(−2x i2 i)} EQ(1)_{x2 i = EQ(−2x i2 i)}

3: P, after receiving the ciphertexts, then executes the following homomorphic operations:

then executes the following homomorphic operations:

{EQ(−2yi)xi = EQ(−2xiyi) | i = 1, 2, 3} EQ(1)_{x2 i = EQ(−2x i2 i)} EQ(1)_{x2 i = EQ(−2x i2 i)}

4: P computes followings and sends them back to other users at y. EQ(_x3 i=1 x2 i + _2) · EQ(_x3 i=1 y2 i ) Y3 i=1 (EQ(−2xiyi)) = EQ(_x3 i=1 (xi − yi)2 + _2) = EQ(_x2 2 x2 3) = EQ(1)_{x2 i = EQ(−2x i2 i)} EQ(1)_{x2 i = EQ(−2x i2 i)}

5: Q uses the private keys DK(_, µ) to decrypt ciphertexts and get _x − y2 + _2 and _2 + _2. If, without the modular operation, both of them are less than the given modulo n, know we have: _x − y2 + _2 < _2 + _2 ⇔ _x − y2 < _

CONCLUSION
In this paper, we proposed Privacy-preserving Location Based Query Protocol (PLQP), which successfully solves privacy issue in the existing LBS application and provide various location based queries. The PLQP using novel distance computations and comparisons protocols to implementing semi-functional encryptions, which support multi-level accessing control, and use CP-ABE as subsidiary of encryption scheme to make the access control to be more fine-grained. Also, during this whole protocol, unless it is intended by the location publishers, the location information will keep all secret to anyone else. We also conducted some experiment evaluation for showing that the performance of protocol is applicable in real mobile networks.

REFERENCES

AUTHOR PROFILE
Ashwini Shinde, pursuing M.Tech (CSE) from Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Venkatakoti Reddy G., Assistant Professor (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Janapati Venkata Krishna, Associate Professor & H O D (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.