https://dx.doi.org/10.22161/ijaers/3.12.41 ISSN: 2349-6495(P) | 2456-1908(O)

Privacy and Protection for Location Based Services

Mrs. M. Lalitha[1], G. Sneha[2]

[1]Asst. Professor, Department of CSE, G. Narayanamma Institute of Technology and Science, Mandal Shaikpet, District Hyderabad, Telangana, India.

[2] M. Tech Student, Department of CSE, G. Narayanamma Institute of Technology and Science, Mandal Shaikpet, District Hyderabad, Telangana, India.

Abstract— *An LBS (location based service) provides services such as finding the nearest location, favourite entertainment areas etc, to the users based on either their residing area or based on the input the give. The services provided by a location based service are typically based on a point of interest database. Therefore retrieval of the data from the database server takes place. The work proposed is a novel protocol for location based queries that has major performance improvements, which is performed based on two stages- firstly, the user determining his/her location privately and secondly, the server protecting its data from unauthorized users for which they have not paid. This protocol enables security for the user's details as well as protects the server's data. The user is protected because the server is unable to determine his/her location. In the same way, the server's data is protected as a malicious user can only decrypt the part of data obtained to the user with the encryption key acquired in the previous phase, that is he/she cannot decrypt the remaining server data that they are not supposed to authorise. In other words, users can never get the data more than what they have paid for. A phase called oblivious transfer phase is present so as to ensure the privacy of the user and a phase called private information retrieval phase is carried out to protect server's data.*

Keywords— Location based service, Point of Interest database, oblivious transfer phase, Private information retrieval phase.

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 offer 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 offers 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. Therefore the LBS has to ensure that LS's 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 system model consists of three types of entities: the set of users who wish to access location data U, a mobile service provider SP, and a location server LS.

The purpose of the mobile service provider SP is to establish and maintain the communication between the location server and the user. The location server LS owns a set of POI records r_i for $1 \leq ri \leq \rho$. Each record describes a POI, giving GPS coordinates to its location (x_{gps}, y_{gps}), and a description or name about what is at the location. We reasonably assume that the mobile service provider SP is a passive entity and is not allowed to collude with the LS. We make this assumption because the SP can determine the whereabouts of a mobile device, which, if allowed to collude with the LS, completely subverts any method for privacy.

https://dx.doi.org/10.22161/ijaers/3.12.41 ISSN: 2349-6495(P) | 2456-1908(O)

II. LITERATURE SURVEY

A preliminary investigation on the privacy issues involved in the use of location-based services. It is argued that even if the user identity is not explicitly released to the service provider, the geo-localized history of user-requests can act as a quasi-identifier and may be used to access sensitive information about specific individuals. Here it formally defines a framework to evaluate the risk in revealing a user identity via location information and presents preliminary ideas about algorithms to prevent this to happen.

It has formally defined the problem of the personal identification of sensitive data in location-based services. We believe that the formal framework we have defined can be used for two very different purposes like, to enforce a certain level of privacy, possibly disabling the service when the level cannot be guaranteed, and to evaluate if the privacy policies that a location-based service guarantees are sufficient to deploy the service in a certain area. This may be achieved by considering, for example, the typical density of users, their movement patterns, their concerns about privacy, as well as the spatiotemporal tolerance constraints of the service and the presence of natural mix-zone in the area. While in this system we presented preliminary results about which we consider as another promising research direction. Regarding it we already pointed out several issues that deserve further investigation, including monitoring multiple LBQ IDs, efficient generalization algorithms and unlinking techniques. In addition, randomization should be used as part of the TS strategy to prevent inference attacks. Another interesting open issue regards user interfaces. On one side, very simple tools should be provided to define LBQ IDs and verify them based on statistical data. On the other side, simple and effective interfaces are needed to specify the level of anonymity required by the user, as well as to notify when identification is at risk. Graphical solutions, like the open and closed lock in an internet browser should be considered.

The popularity of location-based services leads to serious concerns on user privacy. A common mechanism to protect users' location and query privacy is spatial generalization. As more user information becomes available with the fast growth of Internet applications, e.g., social networks, attackers have the ability to construct users' personal profiles. This gives rise to new challenges and reconsideration of the existing privacy metrics, such as k-anonymity. In this system , we propose new metrics to measure users' query privacy taking into account user profiles. Furthermore, we design spatial generalization algorithms to compute regions satisfying users' privacy requirements expressed in these metrics. By experimental results, our metrics and algorithms are shown to be effective and efficient for practical usage.

In this system, we consider a powerful attacker who can obtain user profiles and has access to users' real-time positions in the context of LBSs. Assuming this stronger attacker model, we propose new metrics to correctly measure users' query privacy in LBSs, including k-ABS, α-USI, β-EBA and γ-MIA. For information theory based metrics, the determination of users' specified values is not intuitive. However, users can use other metrics as references. For instance, k-anonymity corresponds to log k-EBA when the distribution for users to issue a query is (close to) uniform. Special generalization algorithms are developed to compute regions satisfying user's privacy requirements specified in the proposed metrics. Extensive experiments show our metrics are effective in balancing privacy and quality of service in LBSs and the algorithms are efficient to meet the requirement of real-time responses. Our metrics are not exhaustive, and there exist other ways to express query privacy. For instance, we can use min-entropy to express information leakage in a way analogous to mutual information: $I_\infty(X; Y) = H_\infty(X) - H_\infty(X \mid Y)$. Intuitively, it measure the amount of min-entropy reduced after the attacker has observed a generalized query. It is very interesting to study differential privacy to see how it can be adopted for LBS scenarios. In future, we want to develop an application for LBS, making use of the proposed metrics to protect users' query privacy. This can lead us to a better understanding of privacy challenges in more realistic situations. The implementation of our algorithms can also be improved as well, e.g., using a better clustering algorithm for kABS. Another interesting direction is to study a stronger attacker model, where the attacker, for instance, can have access to mobility patterns of users.

III. SYSTEM DESIGN

In this system, we propose a novel protocol for location based queries that has major performance improvements with respect to the approach by Ghinita at el. And. Like such protocol, our protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR, to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage.

Our protocol thus provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only

https://dx.doi.org/10.22161/ijaers/3.12.41 *ISSN: 2349-6495(P) | 2456-1908(O)*

decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage. In other words, users cannot gain any more data than what they have paid for. We remark that this system is an enhancement of a previous work.

Advantages of the system

1. Redesigned the key structure.
2. Added a formal security model.
3. Implemented the solution on both a mobile device and desktop machine.

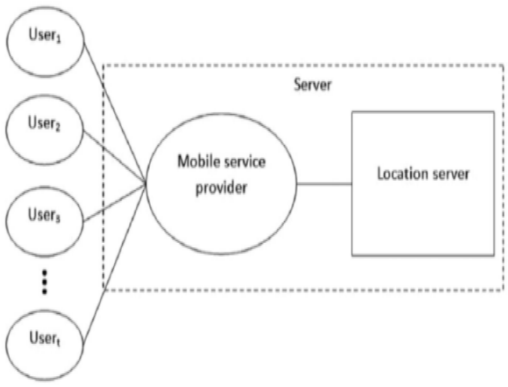

Fig.1: System Model

The system model consists of three types of entities as in the figure:

i) The set of users who wish to access location data.
ii) The purpose of the mobile service provider is to establish and maintain the communication between the location server and the user.
iii) The location server owns a set of point of interests (POI) records. Each record describes a POI, giving GPS coordinates to its location, and a description or name about what is at the location.

IV. FRAME WORK MODULES

There are four modules in the system designed. They are User initiation module, Oblivious transfer module, Private information retrieval and location server module.

User initiation module

The ultimate goal of our protocol is to obtain a set (block) of POI records from the LS, which are close to the user's position, without compromising the privacy of the user or the data stored at the server. We achieve this by applying a two stage approach. The first stage is based on a two-dimensional oblivious transfer and the second stage is based on a communicationally efficient PIR. The oblivious transfer based protocol is used by the user to obtain the cell ID, where the user is located, and the corresponding symmetric key. The knowledge of the cell ID and the symmetric key is then used in the PIR based protocol to obtain and decrypt the location data. The user determines his/her location within a publicly generated grid P by using his/her GPS coordinates and forms an oblivious transfer query. The minimum dimensions of the public grid are defined by the server and are made available to all users of the system. This is implemented using user initiation algorithm, which is:

Input: $X_{1,1},\ldots,X_{m,n}$, where $X_{i,j} = ID_{Q_{i,j}} \| k_{i,j}$
Output: $Y_{1,1},\ldots,Y_{m,n}$

1: $K_{i,j} \leftarrow K_{i,j} = g_0^{g_1^{R_i} g_2^{C_j}}$, for $1 \le i \le n$ and $1 \le j \le m$, where R_i and C_j are randomly chosen
2: $Y_{i,j} \leftarrow X_{i,j} \oplus H(K_{i,j})$, for $1 \le i \le n$ and $1 \le j \le m$, where H is a fast secure hash function
3: **return** $Y_{1,1},\ldots,Y_{m,n}$ {Encryptions of $X_{1,1},\ldots,X_{m,n}$ using $K_{i,j}$}

Fig.2: User Initiation Algorithm

Oblivious Transfer module

The purpose of this module is for the user to obtain one and only one record from the cell in the public grid P, We achieve this by constructing a 2-dimensional oblivious transfer, based on the ElGamal oblivious transfer, using adaptive oblivious transfer proposed by Naoret al. We remark that this key structure of this form is an enhancement from, as the client doesn't have access to the individual components of the key.

This phase is implemented by using an algorithm called as oblivious transfer algorithm. It is as follows:

Input: **User:**i,j
Output: **User:**$(ID_{Q_{i,j}}, k_{i,j})$

1: **User** $(QG1)$
2: $y_1 \leftarrow g_1^{x_1}$, where y_1 is the public key for the row and x_1 is chosen at random
3: $y_2 \leftarrow g_2^{x_2}$, where y_2 is the public key for the column and x_2 is chosen at random
4: $\boldsymbol{C_1} \leftarrow (A_1, B_1) = (g_1^{r_1}, g_1^{-i} y_1^{r_1})$
5: $\boldsymbol{C_2} \leftarrow (A_2, B_2) = (g_2^{r_2}, g_2^{-j} y_2^{r_2})$
6: $Server \Leftarrow \boldsymbol{C_1}, \boldsymbol{C_2}$
7: **Server** $(RG1)$
8: $\boldsymbol{C'_{1,\alpha}} \leftarrow (A_1^{r'_\alpha}, g_1^{R_\alpha} r_R (g_1^\alpha B_1)^{r'_\alpha})$ for $1 \le \alpha \le n$ and $r_R = g_1^s$, where s is chosen randomly
9: $\boldsymbol{C'_{2,\beta}} \leftarrow (A_2^{r'_\beta}, g_2^{C_\beta} r_C (g_2^\beta B_2)^{r'_\beta})$ for $1 \le \beta \le m$ and $r_C = g_2^t$, where t is chosen randomly
10: $\gamma \leftarrow g_0^{1/r_R r_C}$
11: $User \Leftarrow \boldsymbol{C'_{1,1}}, \ldots, \boldsymbol{C'_{1,n}}, \boldsymbol{C'_{2,1}}, \ldots, \boldsymbol{C'_{2,m}}, \gamma$
12: **User** $(RR1)$
13: Let $(U_{1,i}, V_{1,i}) = \boldsymbol{C'_{1,i}}$ and $(U_{2,j}, V_{2,j}) = \boldsymbol{C'_{1,j}}$
14: $W_1 \leftarrow U_{1,i}^{-x_1}$
15: $W_2 \leftarrow U_{2,j}^{-x_2}$
16: $W_3 \leftarrow V_{1,i} W_1$
17: $W_4 \leftarrow V_{2,j} W_2$
18: $K'_{i,j} \leftarrow \gamma^{W_3 W_4}$
19: $X'_{i,j} \leftarrow Y_{i,j} \oplus H(K'_{i,j})$
20: Reconstruct $(ID_{Q_{i,j}}, k_{i,j})$ from $X'_{i,j}$
21: **return** $(ID_{Q_{i,j}}, k_{i,j})$ {Cell id of grid Q, with associated cell key}

Fig.3: Oblivious Transfer Algorithm

https://dx.doi.org/10.22161/ijaers/3.12.41 *ISSN: 2349-6495(P) | 2456-1908(O)*

Private Information Retrieval Module

With the knowledge about which cells are contained in the private grid, and the knowledge of the key that encrypts the data in the cell, the user can initiate a private information retrieval protocol with the location server to acquire the encrypted POI data. Assuming the server has initialized the integer e, the user u_i and LS can engage in the following private information retrieval protocol using the $ID_{Qi,j}$, obtained from the execution of the previous protocol, as input. The $ID_{Qi,j}$ allows the user to choose the associated prime number power πi, which in turn allows the user to query the server.

This phase is implemented by using an algorithm called as private information retrieval algorithm. It is as follows:

Input: User:$ID_{Q_{i,j}}$
Output: User:C_i
1: **User** $(QG2)$
2: $\pi_0 \leftarrow \pi_i$, where π_i is chosen based on the value of $ID_{Q_{i,j}}$
3: Generate random group G and group element g, such that π_0 divides the order of g
4: $q \leftarrow |\langle g \rangle| / \pi_0$
5: $h \leftarrow g^q$
6: $Server \Leftarrow G, g$
7: **Server** $(RG2)$
8: $g_e \leftarrow g^e$
9: $User \Leftarrow g_e$
10: **User** $(RR2)$
11: $h_e \leftarrow g_e^q$
12: $C_i \leftarrow log_h h_e$, where log_h is the discrete log base h
13: **return** C_i {The requested (encrypted) data}

Fig.4: Private Information Retrieval Algorithm

Location Server Module

The Location Server (LS), which offers 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. Therefore the LBS have to ensure that LS's 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.

V. EXPERIMENTAL RESULTS

Once the server application is run, the server side screen is starts and then the LBQ server needs to be run and then the LBQ server also starts. Once this is done the user can use his/her application.

After starting the application, the user needs to login on the login page else he/she needs to register and then login. Then a search screen appears on the page where the latitude and longitude values when given, displays the nearest places to the place given as input. The ouput of the nearest places looks like the below image:

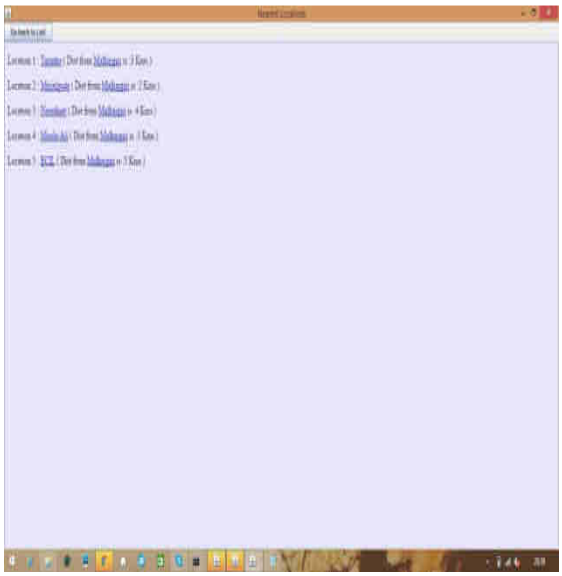

Fig.5: Screen shot of output screen

When the user clicks on the links of the places, the map of the place clicked is displayed on a new window.

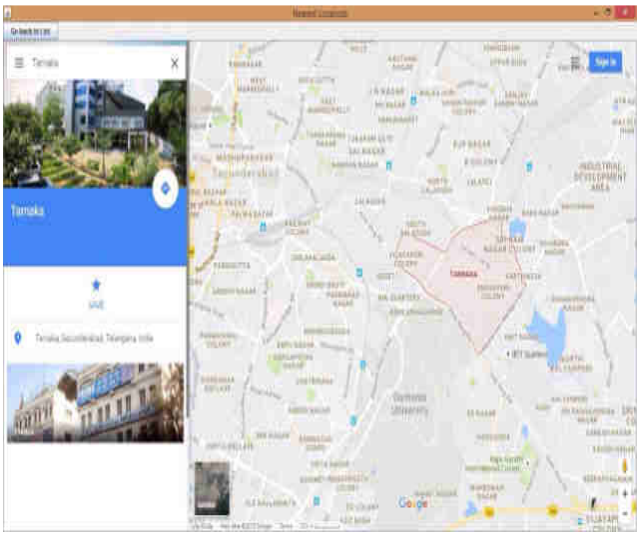

Fig.6: Screen shot of map upon clicking the place

This helps the user to know all the nearest point of interests, streets, lanes, roads, lakes etc.

VI. CONCLUSION

In this system we have presented a location based query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is for a user to privately determine his/her location using oblivious transfer on a public grid. The second step involves a private information retrieval interaction that retrieves the record with high communication efficiency. We analyzed the performance of our protocol and found it to be both computationally and communicationally more

https://dx.doi.org/10.22161/ijaers/3.12.41 *ISSN: 2349-6495(P) | 2456-1908(O)*

efficient than which is the most recent solution. We implemented a software prototype using a desktop machine. The software prototype demonstrates that our protocol is within practical limits.

VII. FUTURE ENHANCEMENT

Future work will involve testing the protocol on many different mobile devices. Also, we need to reduce the overhead of the primality test used in the private information retrieval based protocol. Additionally, the problem concerning the LS supplying misleading data to the client is also interesting. Privacy preserving reputation techniques seem a suitable approach to address such problem. Once suitable strong solutions exist for the general case, they can be easily integrated into our approach.

REFERENCES

[1] Openssl[Online]. Available: http://www.openssl.org/ Jul-7 2011.s
[2] M. Bellare and S. Micali, “Non-interactive oblivious transfer and applications,” inProc. CRYPTO, 1990, pp. 547–557.
[3] A. Beresford and F. Stajano, “Location privacy in pervasive computing, ”IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.
[4] C. Bettini, X. Wang, and S. Jajodia, “Protecting privacy against location-based personal identification,” in Proc. 2nd VDLB Int. Conf. SDM, W. Jonker and M. Petkovic, Eds., Trondheim, Norway, 2005, pp. 185–199, LNCS 3674.
[5] X. Chen and J. Pang, “Measuring query privacy in location-based services,” inProc. 2nd ACM CODASPY, San Antonio, TX, USA, 2012, pp. 49–60.
[6] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” J. ACM, vol. 45, no. 6, pp. 965–981, 1998.
[7] 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. 123–148, 2010.
[8] 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. 243–251, LNCS 3468.
[9] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,”IEEE Trans. Inform. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.
[10] B. Gedik and L. Liu, “Location privacy in mobile systems: A personalized anonymization model,” in Proc. ICDCS, Columbus, OH, USA, 2005, pp. 620–629.