International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Privacy Preserving Procedure for Reporting Region Based Activity Summaries

S. Sumiya Sultana[1], Dr. P. Kuppusamy[2]
[1]PG Student. Department of Computer Science & Engg. Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India
[2]Associate Professor. Department of ComputerScience & Engg. Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India

ABSTRACT

Location-based services (LBS) need users to incessantly report their location to a probably untrusted server to get services supported their location, which might expose them to privacy risks. Unfortunately, existing privacy-preserving techniques for LBS have many limitations, like requiring a fully-trusted third party, providing restricted privacy guarantees and acquisition high communication overhead. In this paper, we propose a user defined privacy grid model known as dynamic grid system(DGS), the primary holistic system that accomplish four important needs for privacy-preserving snapshot and continuous LBS. (1) the system solely needs a semi-trusted third party, liable for finishing up straightforward matching operations properly. This semi-trusted third party doesn't have any data a few users' location. (2) Secure photo and continuous location privacy is secure under our outlined somebody models. (3) The communication price for the user doesn't depend upon the user's desired privacy level; it solely depends on the quantity of relevant points of interest within the neighborhood of the user. (4) though we tend to solely concentrate on vary and k-nearest-neighbor queries during this work, our system will be simply extended to support different spacial queries while not dynamical the algorithms pass the semi-trusted Third party and also the info server provided the desired search space of a spacial question will be abstracted into spacial regions Experimental results show that our DGS is a lot of economical than the progressive privacy-preserving technique for continuous LBS.

Keywords : Location Based Services, Communication, Service Provider.

I. INTRODUCTION

In the existing systems, we tend to present Secure Run, a secure privacy-preserving system for reportage location-based activity summaries (e.g., the whole distance lined and also the elevation gain). Secure Run is predicated on a mix of crypto logic techniques and geometric algorithms, and it depends on existing Wi-Fi access-point networks deployed in urban areas. we tend to judge Secure pass using real data-sets from the FON hotspot community networks and from the Garmin Connect activity-based social network, and that we show that it are able to do tight (up to a median accuracy of over eighty percent) verifiable lower-bounds of the space lined and of the elevation gain, whereas protective the placement privacy of the users with relevancy each the social network operator and also the access purpose network operator(s). The results of our on-line survey, targeted at Run Keeper users recruited through the Amazon Mechanical Turki platform, highlight the dearth of awareness and vital considerations of the participants concerning the privacy and security problems with activity-tracking applications. They also show a decent level of satisfaction relating to Secure Run and its performance. Within the planned system we tend to propose a user-defined privacy grid system referred as dynamic grid system(DGS) to support privacy preserving snapshot and continuous location based service. The essential plan is to present the semi trusted third party called query server among the user and service supplier. Query server requires to be semi trusted because it won't gather to any user region data.

The major plan of our DGS. In dynamic grid system, a query user primarily verifies query region, where a user is convenient to reveal the truth that she is at some place within the query region. The query region is partition into equal sized grid cell depend on the dynamic grid system stated by user. Then user encoded a query that contains the data of query region and dynamic grid system, and encoded the integrity of every grid cell intersecting the needed seeking region of the spatial query to introduce a collection of encrypted attributes.

II. SYSTEM ARCHITECTURE

Figure 1 illustrates the system design of our dynamic grid system (DGS) designed to supply privacy-preserving continuous LBS for mobile users. Our system consists of 3 main entities, service suppliers, question servers and mobile users. We are going to describe the most entities and their interactions, so present the 2 spatial queries, i.e., vary and k-nearest-neighbor (NN) queries, supported by our system.

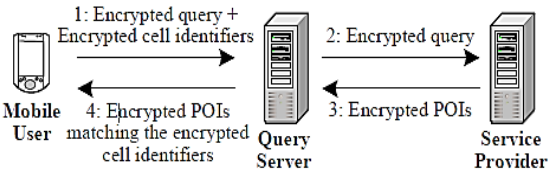

Figure 1. System Architecture

Service providers (SP):

Our system supports any range of freelance service suppliers. Every SP could be a spacial management system that stores the situation data of a specific variety of static POIs, e.g., restaurants or hotels, or the store location data of a specific company, e.g., Starbucks or McDonald's. The spacial information uses associate degree existing spacial index (e.g., R-tree or grid structure) to index POIs and answer vary queries (i.e., retrieve the POIs placed in a very bound area). As delineate within the higher than diagram SP doesn't communicate with mobile users directly, however it provides services for them indirectly through the question server (QS).

Next, the user transmit the request that contain (1) the encoded query (2) the encoded attributes to query server, that is semi trusted party situated among user and service provider. Query server collects encoded attributes and sends encoded query to service supplier mentioned by user. Service supplier decoded the query and preferred the POIs within the query region from its database.

Mobile Users

Every mobile user is supplied with a GPS-enabled device that determines the user's location within the kind (x_u, y_u). The user will get snapshot or continuous LBS from our system by issuance a spacial question to a specific SP through QS. Our system helps the user choose a question space for the spacial query, such the user is willing to give away to SP the actual fact that the user is found within the given space. Then, a grid structure is made and is embedded within an encrypted question that's forwarded to SP; it'll not reveal any data regarding the question space to QS itself. Additionally, the communication price for the user in DGS doesn't rely on the question space size. This is often one in every of the key options that distinguish DGS from the present techniques supported the Fully-trusted third party model.

Query Servers (QS):

QS May be a semi-trusted party placed between the mobile user and SP. similar to the foremost common infrastructure in existing privacy-preserving techniques for LBS, QS can be Maintained by a medium operator [16]. The control/data flows of our DGS are as follows (from the higher than diagram):

1) The mobile user sends a request that has (a) the identity of a user-specified SP, (b) associate encrypted question (which includes info regarding the user-defined dynamic grid structure), and (c) a collection of encrypted identifiers (which square measure calculated supported the user-defined dynamic grid structure) to QS.

2) QS store the encrypted identifiers and forward the encrypted question to the user-specified SP.

3) SP decodes the question and finds a correct set of POIs from its information. It then encodes the POIs and their corresponding identifiers supported the dynamic grid structure specific by the user and send them to QS.
4) QS come back to the user each encrypted dish whose encrypted symbol matches one among the encrypted identifiers at the start sent by the user. The user decodes the received POIs to construct a candidate answer set, and then performs a straightforward filtering method to prune false positives to reckon a certain question answer.

III. DYNAMIC GRID SYSTEM (DGS)

Range Query Processing:
A continuous vary question is outlined as keeping track of the POIs inside a user-specified distance range of the user's current location (x_u, y_u) for an explicit period of time. In general, the privacy-preserving vary question process protocol has six main steps.

Step 1. Dynamic grid structure (by the user).
The idea of this step is to construct a dynamic grid structure fixed by the user. A querying user initial specifies a question space, wherever the user is comfortable to reveal the very fact that she is found somewhere inside that question space. The question space is assumed to be an oblong space, described by the coordinates of its bottom-left vertex (x_b, y_b) and top-right vertex (x_t, y_t). Notice that the user isn't essentially needed to be at the middle of the question space. Instead, its location will be anyplace within the space. However, our system may support irregular spacial regions, e.g., the boundary of a town or a county, by employing a minimum bounding parallelogram to model the irregular spacial region as an oblong space. The question space is split into m × m equal-sized grid cells to construct a dynamic grid structure, wherever m could be a user-specified parameter. every grid cell is known by (c, r), wherever c is that the column index from left to right and r is that the row index from bottom to high, severally, with $0 \leq c, r$ < m.

Step 2. Request generation (by the user).
During this step, the querying user generates a call for participation that features (1) a question for a SP fixed by the querying user and (2) a group of encrypted identifiers, Se, for QS. The user initial selects a random key K and derives 3 distinct keys:

$$(\mathrm{HK}, \mathrm{EK}, \mathrm{MK}) \leftarrow \mathrm{KDF}(K) \quad (1)$$

Where KDF (·) could be a key derivation operate ([24]). Then, the user sets question and Se as follows:
(1) Query generation. Associate degree encrypted question for a particular SP is ready as:

$$\text{query} \leftarrow \mathrm{IBE.Enc}_{SP}(\text{POI-type}, K, m, (x_b, y_b), (x_t, y_t)) \quad (2)$$

Where IBE. EncSP (·) is Identity-Based coding (IBE) below the identity of SP (details of IBE area unit in [17]). Within the encrypted question, POI-type specifies the sort of POIs, K is that the random key elite by the user, and also the personalized dynamic grid structure is fixed by m, (x_b, y_b), and (x_t, y_t).
(2) Encrypted symbol generation. Given the question region of the vary question, the user selects a group of grid cells Sc within the dynamic grid structure that encounter the question region, i.e., a circle targeted at the user's current location (x_u, y_u) with a radius of vary. For every elite grid cell i in Sc, its identity (c_i, r_i) is encrypted to come up with associate degree encrypted identifier:

$$h_i \leftarrow H(c_i, r_i) \quad (3)$$
$$C_i \leftarrow \mathrm{SE.Enc}_{\mathrm{HK}}(h_i) \quad (4)$$

Where H(·) could be a collision-resistant hash operate and SE. Enckey(·) a centrosymmetric coding formula (for example AES-based) below key "key". Once encrypting all the grid cells in Sc, the user generates a group of encrypted identifiers Se. it's vital to notice that the user can confirm that the identifiers in Se area unit ordered randomly. Finally, the user produces a call for participation as below and sends it to QS:

$$\text{request} \leftarrow \langle SP, \text{query}, S_e \rangle \quad (5)$$

Step 3. Request processing (by QS).
Once QS receives the request from the user, it merely stores the set of encrypted identifiers Se and forwards the encrypted question to SP fixed by the user.

Step 4. Query processing (by SP).
SP decrypts the request to retrieve the POI-type, the random key K selected by the user within the request generation step (Step 2), and also the question space outlined by m, (x_b, y_b), and (x_t, y_t). SP then selects a group of np POIs that match the desired POI-type inside the user specified question space from its information. For every elite dish j with a location (x_j, y_j)) ($1 \leq j \leq np$), SP computes the identity of the grid cell within the user fixed dynamic grid structure covering j by

$c_j, r_j) = \left(\left\lfloor \frac{x_j - x_b}{(x_t - x_b)/m} \right\rfloor, \left\lfloor \frac{y_j - y_b}{(y_t - y_b)/m} \right\rfloor\right)$.

Then, SP generates $(\mathrm{HK}, \mathrm{EK}, \mathrm{MK}) \leftarrow \mathrm{KDF}(K)$ and computes the following:

$$h_j \leftarrow H(c_j, r_j) \quad (6)$$

$$C_j \leftarrow \mathrm{SE.Enc}_{\mathrm{HK}}(h_j) \quad (7)$$

$$l_j \leftarrow \mathrm{SE.Enc}_{\mathrm{EK}}(x_j, y_j) \quad (8)$$

$$\sigma_j = MAC_{\mathrm{MK}}(C_j, l_j) \quad (9)$$

Where MACkey (·) could be a message authentication code below key. The C_j is that the corresponding encrypted symbol of a dish, the l_j contains the precise location of a dish in encrypted kind, and also the σj is enclosed to stop bound attacks by QS (such as meddling with the encrypted POIs).

Finally, SP sends the set of selected POIs back to QS within the following form:

$$\langle \mathrm{POI}_j = (C_j, l_j, \sigma_j)\rangle, \quad \text{where } j = 1, \ldots, n_p. \quad (10)$$

Step 5. Encrypted identifier matching (by QS).

Upon receiving np triples, QS determines the set of matching dishs by comparison the encrypted identifiers Cj (1 ≤ j ≤ np) of the received POI with the set of encrypted identifiers Se antecedently received from the user. A match between a Cj and a few Ci within the set Se indicates that the poi j is in one among the grid cells needed by the user. Thus, QS forwards each matching poi to the user. If the question could be a shot question, QS then deletes the received POIs and their encrypted identifiers. However, if the question could be a continuous one, QS keeps the received POIs at the side of their encrypted identifiers till the user unregisters the question.

Step 6. Answer computation (by the user).

Suppose that there are a unit μ matched POIs received by the user. for every of those matched POIs, say , the user decrypts lj mistreatment EK and gets access to the precise location (xj, yj) of the dish. From (xj, yj) and lj, the user verifies σj by re-calculating the mac worth and compares it against σj . If they match, the user finds the solution that features the dish whose location is inside a distance of vary of the user's current position (xu, yu). Within the the user receives five POIs from QS, wherever the vary question answer includes two POIs, i.e., p4 and p6.

IV. ENCRYPTION TECHNIQUES

We use three types of techniques

- IBE Encryption
- Hash / Encryption
- AES Decryption

Identity-based encryption (IBE):

It is a crucial primitive of ID-based cryptography. As such it's a sort of public-key secret writing within which the general public key of a user is a few distinctive info concerning the identity of the user (e.g. a user's email address). this implies that a sender UN agency has access to the general public parameters of the system will encode a message mistreatment e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decipherment key from a central authority that must be sure because it generates secret keys for each user.

Hash / Encryption:

A hash perform may be a special category of hash perform that has sure properties that build it appropriate to be used in cryptography. it's a mathematical rule that maps knowledge of arbitrary size to a little string of a hard and fast size (a hash perform) that is intended to even be a unidirectional function, that is, a perform that is impracticable to invert.

AES encryption and decryption algorithm:

AES relies on a design principle called a substitution-permutation network, a mix of each substitution and permutation, and is quick in each software system and hardware. Not like its predecessor DES, AES doesn't use a Feistel network. AES may be a variant of Rijndael that features a fastened block size of 128 bits, and a key size of 128, 192, or 256 bits. In contrast, the Rijndael specification as such is specific with block and key sizes which will be any multiple of thirty two bits, each with a minimum of 128 and a most of 256 bits.

V. RESULTS

Here, the home page contain some fields such as register, user login, query server and service provider. When a user click on register field then registration

page will display then user can register. Fig 2 depicts registration page.

Figure 2. Registration page

When a user register successfully then he/she can login, after login successfully a user can perform some activities such as share their location, view their friends notification, search any location and view location notification.

If a user send any information that information will sent to query server in encrypted format. After login as query server, then it performs two activites such as share request and location request. Query server send share request and location request to service provider in encoded format. Fig. 3 depicts share request to service provider.

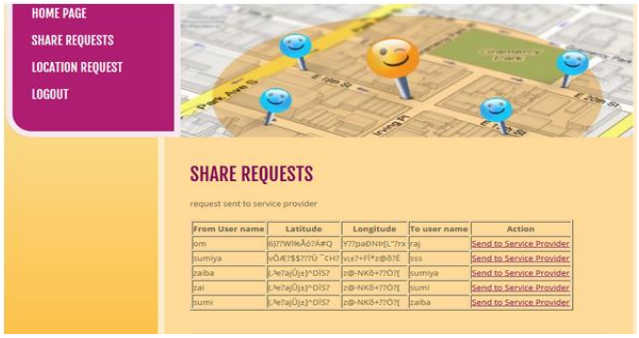

Figure 3. Share request to service provider

After login as service provider, then it sends data to recipient which it receives from query server. Fig. 4 depicts location request which is send to recipient.

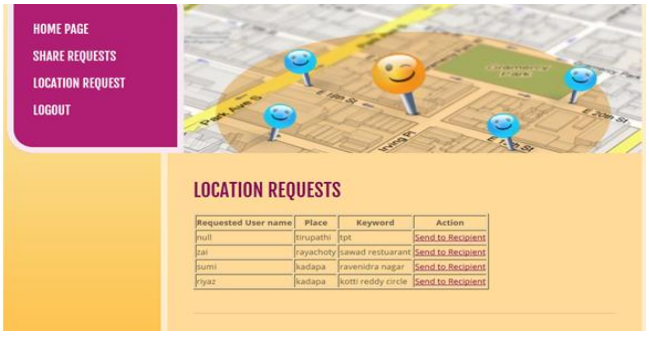

Figure 4. location request to recipient.

When location request send to recipient then recipient can find particular region and add that region information to database.

VI. CONCLUSION

We projected a dynamic grid system (DGS) for providing privacy-preserving continuous LBS. Our DGS includes the question server (QS) and therefore the service supplier (SP), and science functions to divide the entire question process task into two elements that area unit performed one by one by QS and SP. DGS doesn't need any fully-trusted third party (TTP); instead, we have a tendency to need solely the a lot of weaker assumption of no collusion between QS and SP. This separation additionally moves the info transfer load far away from the user to the cheap and high-bandwidth link between QS and SP. we have a tendency to additionally designed economical protocols for our DGS to support each continuous k-nearest-neighbor (NN) and vary queries. To evaluate the performance of DGS, we have a tendency to compare it to the progressive technique requiring a TTP. DGS provides higher privacy guarantees than the TTP theme, and therefore the experimental results show that DGS is an order of magnitude a lot of economical than the TTP theme, in terms of communication price. In terms of computation price, DGS additionally forever outperforms the TTP scheme for NN queries; it's comparable or slightly dearer than the TTP scheme for vary queries.

VII. REFERENCES

[1]. B. Bamba, L. Liu, P. Pesti, and T.Wang, "Supporting anonymous location queries in mobile environments with PrivacyGrid," in WWW, 2008.

[2]. C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in SSTD, 2007.

[3]. B. Gedik and L. Liu, "Protecting location privacy with personalized kanonymity: Architecture and algorithms," IEEE TMC, vol. 7, no. 1, pp. 1-18, 2008.

[4]. M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in ACM MobiSys, 2003.

[5]. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE TKDE, vol. 19, no. 12, pp. 1719-1733, 2007.
[6]. M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new Casper: Query processing for location services without compromising privacy," in VLDB, 2006.
[7]. T. Xu and Y. CAI, "Location anonymity in continuous location-based services," in ACM GIS, 2007.
[8]. "Exploring historical location data for anonymity preservation in location-based services," in IEEE INFOCOM, 2008.
[9]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in ACM SIGMOD, 2008.
[10]. M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, "Efficient oblivious augmented maps: Location-based services with a payment broker," in PET, 2007.
[11]. R. Vishwanathan and Y. Huang, "A two-level protocol to answer private location-based queries," in ISI, 2009.
[12]. J.M. Kang,M. F.Mokbel, S. Shekhar, T. Xia, and D. Zhang, "Continuous evaluation of monochromatic and bichromatic reverse nearest neighbors," in IEEE ICDE, 2007.
[13]. C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang, "Effective density queries of continuously moving objects," in IEEE ICDE, 2006.
[14]. S. Wang and X. S. Wang, "AnonTwist: Nearest neighbor querying with both location privacy and k-anonymity for mobile users," in MDM, 2009. 15W. B. Allshouse,W. B. Allshousea,M. K. Fitchb, K. H. Hamptonb, D. C. Gesinkc, I. A. Dohertyd, P. A. Leonebd, M. L. Serrea, andW. C. Millerb, "Geomasking sensitive health data and privacy protection: an evaluation using an E911 database," Geocarto International, vol. 25, pp. 443-452, October 2010.
[15]. A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "Providing kanonymity in location based services," SIGKDD Explor. Newsl. vol. 12, pp. 3-10, November 2010.
[16]. D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO, 2001.
[17]. A. Menezes, M. Qu, and S. Vanstone, "Some new key agreement protocols providing mutual implicit authentication," in SAC, 1995.
[18]. S. Yau and H. An, "Anonymous service usage and payment in servicebased systems," in IEEE HPCC, 2011, pp. 714-720.
[19]. M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, "Where's that phone?: Geolocating ip addresses on 3G networks," in ACM SIGCOMM IMC, 2009.
[20]. R. Dingledine, N. Mathewson, and P. Syverson, "Tor: the secondgeneration onion router," in USENIX Security, 2004.
[21]. G. Bissias, M. Liberatore, D. Jensen, and B. Levine, "Privacy vulnerabilities in encrypted HTTP streams," in PET, 2006.
[22]. P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in Pervasive Computing, 2009.
[23]. IEEE, P1363-2000: Standard Specifications for Public-Key Cryptography, 2000.
[24]. A. B. Lewko and B. Waters, "Efficient pseudorandom functions from the decisional linear assumption and weaker variants," in ACM CCS, 2009.