IJARES/December 2015/Volume-3/Issue-12/2261-2266 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

EFFICIENT DOCUMENT RETRIEVAL USING CONTENT SEARCH & QUERY VALUE SEARCH

Panchangula Priyanka[1], B.Lakshmi Kanth[2]

[1]PG Scholar, Dept of CSE, Krishnaveni Engineering College for Women, Narasaraopet, AP, India

Email: priyanka.panchangnula@gmail.com

[2]Assistant Professor, Dept of CSE, Krishnaveni Engineering College for Women, Narasaraopet, AP, India

Email: lakshmikanthit@gmail.com

ABSTRACT:

Retrieval methods of private information permit a user to get back data from a database, devoid of disclosing index of data to be recovered to database server. By mobile devices and operating all the way through a mobile network, a location based service is normally accessible. In support of location based queries in our work we provide a clarification to one of location-based query problems. We suggest a novel process that utilizes two protocols that facilitate a user to confidentially determine and obtain location data in which initial step is for a user to secretly determine their location by means of oblivious transfer on a public grid and the other step involves a confidential information recovery interaction that recovers record by means of high communication efficiency. In numerous circumstances this solution is scalable and well-organized. Devoid of compromising privacy of user or data that is stored at server, the ultimate objective of our procedure is to get hold of a set of points of interest records from location servers, which are close to user position. We attain this by application of a two stage approach in which initial stage is on basis of oblivious transfer and other stage is based on private information retrieval.

Keywords: Database server, Private information retrieval, Oblivious transfer, Location based queries, Points of interest.

1. INTRODUCTION:

In recent times there has been a remarkable enhancement in mobile devices querying location servers for information regarding point of interest. Among numerous challenging barriers towards extensive consumption of such application, privacy assertion is a most important problem. The location server which offers a little location based service use up its resources to assemble information in relation to a variety of interesting point of interests. It is likely that location server would not reveal any information without charge consequently location based service has to make certain that location server data is not accessed by any unofficial user. A location based service offers numerous services towards users on basis of geographical location of their mobile device [1]. By means of recovering Points of Interest from the database server, user can obtain answers towards a variety of location based queries. It is consequently important that solutions be set up that deal with privacy of the users providing queries, but moreover put off users from accessing of content for which they are not allowed. Innovative privacy metrics were projected that captures users' privacy relating to location based service. From these confidentiality metrics they moreover recommend spatial generalisation algorithms that correspond with user's privacy needs [2][3]. In our work we present a location based query solution that utilizes two protocols that facilitate a user to confidentially determine and obtain location data. The initial step is for a user to secretly determine their location by means of oblivious transfer on a public grid. The second step involves a confidential information recovery interaction that recovers record by means of high communication efficiency.

2. AN OVERVIEW OF EXISTING WORKS:

For the most part of the earlier efforts are resolved by the beginning of a private information retrieval location system and its fundamental idea is to facilitate the user to query location database devoid of compromising privacy of query. Normally private information retrieval schemes permit

a user to get back data from a database, devoid of disclosing index of data to be recovered to database server. Ghinita *et al.* utilized a variant of private information retrieval which is based on quadratic residuosity difficulty. Mainly the quadratic residuosity difficulty states that it is computationally tough to find out whether a number is quadratic remains of some composite modulus. This proposal was extended to offer database protection and this procedure consists of two stages such as in initial stage, user as well as server makes use of homomorphic encryption to permit user to confidentially find out whether their location is contained in a cell, devoid of disclosing their coordinates towards the server. In other stage, private information retrieval is used to get back the data contained in suitable cell. The difficulty concerning location server supplying false data towards the client is moreover interesting. Privacy preserving reputation method seems an appropriate approach to tackle such problem. In our work we present an explanation to one of location-based query problems which is defined as follows: a user needs to query a database of location data, recognized as points of interest, and does not desire to make known their location towards server due to privacy concerns; the owner of location data, specifically the location server, does not desire to just deal out its data towards the entire users [4]. We put forward a location based query solution that utilizes two protocols that facilitate a user to confidentially determine and obtain location data in which initial step is for a user to secretly determine their location by means of oblivious transfer on a public grid and the other step involves a confidential information recovery interaction that recovers record by means of high communication efficiency [5]. This solution is scalable and efficient in numerous circumstances.

3. AN OVERVIEW OF PROPOSED SYSTEM:

We recommend a novel procedure for location based queries that contain most important performance improvements relating to approach by Ghinita at el. Like such procedure, our procedure is organized in relation to two stages such as first stage; where user privately determines location within a public grid, by means of oblivious transfer containing both *ID* as well as connected symmetric key for block of data within private grid. In second stage, user

performs a communicational resourceful private information retrieval to recover the suitable block within private grid that is decrypted by means of symmetric key obtained in earlier stage. Our procedure as a result provides protection for user as well as the server. The user is secluded since server is incapable to determine location. In the same way, server's data is sheltered as a malevolent user can merely decrypt block of data obtained by private information retrieval with encryption key obtained in earlier stage. Users cannot achieve any additional data than what they have paid for. The system representation consists of three types of entities such as set of users who wish towards accessing location data, a mobile service provider, as well as location server. From the opinion of a user, service provider and location server will compose a server, which will provide both functions. The user does have no need to be concerned with particulars of the communication. The users in our representation utilize several location-based services that are provided by location server. The ultimate objective of our procedure is to get hold of a set of points of interest records from location servers, which are close to user position, devoid of compromising privacy of user or data that is stored at server. We attain this by application of a two stage approach. In initial stage is on basis of oblivious transfer and other stage is based on private information retrieval. The oblivious transfer based procedure is used by user to get hold of the cell ID, where user is positioned, and equivalent symmetric key [6]. The knowledge of cell ID as well as symmetric key is subsequently used in private information retrieval based procedure to get hold of and decrypt location information.

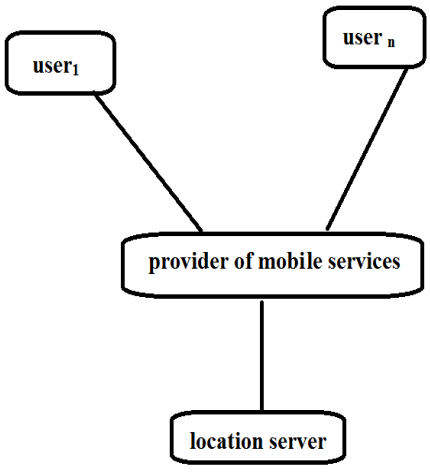

Fig1: View of System representation.

4. CONCLUSION:

On basis of geographical location of their mobile device a location based service offers numerous services towards users. Relating to location based service innovative privacy metrics was projected that captures users' privacy. The complexity relating to location

server supplying false data towards the client is moreover interesting. In our work we provide an explanation to one of location-based query problems We present one of location-based query problems which is defined as follows: a user needs to query a database of location data, recognized as points of interest, and does not desire to make known their location towards server due to privacy concerns; the owner of location data, specifically the location server, does not desire to just deal out its data towards the entire users. The eventual purpose of our process is to get hold of a set of points of interest records from location servers, which are close to user position, devoid of compromising privacy of user or data that is stored at server. We propose a location based query solution that utilizes two protocols that facilitate a user to confidentially determine and obtain location data in which initial step is for a user to secretly determine their location by means of oblivious transfer on a public grid and the other step involves a confidential information recovery interaction that recovers record by means of high communication efficiency. This is resourceful in numerous circumstances. We reach this by application of a two stage approach. In initial stage is on basis of oblivious transfer and other stage is based on private information recovery.

REFERENCES

[1] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998.

[2] 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.

[3] 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.

[4] E. Kushilevitz and R. Ostrovsky, "Replication is not needed: Single database, computationally-private information retrieval," in Proc. FOCS, Miami Beach, FL, USA, 1997, pp. 364–373.

[5] L. Marconi, R. Pietro, B. Crispo, and M. Conti, "Time warp: How time affects privacy in LBSs," in Proc. ICICS, Barcelona, Spain, 2010, pp. 325–339.

[6] S. Mascetti and C. Bettini, "A comparison of spatial generalization algorithms for lbs privacy preservation," in Proc. Int. Mobile Data Manage., Mannheim, Germany, 2007, pp. 258–262.

Panchangula Priyanka received her B.Tech degree in Computer Science and

Engineering in the year 2013 and pursuing M.Tech degree in Computer Science and Engineering from Krishnaveni Engineering College for Women.

B.Lakshmi Kanth received his M.Tech degree in Computer Science and Engineering and B.Tech degree in Computer Science and Information Technology. She is currently working as an Asst Professor in Krishnaveni Engineering College for Women.