IJARES/August 2015/Volume-3/Issue-8/2114-2119 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

TOWARDS ENSURING OF SECURED PRIVACY CONCERNING LOCATION BASED DATA

Ramya Venna[1], G.Mahesh[2]

[1]M.Tech Student, Dept of CS, Arjun College of Technology & Sciences, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, Arjun College of Technology & Sciences, Hyderabad, T.S, India

ABSTRACT:

The services that are offered by the location based services are based on the interesting points of database. Novel issues of privacy metrics were projected that confines user confidentiality regarding location based services. By means of recovering of interesting Points from the database server, user obtains answers to several queries of location based. We initiate an improved approach on previous methods for the queries of location based by introduction of two stage approach, in which the initial is based on oblivious transfer and other is on the basis of retrieval of private Information for achieving of protective solution for both user and server parties. The intention of our protocol is to obtain a set of interesting points records from location server, which are close to user position, devoid of compromising user privacy or else data that is stored at server.

Keywords: Location based services, Private Information retrieval, Database, User privacy, Location server, Oblivious transfer.

.

1. INTRODUCTION:

There was a remarkable increase in mobile devices that are querying location servers for points of interest data. Among several challenges that were projected to extensive deployment of such an application, assuring of privacy is the most considered issue. The

location server provides the services based on location and uses up its assets to collect data regarding several important and interesting points hence location server will not reveal any information devoid of price [1]. Hence the services based on location should make sure that data of location servers are not provided permission by any illegal user. During transmission procedure, users are not authorized to find out any information for which they are not allowed and is important that solutions are devised that deal with queries of user privacy issues, however also put off users from accessing of content to which they do not contain permission. In our work we introduce an improved method for the queries of location based by introduction of two stage approach, in which the initial is based on Oblivious Transfer and other is on the basis of retrieval of private Information for achieving of protective solution for both user and server parties. The user is secluded since server is not capable to determine the location. Correspondingly, the data of server is secured as the malicious user can decrypt block of data that is obtained by the retrieval of private information by encryption key that is acquired in earlier stage [2][3]. Users cannot achieve any additional information than they have paid for.

2. METHODOLOGY:

For the most of the discussed issues in the past are solved by introduction of a scheme of private information retrieval location method. The fundamental proposal is to utilize information retrieval to facilitate user to query the location database devoid of compromising query privacy. The methods of private information retrieval permit a user to recover data from a database, devoid of disclosing index of data to be retrieved to database server. Ghinita et al. have applied a variant of private information retrieval which is on basis of quadratic residuosity. The problem of quadratic residuosity states that it is computationally tough to decide whether a number is quadratic residue of composite modulus p ($y^2 = x \pmod p$), where factorisation of p is unidentified. This idea was expanded to make available database protection and hence this procedure consists of two stages. In earliest stage, user as well as server makes use of homomorphic encryption to permit user to secretly decide whether location is present within a cell, devoid of disclosing coordinates to server. In second stage, private information retrieval

is used to recover data that is contained within proper cell. We introduce a novel method for the queries of location based that contain important enhancement regarding Ghinita et al. approach. The users in our representation make use of some location-based service that is provided by location server. The intention of our protocol is to obtain a set of interesting points records from location server, which are close to user position, devoid of compromising user privacy or else data that is stored at server. Our proposal is organized as two stage approach, in which the initial is based on Oblivious Transfer and other is on the basis of retrieval of private Information for achieving of protective solution for both user and server parties. In initial stage, user secretly decides their location within a public grid, by means of oblivious transfer which contains the data of Identity as well as related symmetric key for block of data within private grid. In other stage, user implements a communicational resourceful private information retrieval to recover suitable block within private grid [4]. This block is decrypted by means of symmetric key that has got in earlier stage. Hence our protocol provides security for user and server.

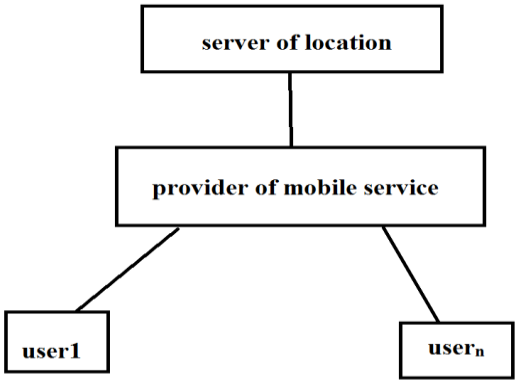

Fig1: a view of system model.

3. AN OVERVIEW OF PROPOSED SYSTEMS:

The authors have proposed privacy metrics that enables users to identify values that match better to their query privacy needs. From these metrics they recommend spatial generalisation algorithms that coincide with user privacy needs. We introduce an improved approach on earlier methods for the queries of location based by introduction of two stage approach, in which the initial is based on oblivious transfer and other is on the basis of retrieval of private Information for achieving of protective solution for both user and server parties. The proposed solution was efficient and realistic in numerous circumstances. The system representation consists of three types of entities such as shown in fig1 such as set of users who desire to access location data,

provider of mobile service as well as location server. From viewpoint of user, provider of mobile service as well as location server will compose a server, which serves functions. The user does not require being concerned with specifics of communication. The users in our representation make use of some location-based service that is provided by location server. The user is secluded since server is not capable to determine the location. Correspondingly, the data of server is secured as the malicious user can decrypt block of data that is obtained by the retrieval of private information by encryption key that is acquired in earlier stage. Users cannot achieve any additional information than they have paid for. Intention of mobile service provider is to set up and preserve communication among location server as well as user. We assume that mobile service provider is trustworthy to preserve the connection; we make a consideration of only two possible adversaries. The final objective of our protocol is to obtain a set of interesting points records from location server, which are close to user position, devoid of compromising user privacy or else data that is stored at server [5]. We attain this by application of two stage approach in which first is based on oblivious transfer and other is on the basis of retrieval of private Information. The oblivious transfer based procedure is used by user to get hold of the cell identity, where user is located, as well as equivalent symmetric key. The knowledge of cell Identity as well as symmetric key is subsequently used in private information retrieval based procedure to get hold of and decrypt location data. User implements a communicational resourceful private information retrieval to recover suitable block within private grid. This block is decrypted by means of symmetric key that has got in earlier stage. Hence our protocol provides security for user and server. The user determines location within openly generated grid by means of GPS coordinates and outlines an oblivious transfer query [6]. As private information retrieval does not necessitate that a user is controlled to obtain just single block, location server desires to implement some defence for its records. Thus when user makes use of private information retrieval to get hold of more than single record, data will be insignificant resulting in enhanced security for server database.

4. CONCLUSION:

A location based service can be a data service as well as utility service that are manageable by mobile devices. The private information retrieval techniques permit a user to recover data from a database, devoid of disclosing index of data to be retrieved to database server. We commence an enhanced approach on earlier methods for the queries of location based by introduction of two stage approach, in which the initial is based on oblivious transfer and other is on the basis of retrieval of private Information for achieving of protective solution for both user and server parties. The intention of our procedure is to obtain a set of interesting points records from location server, which are close to user position, devoid of compromising user privacy or else data that is stored at server. In early stage, user secretly decides their location within a public grid, by means of oblivious transfer which contains the data of Identity as well as related symmetric key for block of data within private grid. In other stage, user put into practice a communicational resourceful private information retrieval to recover suitable block within private grid. This block is decrypted by means of symmetric key that has got in earlier stage and hence our protocol provides security for user and server.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in Proc. CRYPTO, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791–791.

[5] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. EUROCRYPT, vol. 1592, Prague, Czech Republic, 1999, pp. 223–238.

[6] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino, "Privacypreserving and content-protecting location based queries," in Proc. ICDE, Washington, DC, USA, 2012, pp. 44–53.

Ramya Venna, Graduate in B.Tech CSE from Kodada Institute of Technology and Science, kodad Nalgonda District.

Graduated in B.Tech CSE in 2007 from Madira Inst. Of Technology & Science(MITS), odad,NLG Dist He received Masters Degree in M.Tech [CSE] Arjun College of Technology & Sciences,R.R. Dist. Presently he is working as Assistant Professor in CSE Dept. in Arjun College of Technology & Sciences, Hayathnagar,R.R. Dist Telangana State, India.