ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Survey on Preserving User Privacy and Preventing Server Content in Location Based Service

Mhetre Suhasini S. [1], Prof. Phatak Amol A.[2], Prof. Pottigar Vinayak V[3]

Department of Computer Science and Engineering, Sinhgad College of Engineering, Kegaon, Solapur, India

Head of Department, Department of Computer Science and Engineering, Sinhgad College of Engineering, Kegaon, Solapur, India

Department of Computer Science and Engineering, Sinhgad College of Engineering, Kegaon, Solapur, India

ABSTRACT: In this mobile world all the services are available in a single entity with one click. Location Based Services [LBS] is a data, stimulation and utility administration by and large available by cell phones, for example, cellular telephones, GPS gadgets, pocket PCs, and working through a portable system. LBS can offer numerous administrations to the clients in light of the topographical position of their cell phone. The administrations gave by LBS are commonly in view of a Points of Interest [POI] database. By recovering the Points of Interest from the database server, the client can get answers to different area based inquiries however while doing this client area data can be followed by different ways and it can be utilized for area based advertising and other powerless purposes. These days, it is simple for a man to take in his or her area with the assistance of a location based server empowered gadget. An area based administration called LBS is another and creating innovation for portable clients. When this area is given to LBS through questioning, it is conceivable to learn area subordinate data, for example, areas of companions or places, climate or activity conditions around the area. This issue is characterized as tails: (i) a client needs to question a database of area information, known as POIs as well as does not have any desire to uncover his or her area to the server because of protection concerns; (ii) the proprietor of the area information, that is, the area server, does not have any desire to just appropriate its information to all clients. This work proposes a noteworthy upgrade upon past arrangements by presenting a two phase approach, where the initial step depends on Oblivious Transfer and the second step depends on Private Information Retrieval, to accomplish a safe answer for both sides. The arrangement it present is productive and viable in numerous situations. This work executes our answer on a desktop machine and a cell phone to survey the Efficiency of our convention. It likewise presents a security demonstrates and examines the security with regards to our convention. At last, our proposed framework highlights a security shortcoming of our past work and introduces an answer for defeat it.

KEYWORDS: Location Services, Querying, Point of Interest, Location Server, Privacy Maintenance.

I. INTRODUCTION

An area based administration called LBS is a versatile application that is reliant on the area of a cell phone, similar to cellular telephone -Data administrations available with cell phones through the portable system and using the capacity to make utilization of the area of the cell phone - Open Geospatial Consortium - characterized LBS benefit also-"A remote IP benefit that utilizations geographic data to serve a versatile client, any application benefit that endeavors the position of a portable terminal." A Location Based Service (LBS) is a data and diversion administration, open with cell phones through the portable system and using the capacity to make utilization of topographical position of the cell phone.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Area based administrations give the versatile customer's customized administrations as indicated by their present area. The Location object speaks to a geographic area which can comprise of a scope, longitude, timestamp, and other data, for example, bearing, elevation and speed [4]. In area based administrations (LBS), clients with area were cell phones can question their surroundings anyplace and whenever. While this pervasive processing worldview brings awesome comfort for data access, it raises a worry of potential interruption on client's area protection, which has hampered the broad utilization of LBS [1].

The location based server is situated in route framework that gives area and details to the clients requesting for their services. Location based server transmits location information that shows requesting area details to corresponding clients. All location based services synchronize operations so that these rehashing signs are transmitted at the same moment. The signs, moving at the pace of light, land at a location based server provides distinctive details since a few other servers are not provide those details. The separation to these servers can be controlled by assessing the measure of location details and it takes for their signs to achieve the recipient.

A few social studies report that clients turn out to be more mindful about their protection and may wind up not utilizing any of the area based administrations. A Location based administration can offer numerous administrations to the clients taking into account the land position of their cell phone. New innovations can pinpoint your area whenever and place. They guarantee wellbeing and comfort yet undermine protection and security.

The administrations gave by a LBS are regularly taking into account a state of interest database. By recovering the Points Of Interest [POIs] from the database server, the client can get answers to different area based questions, which incorporate yet are not restricted to - finding the closest ATM machine, corner store, healing facility, or police headquarters. As of late there has been a sensational increment in the quantity of cell phones questioning area servers for data about POIs. Among numerous testing obstructions to the wide organization of such application, security confirmation is a noteworthy issue. Case in point, clients may feel hesitant to reveal their areas to the LBS, since it might be workable for an area server to realize who is making a specific question by connecting these areas with a private telephone directory database, since clients are liable to perform numerous inquiries from home. LBS need to guarantee that LS's [Location-Server] information is not got to by any unapproved client. Amid the procedure of transmission the clients ought not to be permitted to find any data for which they have not paid. It is in this way urgent that arrangements be formulated that address the security of the clients issuing questions, additionally keep clients from getting to substance to which they don't have approval.

II. COMPARATIVE STUDY

The comparative study of this topic includes various method analysis based on Recall, functional flow of the system, average guessing threshold and random threshold levels.

Methodology	Recall	Functional Flow	Average Guessing	Random Guessing
Location Accuracy	1.0000	0.2931	0.2941	0.2551
Location Based Searching Service	0.0044	1.5932	1.2541	5.2551
Oblivious Transfer Algorithm	1.2220	0.3951	0.3941	0.3551
Private Information Retrieval Algorithm	0.0544	2.4432	2.3341	4.331
Query Retrieval Algorithm	2.2220	1.3951	1.3941	5.3551

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A reciprocal procedure to the blend zone approach depends on k-secrecy. The idea of kanonymity was presented as a strategy for saving protection while discharging delicate records. This is accomplished by speculation and concealment calculations to guarantee that a record couldn't be recognized from (k − 1) different records.

The answers for LBS utilize a trusted anonymiser to give secrecy to the area information, with the end goal that the area information of a client can't be recognized from (k − 1) different clients. An upgraded trusted anonymiser approach has additionally been proposed, which permits the clients to set their level of protection in view of the estimation of k. This implies, given the overhead of the anonymiser, a little estimation of k could be utilized to expand the effectiveness. Then again, a huge estimation of k could be enhanced the security, if the clients felt that their position information could be utilized noxiously. The principal stage depends on a two-dimensional absent exchange and the second stage depends on a communicational proficient PIR.

The unaware exchange based convention is utilized by the client to acquire the cell ID, where the client is found, and the comparing symmetric key. The learning of the cell ID and the symmetric key is then utilized as a part of the PIR based convention to get and decode the area information. The motivation behind this technique is for the client to acquire one and one and only record from the cell in people in general network P.

III. EXISTING METHODOLOGY

In the existing system, all the researchers, developers and authors characterize the issues in existing methodology that does not deal with security of the client furthermore neglected to ensure the area server content. Questioning about the area subtle elements, the server can't keep their points of interest from the client and the client can't protect their security from server [6].

IV. PROPOSED METHODOLOGY

A definitive objective of our proposed framework is to get a set of Point Of Interest records from the Location Server, which are near the client's position, without trading off the protection of the client or the information put away at the server. We propose this by applying a two phase approach:

- Oblivious Transfer [OT]
- Private Information Retrieval [PIR]

The primary stage depends on a two-dimensional unaware exchange. The second stage depends on a communicational efficient PIR.

The Steps required in every errand is said beneath. They are:

The client secretly decides his/her area inside an open lattice, utilizing neglectful exchange: This information contains both the ID and related symmetric key for the square of information in the private matrix. The client executes a communicational effective PIR, to recover the suitable piece in the private grid: This square is decoded utilizing the symmetric key got as a part of the past stage. Our convention in this way gives security to both the client and the server. The client is secured in light of the fact that the server can't decide his/her area. Essentially, the server's information is ensured subsequent to a pernicious client can just decode the square of information got by PIR with the encryption key obtained in the past stage. At the end of the day, clients can't increase any a bigger number of information than what they have paid for.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

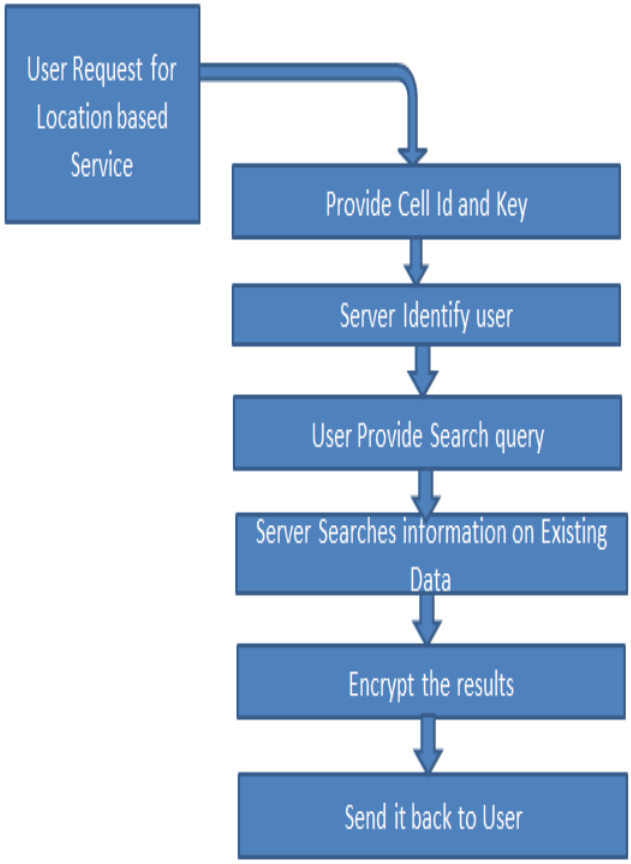

Fig.3. System Flow Diagram

V. CONCLUSION

This proposed approach model exhibits the effectiveness as for rate and common sense of our methodology for desktop and cell phones inside down as far as possible. We broke down the execution of our convention and observed it to be both computationally and communicationally more proficient than the arrangement by Ghinita et al., which is the latest arrangement. We likewise executed a product model that highlighted the proficiency of our convention. Further to this work, the protection of client data who attempt to recover the information can be kept up by applying the private data recovery calculation.

REFERENCES

[1] Beresford, F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):46-55, 2012.
[2] Hoh and M. Gruteser, "Protecting location privacy through path confusion," Proc. SecureComm'05, 2005, pp. 194 - 205.
[3] Damiani ML, Bertino E, Silvestri C (2010) The probe framework for the personalized cloaking of private locations. Trans Data Privacy 3:123–148
[4] Dewri R, Ray I, Whitley D (2010) Query m-invariance: Preventing query disclosures in continuous locationbased services. In: Eleventh international conference on mobile data
[5] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection," GeoInformatica, pp. 1 - 28, 2010.
[6] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, Private queries in location based services: anonymizers are not necessary," Proc. SIGMOD'08., 2008, pp. 121 - 132.
[7] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacy preserving matching of spatial datasets with protection against background knowledge," Proc. GIS '10, 2010, pp. 3 - 12.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

[8] M. Gruteser and D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking," Proc. 1st international conference on Mobile systems, applications and services, 2003, pp. 31 - 42.
[9] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," Proc. UbiComp'07, 2007, pp. 372 - 390.
[10] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," Proc. CRYPTO'89. 1990, pp. 547 - 557.
[11] "Openssl," http://www.openssl.org/, 2011, [Online; accessed 7-July-2011].
[12] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," Proc. CRYPTO'89. 1990, pp. 547 - 557.
[13] A. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Computing, vol. 2, no. 1, pp. 46 - 55, 2003.
[14] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against locationbased personal identification," Proc. Secure Data Management, Lecture Notes in Computer Science, W. Jonker and M. Petkovic, Eds., 2005, vol. 3674, pp. 185 - 199.
[15] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965 - 981, 1998.