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. 3, Issue 12, December 2015

Privacy Grid System for Continuous Location-Based Services: A Survey

Trupti Takale Prof. Soniya Mehata

Dept. of Computer Engineering, Alard college of Engineering and Management, Pune, India

ABSTRACT: Recently, Smartphone are highly accurate at finding location information that it enables many users to afford various location complex services and on the other side that having mostly personal information. The security of location privacy is one of the most important problems in location-based services. For Continuous Snapshot and LBS we required third party of semi-trusted domain for accessing similar operations and giving the results to the users.This can be the find for nearby points of interest (POIs) (e.g.restaurants, bank, ATMS and hotels), location-aware advertising by companies, road traffic information tailored to the roads or highways and path of a user is traveling and so on.

I.INTRODUCTION

This can be the search for near points of interest(POIs) (e.g. restaurants and hotels), location-aware advertisingby companies, traffic information tailored to the highwayand direction a user is traveling and so forth. The useof LBS, but can tell much more about a person tohypothetically untrustworthy service providers than many peoplewould be willing to disclose. By tracking the requests ofa person it is possible to build a movement profile whichcan reveal information about a user's work (office location), medical records (visit to specialist clinics), governmental views(attending governmental events), etc.Enabled by arranging infrastructures such as GPS, location-based services (LBS) are becoming an progressively essential element of not only travel but also serious applications such as emergency response, public safety etc.[2]

II.RESEARCH BACKGROUND

An overview of various location privacy thoughts including location *k*-anonymity, location confusion, location spatial cloaking or patio-temporal cloaking. Then how these concepts relate to the privacy concepts for outdated databases. Basically existing system is based on the bottom up generation method and it works on the statistics of the user locations. It employed a grid structure that hierarchically decomposes the whole space into levels. The root of the grid is at the level zero that covers the whole space and has only one grid cell. The Casper cloaking algorithm first locates the request issuer in a corresponding grid cell and checks the number of users in the grid cell. If it satisfies the k-anonymity then the grid cell as the cloaking region. If not it checks for the horizontal or vertical cells and check the total number of users in cell plus horizontal cell or cell plus vertical cell. The horizontal sum is checked against the vertical sum, if the greatest sum is greater than k, and then selects it as the cloaked region. The above check is not meet the k-anonymity goes up the parent grid. Casper cloaking works well in the traditional architecture model because it can generate the smallest possible cloaked region safely and quickly and it provides good quality of services.

1.Location *k*-anonymity

For location privacy is a *k*-anonymity based approach which depersonalizes data through concernmethods before forwarding it to the LBS providers. Location *k*-anonymity is first studied by Gruteser and Grunwald. The work travels from several drawbacks. First,it assumes asystem wide static *k* value for all mobile clients, whichdetects service quality for those mobile users or clientswhose privacy necessities can be fulfilled using less*k* values. Second, approach flops to provideany quality of service warranties with respect to sizes of the cloaking boxes formed. Because of thequad tree based algorithm anonymizes messages by dividing quadtree cells till the no ofmessages in each cell falls below *k* and by returning the earlier quadrant for each cell as the spatial cloakingbox of the messages under that cell.

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. 3, Issue 12, December 2015

2. Location confusions

Location confusion defined as "the means of consciouslycorrupting the quality of materialabout an individual's locality in command to protect that individual's location privacy."The main idea is forthe system to alter or hide the original location of the user while still being able to offer the appropriate levelof service to the user. In addition, the user must have a way to determine the level of modification that its locationwill suffer, depending on the amount of information give its exact position.From methods in the noise based method adds Gaussian noise to samples in order to produce a new location. Even this technique is easiest one available, it may have drawbacks For example, the noise may tend to leave the new confused point closer to the center than a consistentlyrandom position.

III.LOCATION SPATIAL CLOAKING

The centralized model utilizes a centralized trustworthy third party, known as locationanonymizing server, as a middleware among users and LBS database servers. locationanonymizingserver collects exact location information and confuses them into a cloaked region. Proposedspatio-temporal cloaking algorithm assumes a unified k-anonymity requirement which brings less flexibility to the users. it enables a personalized k-anonymity necessity it faceswith large working out overhead for calculating the clique graph and it is restricted to a narrow range of small k. New Casperuses a plain or adaptive grid-based pyramid structure to find proper cloaking region butmay often generate larger cloaked region than predictable. when the total of mobile user is big or they are moving speedily, system can simplyencounter its performance bottleneck.

IV.SPATIO-TEMPORAL CLOAKING

Motivated by anonymization procedures in privacy preserving data mining, a large body of work in location privacy is centered on the idea of k-anonymity or location cloaking With this methodology, a reliable anonymizer distortions raw user positions by spreading them from a point location to an area and sending a regioncoveringmore than a few other users to the untrusted server. Aside from the famous privacy problems of anonymization in data mining, location anonymization and cloaking undergo from numerous drawbacks.

V.LITERATURE REVIEW

Spatial cloaking techniques have usually used to reserveuser location confidentiality in LBS. Most of the existing spatial cloaking techniques on a fully-trusted third party,generally termed location anonymizer, that is necessary between user and service. Operatorgives to LBS, the location anonymizer will blur the userprecise location into a cloakedarea such that cloaked area includes at least k otherusers to satisfy k-anonymity. The TTP model has four major drawbacks as It is difficult to find a third party that can be fully trusted. Second, All users need to constantly update theirlocalities with the location anonymizer, even when they arenot contributed to any LBS, so the location anonymizerhas plentyevidence to compute cloaked areas. Third, Because the location anonymizer stores the exact locationinformation of all users, give in the position anonymizer exposes their locations. Fourth, k-anonymity normallyreveals the inexact location of aoperator and the positionprivacy depends on the user distribution. In a system with such regional location privacy it is tough for the user tospecify personalized privacy requirements. The sensitivitybased approach relieves this issue by discovery acloaked area based on the number of its companions that is minimum as popular as the user's specified public region.

VI.CONCLUSION

In this paper, we proposed a dynamic grid system for giving privacy-preserving endless LBS. Our DGS Contains query server and service provider andcryptographic tasks to distribute the whole query processing assignment into two parts that are achievedindependentlyby QS and SP. DGS does not involve any fully trusted third party, instead we require only the much weakersupposition of no approval between QS and SP. Thissplit-up also moves the data transfer load away fromthe operator to the low-cost and high-bandwidth linkbetween QS and SP. We also considered efficient protocolsfor our DGS to support both continuous k-nearest-neighborand range queries. To calculateperformance ofDGS, we match it to the state-of-the-art techniquerequiring a TTP. DGS delivers better privacy assurances than the TTP scheme and the experimental resultsshow that DGS is an order of level more capablethan the TTP pattern, in terms

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. 3, Issue 12, December 2015

of communication cost.DGS also constantly outperformsthe TTP scheme for NN queries; it is equivalentor slightly more expensive than the TTP scheme for rangequeries.

VII.FUTURE WORK

To build a Technique for providing security for Mobile peer to peer Network from disclosing its location for not so safe Location Base Server with the help of Dual Spatial Cloaking Algorithm.

REFERENCES

1. International Journal of Science and Research (IJSR)"Survey on Security and Privacy Aware Location Based Service System". By Sneha Sonwane, D. A. Phalke.
2. IEEE INFOCOM 2011, "Protection of Query Privacy for Continuous Location Based Services"Aniket Pingley, Nan Zhang, Xinwen Fu, Hyeong-Ah Choi, Suresh Subramaniam, and Wei Zhao.
3. "A Survey of Location-Based Privacy Preserving" by Gaoming Yang, Jingzhao Li, Shunxiang Zhang, Huaping Zhou.
4. IJCTT FEB 2015, "Location Based Search Queries with Ultimate Privacy Preserving Considerations" by M.S.Ramadevi, S. Prabhu.
5. "Achieving Efficient Query Privacy for Location Based Services" by FemiOlumofin, Piotr K. Tysowski, Ian Goldberg, and UrsHengartner.
6. "Location Privacy" by *Ashwin Machanavaj jhala.*
7. WWW 2008 / Refereed Track: Mobility April 21-25, 2008 · Beijing, China, "Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid" by BhuvanBamba, Ling Liu, Peter Pesti, Ting Wang.
8. *International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 03 – Issue 06, November 2014,* "Improving the Similarity for Privacy in Location Based Service" Reemah M. Alhebshi, Jonathan Cazalas.
9. Springer Science Business Media, LLC. 2008, "Privacy Protected Spatial Query Processing for Advanced Location Based Services" by Wei-Shinn Ku · Yu Chen · Roger Zimmermann.
10. "Enabling Private Continuous Queries For Revealed User Locations" by Chi-Yin Chow and Mohamed F. Mokbel.
11. TRANSACTIONS ON DATA PRIVACY 5 (2012), "Mobile Systems Privacy: 'MobiPriv' aRobust System for Snapshot or Continuous Querying Location Based Mobile Systems".by Leon Stenneth and Philip S. Yu
12. March 2013,"A Grid-based Cloaking Area Creation Scheme for Continuous LBS Queries in Distributed Systems" by Hyeong-Il Kim, Yong-Ki Kim, Jae-Woo Chang.
13. "Scaling location-based services with location privacy constraint: architecture and algorithms" by Bhuvan Bamba.