Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 12, Number 1 (2016), pp. 733-740

http://www.ripublication.com

Geo tagged Query based on Privacy Location Services with Three Levels of Security

[*1]Angel Sweety Sheeba.S and [2]Kavitha Esther Rajakumari

*[*1]PG, Computer Science Department, Sathyabama University, Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai-600 119, Tamilnadu, India.*

[2]Research Scholar in Computer Science Department, Sathyabama University, Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai-600 119, Tamilnadu, India.

Abstract

Data mining is a popular technology which is used to find out the message in the data warehouse. The tools of data mining also used to anticipate or estimate the trends of a particular Business. The events occurred in the past can be studied and analyzed to get the knowledge of the future outcome. These tools will provide solution but takes time to solve. The experts may miss the exact information, since they are out of the assumptions. There are two aspects which are favorable in data mining. They are high end security and potential security risk. In order to overcome the security risk, the three layer of security model is suggested. The 3 levels of security hide the user's exact location and server will provide the information about the wide range of area depends on the query. KNN-query algorithm is used to select the users nearest location and ontology is used to fetch the relevant information.

Keywords Three levels of Security, Information, K-Nearest Neighbor, Ontology.

Introduction

Location based services provides the information about various Service Providers like Hospital, Hotel, Schools, Colleges and etc. The LBS can be implemented by Android application with geo tagged information about Service Providers. The user can penetrate their Query. As per the Query entered the nearest Service Provider information is fetched. Geo tagged LBS information is loaded. Service Provider can be categorized as normal and paid Service Providers. i) Normal SP-User name, Type of service. ii) Paid SP-Images, Video, Awards and Rewards. Registered and non-

registered service provider information is also stored. Semantic concept is used to correlate the nearest information. E.g.: Schools, colleges, etc. Android user makes a query to the intermediate server. Then it sends the query to server. In that data can be retrieved on the basis of geo tagged query and checking privacy profile (user). The modifications are made to have the privacy of user location in which query is restricted. 3 levels of security have been used such as High, Medium and Low. These 3 levels are used for privacy protection. High level is used to hide the user's exact location. Medium level is used to give the nearest location and the Low level provides the exact location.

Literature Survey

[1] Gabriel Ghinita et.al, have suggested Prive is a decentralized architecture to provide high end privacy to user. It hides the user information by giving related spatial Queries to LBS. The user can give their query to intermediate trusted common server. This intermediate server hides user information like his ID, Location etc. This intermediate server submits the Query to LBS by preserving user Privacy, so security enhanced. Prive provides HILBASR anonymization technique gives confidentiality of user information irrespective of user type. Mobile user gives location based Query and their information is stored in order such that it provides hierarchical manner.

[2] Man Lung Yiu et.al, have scheduled Space twist method starts with random location different from users actual location, then it will track nearest neighbor which tend to achieve user location. The nearest neighbor continuously identified till the exact user identified. The user query processing from the client gets the Point of Interest (POI) progressively from the Server. It improves user privacy and performance. Server side granular search technique improves accuracy, reduces cost and time. Space twist uses server side granular search technique and client side processing technique. So this method provides higher location privacy and less cost.

[3] Reynold Cheng et.al, have planned the privacy of the user is improved by hiding the location of the service requesting user. This model provides the protection method to improve privacy of the user. Tracking is difficult in this method. In LBS present and past location privacy of the requester has to be maintained confidential. Cloaks will improve the privacy by giving lower resolution information about the user. The result of Query will give all relative information to the time and space. By search engine optimization, the user position will be located. This method is also a time consuming to relate the user current location. ILRQ imprecise location based range query gives approximate probable answer for every Query, which gives the percentage of correctness of the answer. This paper handles information cloaking, User information confidentiality and Service Quality. Estimated queries protect the user information.

[4] Hidetoshi Kido et.al, have perspective Anonymous communication technique, In that the user will send false position with their true position data in order to

maintain security or privacy. The location of the user will be detected with the true position data. Anonymous communication techniques in LBS discuss about 2 issues. i) Increasing cost and Time, speed reduction. ii) Easy identification of dummy movement. In anonymous communication technique, the server of the network creates the false and true position data. The user will not generate. It improves the privacy, cost, speed and time of communication.

[5] Yinan Jing et.al, have proposed the user provides Query to cloud service provider. The Owner of the data assigns the database management to other vendor called service provider. It uses Euclidean distance instead of the road network distance. K-nearest neighbor Query verification technique makes use of voronoi diagram and gives the honest to user query result. This paper verifies the K-nearest neighbor gives both shortest path from Query point and Euclidean space. Voronoi diagram of network verification approach uses each result object's network voronoi cell in order to complete the correctness of KNN result. It regards both path and distance.

[6] Macro Gruteser et.al, have suggested to use middleware architecture and algorithm for centralized LBS. User will give the lower resolution information with respect to space and time. Middleware of the specific constraints are used to identify the exact user. Anonymity in LBS has to provide way to identify exact user. The user anonymous information should be sufficient to identify the user by server. This middleware algorithm provides scale for location anonymity. It decreases either spatial resolution or temporal resolution to improve user privacy. By giving lower Spatial and temporal resolution of user the privacy is improved.

[7] Pierangela Samarati et.al, have determined Micro data is the specific data to protect the anonymity of entities. This paper provides solution to release micro data when conserving the respondent's anonymity. K-anonymity provides link to identify the information. By suppression technique, the truthfulness of entity confirmed. Nowadays the recipient can combine the de identified micro data with other public data. In one table the Public data can be displayed by suppressing the confidential data. Each row in the table has the link to one more table which has all information of the user. So generalization and suppression is the techniques used to protecting respondents identities. This paper discusses generalize table concept, minimal elimination and minimal observation. It handles what needs to be suppressed and what should be generalized.

[8] Gabriel Ghinita, Keliang Zhao et.al, have proposed Spatial K-anonymity protects the user location information. SRA replaces the correct location of the user. This paper provides the framework to get safe cloaking algorithm which is established on spatial index for a user U. The sub tree given in a tree structure can be identified to anonymize user U. If the user U and Sub tree given two algorithms GH and AR gives the ASR for U. This method also has frequency aware property to identify the frequent hit of same query by the right user. Also provide efficient and effective way of secured methods. This

paper discussed reciprocal framework which provide many security algorithms for spatial K-anonymity with variable query frequency.

[9] Brian et.al, have scheduled the data holder provides information to service provider application. This paper gives framework of anonymization is to help mobile users in the scheme of outsourcing domain driven data mining. This method has many components designed to anonymize data, in the same way it preserves relevant or actionable patterns. Attribute correlation are computed to assure care of main features. The knowledge discovery of traditional data mining is done with no domain knowledge. It affects real needs. This produces the gap between intellectual objective and business assumptions. The experts of domain and domain knowledge will get valid pattern and model which is suitable to real scenario. To prevent identification of individual during redistribution of data could be secured via anonymization. The privacy retaining methods are able to anonymize data for usage by domain-driven method. By using this methodology, the publishers can get good quality for domain-driven method by sustaining security needs.

[10] Tao Gu et.al, have introduced the infrastructure which provides awareness context. It needs correct context model to mention, shape and to get the information of context. Based on our context model, context-aware services provided by middleware architecture. The application should be capable to work in frequently changing environment, Agents, Devices and Services. Context aware system constructing method is difficult and tedious. In this paper, context model utilizes owl ontology to give support in context aware middleware duty. Based on owl to show, manage and approach context information in brilliant environment. This model explains context, categorization, their need of each other information quality and context reasoning.

[11] Yingyi Bu et.al, have proposed Inconsistent context is the unlikable behaviors of context-aware applications, which tends to use less believed it. In this paper, the context modeling approach which is based on ontology extended to avoid inconsistent. Context awareness intent to reduce user's consideration to different computational devices. A nice context model will give simple and well structured context aware applications. In real world, the context aware application is weak. It extends ontology based model in terms of providing detailed information like context state, frequency and time. The perfect and logical context is provided by inconsistency resolution algorithm. The PVCM model creates the mechanism of context management and gives model of conflicting resolution algorithm.

[12] Peter Mika et.al, has suggested binary model for ontology is designed with ternary model of instance, concepts and actor. This representation is shown by community-based semantics through graph transformation process. Ontology is an accurate detail of domain conceptualization. In this paper, is formulated a universal semantic social network model which is called as Actor-Concept-Instance model of ontology's. The comparison study of emerging ontology method as well as traditional ontology method is given in this paper. Creation

and maintenance of semantic web is a social one. This is also called as web for machines. The semantic web uses have required interpretive and related ability for ontology creation and maintenance. So the ontology are mingled with community of context by which it is created.

[13] Matt Duckham et.al, have suggested obfuscation deals about protecting confidential information by degrading quality of information. This paper provides an idea about obfuscated Location-based service. This method balances one's information quality service need and user's location privacy.
It handles secured method to protect user's location information. The complex model and algorithm take care of user's location privacy and high quality location-based services.

[14] Panos Kalnis et.al, have invented the mobile use make use of location based services. This paper provides method for hiding identity based on the location. The user may request spatial query even though this method provides protection for their location based information. Nowadays positioning devices GPS are popular. This is a risk of leaking secured information in Location-based services.
In real scenarios, the user afraid of accessing the service which confess their religious or political partnership. K-anonymity has been used for announcing micro data such as voting registration data, census and medical. The actual location by k-anonymizing spatial region is hidden by cloaking method. The spatial region covers the client who issue the query, also k-1 other users. We studied location based services retain the anonymity of query. The Moto is to cover user location by giving spatial region.

[15] Bugra Gedik et.al, have planned locating technologies where generated firm retail market for location-based applications. An important challenge is in wide distribution of information. This method secured user location privacy from hazards. Because of unchecked usage of LBS.
The mobile client can design and change their specification about their location with one message including least requirement about anonymity level and blender tolerance. The user also should specify spatial and temporal dimensions.

[16] Yin Yang et.al, have suggested the mobile devices are enclosed with positioning ability. The multi dimensional data are used in location based applications by geographical outsourcing. The data management is nominated by the data owners to LBS which process the queries. Outsourcing of database proposed in this paper. Spatial outsourcing provides the spatial data from different sources. The key distribution center gets the private and public key from the data owner. A set of signature needed for authentication purpose is transmitted by the LBS.
The completeness and Soundness of the results can be verified by the client, since LBS are not the data owner. Each and every record has been used in the result set are present in owner's database cannot been modified. The query authentication for multimedia should be replicated. The metrics like cost of the construction, size of index and verification exceeds the current solution.

[17] Adam Meyerson et.al, have planned K-anonymization provides data privacy and integrity. There are two general versions, NP hard and polynomial time algorithm. Slightly changed algorithm removes runtime of the algorithm O (k log k). That is O (k log n) approximation. Here n is the degree of the relation. This algorithm works fast and efficient.

The large volumes of personal information accessed by the data miner are used to spot the data correlation. The privacy-protecting data mining are used for discouraging the Queries and data values. The approximation algorithm O (k log k) is nice. This is best for high-dimensional records. The K-anonymizing is a database used to define the problem via the components and computational risk of tuple. The greedy approximation algorithm is powerful for the problem.

[18] Bugra Gedik et.al, have defines the location privacy protection model for personalizing the K-anonymity process. It has two features. Initially, we maintain a undivided framework for privacy personalization and it support k-anonymity location for the users. Next, the efficient information disorder engine has been prepared to run the protection mediator.

Although with LBS mobile users can get many location based information services, the LBS may lead to threaten the mobile user's privacy and to disclose the LBS to serious vulnerabilities for misuse. Two threats can happen. One is attacks on Passive logging and another is privacy threats. The major way to minimize the privacy risks on location is to preserve the location information in K-anonymity. The location privacy has been maintained by the personalized K-anonymity process. In this process, every user can describe about the granularity of every message.

[19] Latanya Sweeney have explained about Data holder like hospitals or bank held collection of person specific data. The solution is provided protection for K-anonymity and deployment of policies. Autonomous operation by data holders with extent knowledge suffer from releasing instruction. That information is not compromise confidentiality, national interests and privacy. The proper protection is failed and leads loss to the users. In this paper, K-anonymity protection model, which explored related attacks, can be defeated.

[20] Haibo Hu et.al, have suggested the nearest neighbor query recaptures the every point of the nearest neighbor range. The efficient memory processing is proposed and examined the range as rectangle. snipping techniques in Secondary memory for RNN queries used in both high spatial distances and in 2D. Exo tree is auxiliary model with is in rectangular to existing NN processing algorithm. NN query is one of the query type used in spatial databases. NN queries require the input as point nearest neighbor queries. Range nearest neighbor queries, give a spatial data set processing an NN query involves 2 stages: Secondary memory snipping the memory computation of nearest neighbor and isolated index.

It is proposed RNN as an expansion to point nearest neighbor and continuous nearest neighbor. It is also proposed an contemporary solution based auxiliary index, Exo tree has been proposed and all types of NN queries is processed.

Conclusion

Based on the Literature study the following conclusions are known. Actual geo locations for result set efficiency are necessary. A privacy supportive application would allow the user to aggressively tradeoff the service similarity requirement to determine a sufficiently large area for location perturbation. The sharing of location coordinate delays the user centric design until the accuracy has been evaluated. Here, both location privacy and result exactness should be maintained by using high, medium and low level security model.

References

[1] Ghinita, G., Kalnis, P., Skiadopoulos, S., 2007, "PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems", Proc. 16th Int'l Conf. World Wide Web, pp. 371-380.

[2] Yiu, M.L., Christian Jensen, S., Huang, X., Hua Lu, 2008, "SpaceTwist: Managing the Trade-Offs among Location Privacy, Query Performance, and Query Accuracy in Mobile Services", Proc. 24th Int'l Conf. Data Engineering, pp. 366-375.

[3] Cheng, R., Zhang, Y., Bertino, E., Prabhakar, S., 2006, "Preserving User Location Privacy in Mobile Data Management Infrastructures", Proc. Sixth Workshop Privacy Enhancing Technologies, pp. 393-412.

[4] Kido, H., Yanagisawa, Y., Tetsuji Satoh, 2005, "An Anonymous Communication Technique Using Dummies for Location-Based Services", Proc. IEEE Int'l Conf. Pervasive Services, pp. 88-97.

[5] Jing, Y., Hu, L., Wei-Shinn Ku, Cyrus Shahabi, 2014, "Authentication of k nearest neighbor query on road networks", IEEE Transactions on Knowledge and Data Engineering, Vol 26, No. 6, June.

[6] Gruteser, M., Grunwald, D., 2003, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking", Proc. First Int'l Conf. Mobile Systems, Applications, and Services, pp. 31-42.

[7] Samarati, P., 2001, "Protecting respondents identities in micro data release", IEEE Transactions on Data Engineering.

[8] Ghinita, G., Zhao, K., Papadias, D., Kalnis, P., 2010, "A Reciprocal Framework for Spatial k-Anonymity-Information Systems", Vol. 35, no. 3, pp. 299-314.

[9] Brian, Loh, C. S., Patrick, Then, H. H., 2010, "Ontology-Enhanced Interactive Anonymization in Domain-Driven Data Mining Outsourcing", Second International Symposium on Data, Privacy and E-Commerce.

[10] Gu, T., Wang, X. H., Keng Pung, H., Zhang, D.Q., 2004, "An Ontology-based Context Model in Intelligent Environments", Networks and Distributed Systems Modeling.

[11] Bu, Y., Chen, S., Li, J., Tao, X., Lu, J., 2006, "Context consistency management using ontology based model", Current Trends in Database Technology, EDBT 2006 Workshops, LNCS 4254, pp. 741-755.

[12] Peter Mika, 2005, "A unified model of social networks and semantics", The Semantic Web-ISWC.
[13] Duckham, M., Kulik, L., 2005, "A formal model of obfuscation and negotiation for location privacy", Pervasive 2005, LNCS 3468, pp. 152-170.
[14] Kalnis, P., Ghinita, G., Mouratidis, K., 2007, "Preventing location-based identity inference in anonymous spatial queries", Transactions on Knowledge and Data Engineering.
[15] Gedik, B., Liu, L., 2008, "Protecting location privacy with personalized k-Anonymity: Architecture and algorithms", IEEE Transactions on Mobile Computing, Vol. 7, no. 1, January.
[16] Yang, Y., Papadopoulos, S., Papadias, D., George Kollios, 2008, "Spatial outsourcing for location-based services", In Data Engineering, IEEE 24th International Conference on, pp. 1082-1091, IEEE.
[17] Meyerson, A., Williams, R., 2004, "On the complexity of optimal k-anonymity", In Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems. pp. 223-228, ACM.
[18] Gedik,B., Liu, L., 2005, "Location privacy in mobile systems: A personalized anonymization model", In Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on, pp. 620-629. IEEE.
[19] Sweeney, L., "k-anonymity: A model for protecting privacy", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10, no. 05 (2002): 557-570.
[20] Hu, H., Lee, D.L., 2006, "Range nearest-neighbor query", Knowledge and Data Engineering, IEEE Transactions on 18, no. 1 (2006): 78-91.