ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

PRIVACY PRESERVATION IN LOCATION BASED SERVICES

Dr. P. Kamakshi
*Professor, Department of Computer Science, Kakatiya Institute of Technology and Science, Warangal, India

ABSTRACT

With rapid growth in technology and cost reduction of hardware and storage media, huge amount of data can be acquired and stored. Acquisition and storage of information results in the increase of huge databases. Such databases exceeded the ability of an individual to completely understand and use. The process to analyze such information is more severe in geo-spatial information. In order to analyze and utilize such data repositories to fullest, a few techniques like data mining, expert system, database management system, spatial data analysis, machine learning and artificial intelligence etc. have been tried. Nowadays, spatial data mining (SDM) is a well identified domain of data mining. It can be defined as the discovery of interesting, implicit and previously unknown knowledge from large spatial data bases .Generally in spatial database the main concern of an individual is with disclosure of their information about personal location history records. An intruder or unauthorized person can acquire information such as frequent locations visits about a particular person by submitting queries by statistical or pattern mining and deriving the required results from extracted records. In this paper, techniques are suggested to protect the location privacy of an individual depending on level of protection they must be provided .

KEYWORDS: Privacy preservation, spatial database, location privacy.

INTRODUCTION

In various domains there is a need to deal with geometric, geographic, or spatial data. Spatial data means data related to space. The space to be represented can be surface of the earth i.e.geographic space and the database which is designed to store and retrieve spatial data is called spatial database . Data on spatial databases are stored as coordinates, points, lines and polygons. Spatial database can also handle more complex information like3Dobjects, area coverage.

Today the active area of research is spatial databases, which addresses the need of analysis of spatial database in spatial applications such as Geographic Information Systems (GIS). The development of technology enabled collection of huge amount of geographic information and lot of facilities to users by providing location-based information and mobile applications using spatial databases.

Though this large amount of information provides extremely valuable answer to many queries to analyze human behavior and their culture etc. , privacy violation is a forthcoming risk when detailed information from the customer profile about an individual travel patterns are used by commercial or for political annoyance.

Hence, inspite of several advantages of spatial database , people are anxious about their is anxiety for an individual about their location privacy. Over the last few years, the interest in the concept of locational privacy i.e. geoprivacy among the users has been increased tremendously .

This paper focuses on location privacy violation and suggest various methods to protect individual's location privacy in geographic information collection and analysis.

LOCATION PRIVACY BREACHES IN SPATIAL DATABASE

In today's real world geospatial data play a major role in very critical data management applications, like disaster management, observe changes in environmental conditions , building, roads and city planning and military operations. It requires lot of synchronization among various peoples, organizations and their databases. wide variety of available models and techniques are used access and share geospatial information ,but very little concern was shown towards security, privacy and access control policies in GIS applications.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

The development of wireless and mobile technologies have shown marvelous improvement in location-based services (LBSs). Though these services provide improved functionalities, they are exposed to new kind of vulnerabilities that can be exploited to cause security and privacy breaches. Therefore, location data of individuals used by such services must be adequately protected. New model for such services must be provided with privacy preferences for location data and procedures to implement them.

PROPOSED WORK

The development of mobile phones, global ositioning system (GPS) devices, and radio-frequency identification (RFID) chips made easy to access the location information. Users have the ability submit different queries to location based server and get the desired results. To obtain exact and true information one has to submit number of queries to the database server. There is also a possibility that an intruder identifies an unreliable database server and tries to access sensitive information about and an individual based on their location information and queries. For example, an opponent can easily identify a user's habits and interests by observing the places and time the user frequently visits.

Location privacy of an individual can be preserved by spatial cloaking technique. Spatial cloaking technique blurs exact location of the person . To blur the location information, spatial cloaking algorithm can be applied before submitting the results to the client or before it is submitted to a location-based database server.

In this paper the database consists of travelling information of an individual .The data consists of details of all the locations through which a person travels by. Revealing the location information of an individual is more dangerous when the person is top level authority like minister or higher officials.

The location privacy can be completely preserved by hiding all the location through which the higher official travels and stay during his journey. But this doesn't solve the problem. Because for providing security and protection , the other official like army people must be informed about the minute details about the travel information and location through which the higher official travels. Hence, people who want to know the travelling information about a celebrity are divided into three categories.

The first category is for security people who require the detailed information about celebrity travelling plan to provide proper security and protection. The complete details are revealed when first category user submit the query.

The second category users are the people who just want to know only the main locations i.e. starting and destination location of a celebrity. People under this category are students or general public. User under this category receives the answer to their query at a very high abstract level without any detailed information.

The people under third category are of interest. In this category the user are mixed type. Few are genuine and others may be intruders and unauthorized user. They pose number of queries to the database to know whereabouts the important persons. Under this category the people may be from organizations or companies or political parties who really want to know whereabouts of the celebrity. People under this category are the people from organization or companies who really and genuinely want to interact with the particular important persons.

There is also a possibility that there may be intruders who belongs to same or different organizations and who pose number of queries and pretends to be authorized user.

As we can't discriminate the true user and an intruder under third category, a technique is developed to answer the queries in a modified manner. The true value of location is modified in such a manner that the results of the query doesn't deviate much from the expected results and the actual true value of locations are not revealed. Another solution is also proposed for the queries under this category. Each time the user under third category login and pose a query the results are modified by another random value but within the range.

RESULTS

User under Category 1 submits the query and get detailed travelling information about the locations between the source and destination about the person travelling. Figure 1 below shows the detailed information about locations and distances in terms of co-ordinates.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

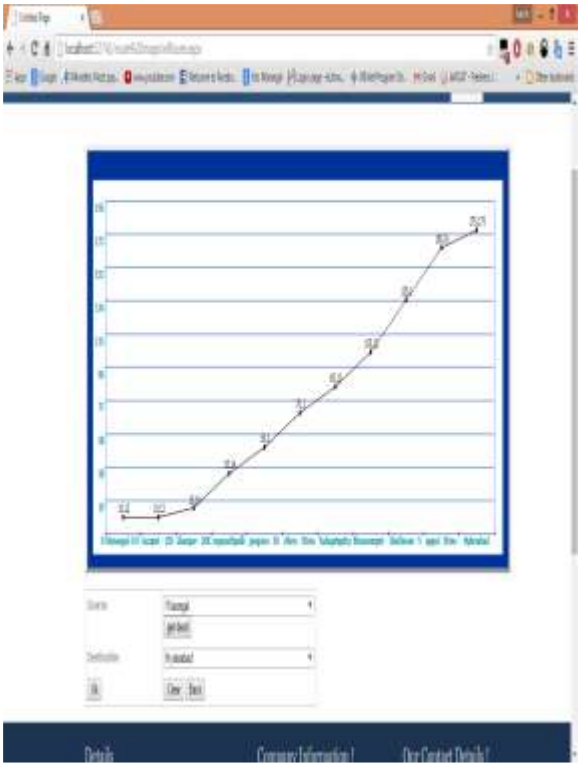

Figure1. Detailed travelling information for user under category1.

User under Category 2 submits the query and obtains only the information at very high abstract level. In the figure 2 below it is observed that only 3 location details out of 11 locations are shown.

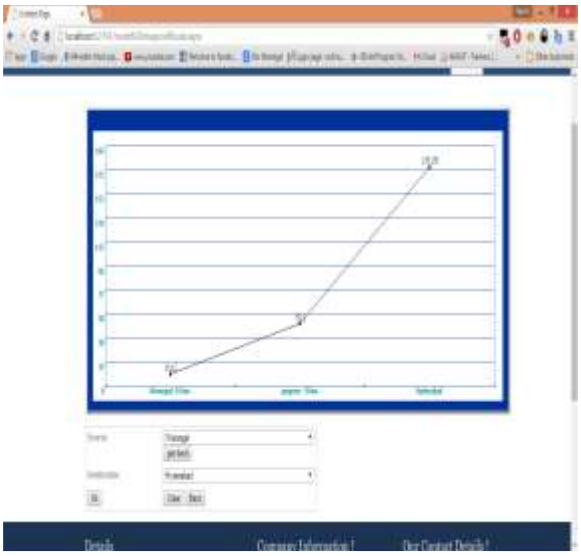

Figure 2. Abstract travelling information for user under category2

User under Category 3 submits the query and gets the modified version of the travelling information. This modified version doesn't deviate completely from the original travelling plan, at the same time it hides the true information about the location. Figure 3 below shows the modified value which hides the true value and also give the result which is within the given range.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

Figure 3 Modified travelling information for user under category3

CONCLUSION

With rapid growth in mobile technology ,cost reduction in storage media huge amount of information can be collected and stored. One of such data is spatial data which is related to location and geographical space. This paper focuses the problem of protecting individual location privacy of an individual while continuously publishing a stream of location data available in database server. In this framework the user who submit the queies are categorized and based on their category the location or travelling information results about an individual is revealed.

This technique provides enough privacy to an individual by not disseminating his or her location information to all users. The desired and true information is revealed only to the people who provide security and protection to the higher officials.

REFERENCES

[1] Wei-Shinn Ku,Yu Chen,Roger Zimmermann, "Privacy Protected Spatial Query Processing for Advanced Location Based Services",in Proc. Springer Science+Business Media, LLC. 2008
[2] Deren Li , Shuliang Wang, " Concepts, principles and applications of spatial data mining and knowledge discovery" , in Proc. ISSTM 2005, August, 27-29, 2005, Beijing, China
[3] Martin Ester, Hans-Peter Kriegel, Jörg Sander, "Algorithms and Applications for Spatial Data Mining", in Proc. Geographic Data Mining and Knowledge Discovery, Research Monographs in GIS, Taylor and Francis, 2001.
[4] Marco Gruteser, Xuan Liu, "Protecting Privacy in Continuous Location- Tracking Applications", in Proc. IEEE Computer Society,2004 IEEE _ IEEE SECURITY & PRIVACY

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

[5] G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications," IEEE Pervasive Computing, vol. 2, no. 1, 2003, pp. 56–64.
[6] J. Cuellar, J. Morris, and D. Mulligan, "IETF Geopriv Requirements," 2002, www.ietf.org/html.charters/geoprivcharter.html.
[7] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking,", in Proc. 1st Int'l Conf. Mobile Systems, Applications, and Services, Usenix Press, 2003, pp. 31–42.
[8] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in Proc. Int'l Conf. Mobile Systems, Applications, and Services, Usenix Press, 2003, pp. 31–42.
[9] A. Beresford and F. Stajano, "Location Privacy In Pervasive Computing," IEEE Pervasive Computing, vol. 2, no. 1, 2003, pp. 46–55.
[10] P. Samarati and L. Sweeney, " Protecting Privacy when Disclosing Information: k-anonymity and its Enforcement Through Generalization and Suppression", tech. report SRI-CSL-98-04, SRI Int'l Computer Science Laboratory, 1998.
[11] L. Sweeney, "Achieving k-Anonymity Privacy Protection Using Generalization and Suppression," in Proc. Int'l J. Uncertainty, Fuzziness, and Knowledge-Based Systems, vol. 10, no. 5, 2002, pp. 571–588.